М. Б. Гузаиров, И. В. Машкина, Е. С. Степанова

ПОСТРОЕНИЕ МОДЕЛИ УГРОЗ С ПОМОЩЬЮ НЕЧЕТКИХ КОГНИТИВНЫХ КАРТ НА ОСНОВЕ СЕТЕВОЙ ПОЛИТИКИ БЕЗОПАСНОСТИ

На сегодняшний день, несмотря на наличие известных зарубежных и отечественных стандартов в области *управления рисками* нарушения информационной безопасности (ИБ), проблема численной оценки риска нарушения ИБ остается актуальной. В стандартах формулируются только критерии оценки безопасности, но не содержится методик оценивания и важных деталей, позволяющих проводить сравнительный анализ различных вариантов защиты информационных систем (ИС).

Известно также достаточно большое число программных продуктов, позволяющих автоматизировать расчет рисков нарушения ИБ. Они обладают определенными достоинствами и недостатками. Так, например, общими недостатками CRAMM, RiskWatch, ГРИФ являются: *ориентация на этап эксплуатации систем защиты информации* (СЗИ); кроме того, в средствах отсутствует возможность учесть данные *об изменении технологии обработки информации* на объекте защиты и сведения о технических х*арактеристиках* используемых или планируемых средств защиты (СрЗ). Вышеперечисленные продукты не позволяют оценить риски нарушения информационной безопасности при проектировании системы защиты информации, сравнить в количественном отношении различные варианты наборов СрЗ для построения СЗИ.

В рамках данной статьи предлагается *разделение* задачи защиты информационных ресурсов от *случайных и преднамеренных, целенаправленных воздействий*. При расчете рисков нарушения информационной безопасности во внимание принимаются угрозы несанкционированного доступа (НСД) и целенаправленных утечек, так как для защиты от *случайных воздействий* должны использоваться средства *повышения надежности* технических и программных средств. Таким образом, целесообразно прежде всего решить вопрос разработки метода оценки риска нарушения информационной безопасности от угроз НСД к защищаемой информации и ее утечки.

Исследования проведены с целью построения модели *актуальных* угроз, которые связаны с нарушением информационной политики безопасности (ИПБ) и попытками внешних вторжений злоумышленника для получения несанкционированного доступа к защищаемой информации.

Для построения модели угроз необходимо располагать сведениями о сетевой инфраструктуре, субъектах и объектах информационного взаимодействия, правах доступа, используемых сервисах безопасности, т. е. об информационной системе – объекте защиты.

Сведения об объекте защиты следует представить в модельной форме, дать математическое описание ИС, что позволит наиболее полно ее исследовать.

Существует несколько подходов к математическому описанию сложных систем. Наиболее общим в теории систем является *теоретико-множественный* подход.

Основой построения модели является описание объектов в виде *совокупности элементов*, связанных между собой *отношениями*, отображающими семантику предметной области.

На основе теоретико-множественного подхода рассмотрим построение модели информационной инфраструктуры СЗИ, соответствующей основным принципам построения архитектуры безопасности, рекомендуемым в [1]:

- введение категорий конфиденциальности (критичности, важности) информации и создание соответственно сетевых сегментов, на хостах которых хранится и обрабатывается информация одного и того же уровня конфиденциальности. При этом каждый пользователь внутри своего сетевого сегмента имеет доступ к информации одного уровня конфиденциальности. В этом случае не смешиваются потоки информации разных уровней конфиденциальности;

- выделение в отдельный сегмент всех внутренних серверов компании. Эта мера также позволяет изолировать потоки информации между пользователями, имеющими различные уровни доступа.

Зададим три категории конфиденциальности (критичности, важности) информации: низкая («Н»), средняя («С») и высокая («В»).

Зададим множество сегментов сети С:

$$C = C^H \cup C^C \cup C^B, \quad (1)$$

где C^H, C^C, C^B — подмножества сегментов, в которых хранится и обрабатывается информация соответственно с низким, средним и высоким уровнем конфиденциальности;

$$C^H = \{c_n^H : c_n^H \in C^H\}, n \in [1,N],$$
$$C^C = \{c_m^C : c_m^C \in C^C\}, m \in [1,M], \quad (2)$$
$$C^B = \{c_l^B : c_l^B \in C^B\}, l \in [1,L],$$

где N, M, L — число сегментов, в которых хранится и обрабатывается информация соответственно категории «Н», «С», «В».

Множество информационных объектов O в сети представляет собой *объединение* множеств:

$$O = O^H \cup O^C \cup O^B, \quad (3)$$

где O^H, O^C, O^B — подмножества информационных объектов категории «Н», «С», «В» соответственно.

В свою очередь, множества O^H, O^C, O^B состоят из подмножеств информационных объектов, обрабатываемых в сегментах сети, и могут быть представлены в виде:

$$O^H = \bigcup_{n \in N} O_n^H,$$
$$O^C = \bigcup_{m \in M} O_m^C, \quad (4)$$
$$O^B = \bigcup_{l \in L} O_l^B,$$

В [2] приведена модель информационной системы, в которой все пользователи, имеющие уровень доступа «С», обладают одинаковыми правами доступа к информации уровня конфиденциальности «С», обрабатываемой соответственно во всем множестве сегментов C^C; все пользователи, имеющие уровень доступа «В», обладают одинаковыми правами доступа к информации уровня конфиденциальности «В», обрабатываемой во всем множестве сегментов C^B.

В данной работе учитывается тот факт, что хотя уровень конфиденциальности информации, обрабатываемой в разных подразделениях компании, может быть один и тот же, однако, в соответствии с бизнес-процессами, доступ к информационным ресурсам пользователям, имеющим достаточный уровень доступа, но относящимся к другим подразделениям, не может быть предоставлен.

Поэтому в данной модели принято:

$$\bigcap_{m \in M} O_m^C = \{\},$$
$$\bigcap_{l \in L} O_l^B = \{\}, \quad (5)$$

что делает потенциально возможными угрозы из сегментов подмножеств C^C и C^B к информационным объектам O^C, O^B, обрабатываемым в других сегментах соответствующих подмножеств C^C и C^B.

Зададим *отображение* множества информационных объектов во множество сегментов соответствующей категории конфиденциальности:

$$O_n^H \to C_n^H,\ n \in N,$$
$$O_m^C \to C_m^C,\ m \in M, \quad (6)$$
$$O_l^B \to C_l^B,\ l \in L,$$

Обозначим множество субъектов доступа через S. По расположению субъекта доступа относительно информационного объекта пользователи подразделяются на внешние и внутренние:

$$S = S^{BH} \cup S^{BHШ}, \quad (7)$$

где S^{BH} – внутренние субъекты доступа;

$S^{BHШ}$ – внешние субъекты доступа.

Множество субъектов доступа, внешних или внутренних, можно рассматривать как множество источников угроз, под которыми понимается атакующая программа или оператор, непосредственно осуществляющий воздействия на сеть.

Внутренние угрозы связаны с нарушением принятой политики безопасности: попытками доступа пользователя к информационным ресурсам, уровень конфиденциальности которых превышает его уровень доступа (попытки сетевых соединений, запуска приложений и другое), нелегальным поведением пользователя на компьютере или сервере.

Множество внутренних субъектов доступа есть объединение подмножеств

$$S^{BH} = S^H \cup S^C \cup S^B, \quad (8)$$

где S^H, S^C, S^B – подмножества пользователей или процессов с уровнем доступа «Н», «С», «В» соответственно.

Множества S^H, S^C, S^B могут быть представлены как:

$$S^H = \bigcup_{n \in N} S_n^H,$$
$$S^C = \bigcup_{m \in M} S_m^C, \quad (9)$$
$$S^B = \bigcup_{l \in L} S_l^B,$$

Зададим отображения множеств субъектов доступа в подмножества сегментов сети:

$$S_n^H \to C_n^H,\ n \in N,$$
$$S_m^C \to C_m^C,\ m \in M, \quad (10)$$
$$S_l^B \to C_l^B,\ l \in L,$$

Множество внешних субъектов доступа есть объединение множеств

$$S^{BHШ} = S^{ПВНШ} \cup S_t^{ВНШ},\ t \in [1, T\ ], \quad (11)$$

где $S^{ПВНШ}$ – внешние пользователи, обладающие правами доступа;

$S_t^{ВНШ}$ – несанкционированный субъект доступа;

T – число точек доступа через периметр.

В [2] предложено для описания угрозы как канала несанкционированного доступа, утечки, деструктивных воздействий указать субъект доступа, информационный объект, к которому осуществляется доступ с нарушением прав и правил, путь распространения угрозы до сегмента, информационный носитель. Таким образом, угроза может быть описана кортежем

$$U = \langle S, A, Э_c, Э_x, П, O(C) \rangle, \quad (12)$$

где S – источник угрозы – субъект доступа (пользователь, внешний злоумышленник или запущенные ими процессы);

A – оборудование в канале связи (коммутаторы, маршрутизаторы и др.);

$Э_c$, $Э_x$ – сервисы безопасности на пути распространения угрозы, соответственно сетевые и хостовые (МСЭ, СОА, журналы регистрации аномальных сетевых соединений, журналы регистрации операционных систем и др.);

$П$ — протоколы;

O — объект доступа в соответствующем сегменте.

Множество угроз включает в себя подмножества:

$$U = U^{ВНШ} \cup U^{ВН} \cup U^{ВН\_С}, \quad (13)$$

где $U^{ВНШ}$ – подмножество внешних угроз через проводные, беспроводные и модемные линии связи;

$U^{ВН}$ – подмножество внутренних межсегментных угроз;

$U^{ВН\_С}$ – подмножество внутренних угроз, источники которых расположены в том же локальном сегменте, что и объект доступа.

С учетом принципа [1] построения архитектуры безопасности объекта защиты $U^{ВН\_С} = \{\}$. Таким образом, в работе рассматриваются внешние угрозы и внутренние межсегментные.

Внешние угрозы — это потенциально возможные действия, заключающиеся в поиске и использовании той или иной уязвимости, предпринимаемые:

- злоумышленником с целью проникновения с удаленного компьютера внутрь защищаемой системы, получения, без права на то, удаленного доступа к ресурсам ИС и хищения данных или вызова отклонения от нормального протекания информационных процессов;
- удаленным пользователем, имеющим определенные права, пытающимся превысить уровень своих полномочий.

Внешняя угроза связана с внешним субъектом доступа и описывается кортежем

$$U^{ВНШ} = \langle S^{ВНШ}, A, З_с, З_х, П, O(C)\rangle. \quad (14)$$

Внутренний нарушитель – сотрудник, прошедший все рубежи авторизации, обладающий определенными полномочиями и имеющий доступ к корпоративной информации, представляет не меньшую опасность, чем злоумышленник и внешний пользователь.

Согласно ГОСТ [3], несанкционированный доступ – процесс ознакомления внутренних пользователей, имеющих уровень доступа «Н» к информации с уровнем конфиденциальности «С», «В»; попытка ознакомления пользователей, имеющих уровень доступа «С», с информацией с уровнем конфиденциальности «В», а также попытка ознакомления с информацией того же уровня конфиденциальности, но обрабатываемой в других подразделениях организации. Утечка – неконтролируемое распространение защищаемой информации, инициируемое субъектами-пользователями с достаточно высокими правами доступа.

Подмножество внутренних угроз включает в себя подмножества угроз несанкционированного доступа $U_{m(n)}^{ВН}$, $U_{l(n)}^{ВН}$, $U_{l(m)}^{ВН}$, $U_{m(\mu)}^{ВН}$, $U_{l(\lambda)}^{ВН}$:

$$U_{m(n)}^{ВН} = \langle S_n^{Н}, A, З_с, З_х, П, O_m^{С}(C_m^{С})\rangle, \quad (15)$$

$$U_{l(n)}^{ВН} = \langle S_n^{Н}, A, З_с, З_х, П, O_l^{В}(C_l^{В})\rangle, \quad (16)$$

где $U_{m(n)}^{ВН}$, $U_{l(n)}^{ВН}$ – угрозы НСД к информационным объектам категории «С» и «В» соответственно в случае, когда нарушитель имеет учетную запись в системе как пользователь с правами доступа к информации с уровнем конфиденциальности «Н» и пытается превысить свои привилегии;

$$U_{l(m)}^{ВН} = \langle S_m^{С}, A, З_с, З_х, П, O_l^{В}(C_l^{В})\rangle, \quad (17)$$

где $U_{l(m)}^{ВН}$ – угроза несанкционированного доступа к информационным объектам категории «В» в случае, когда нарушитель имеет учетную запись пользователя с правами доступа к информации с уровнем конфиденциальности «С» и пытается превысить свои привилегии;

$$U_{m(\mu)}^{ВН} = \langle S_\mu^{С}, \text{А}, З_с, З_х, \text{П}, \text{O}_m^{С}(\text{C}_m^{С})\rangle, \mu\in[1,M], \text{m}\in[1, \mu)\cup(\mu,\text{M}], \quad (18)$$

$$U_{l(\lambda)}^{ВН} = \langle S_\lambda^{С}, \text{А}, З_с, З_х, \text{П}, \text{O}_l^{В}(\text{C}_l^{В})\rangle, \lambda\in[1,L], 1\in[1, \lambda)\cup(\lambda,\text{L}], \quad (19)$$

где $U_{m(\mu)}^{ВН}$, $U_{l(\lambda)}^{ВН}$ – угрозы информационным объектам, обрабатываемым в сегментах $C_m^{С}$, $C_l^{В}$, реализуемые нарушителями, имеющими учетные записи в системе как пользователи с

правами доступа «С», «В», но относящимися к разным сегментам соответствующих подмножеств сегментов C^C, C^B. Таким образом, субъект доступа в сегменте $C_{\mu}{}^{C}$ потенциально рассматривается как источник угрозы объектам, обрабатываемым в других сегментах из множества C^C. Субъект доступа в сегменте $C_{\lambda}{}^{C}$ рассматривается как источник угрозы объектам, обрабатываемым в других сегментах из множества C^B.

Кроме того, подмножество внутренних угроз включает подмножества $U_{m(m)}{}^{BH}$ и $U_{l(l)}{}^{BH}$:

$$U_{m(m)}{}^{BH} = \langle S_m{}^{C}(O_m{}^{C}), \text{А}, \text{З}_\text{с}, \text{З}_\text{х}, П, O_n{}^{H}\rangle, \quad (20)$$

$$U_{l(l)}{}^{BH} = \langle S_l^{B}(O_l^{B}), \text{А}, \text{З}_\text{с}, \text{З}_\text{х}, П, O_m{}^{C} \cup O_n{}^{N}\rangle, \quad (21)$$

где $U_{m(m)}{}^{BH}$ и $U_{l(l)}{}^{BH}$ – угрозы неконтролируемого распространения (утечки) информационных объектов категорий «С» и «В», реализуемые пользователями соответствующих сегментов.

Основой для организации процесса защиты информации является информационная политика безопасности, которая задает правила взаимодействия информационных субъектов (пользователей, процессов) с информационными объектами.

Разграничение прав доступа на уровне сети определяется в соответствии с принятой информационной политикой безопасности.

Модель управления доступом является формальным выражением разграничительной политики и определяет правила ее задания для доступа к защищаемым ресурсам, а также правила обработки запросов доступа к защищаемым ресурсам [4]. Авторизованными считаются операции с правами доступа, определенными в матрице доступа.

Модель доступа, как дискреционную, так и мандатную, можно представить в виде матрицы, где линейно упорядоченные множества объектов доступа O и субъектов доступа S характеризуют строки и столбцы соответственно. Множества упорядочены таким образом, что по мере возрастания порядкового номера субъекта или объекта права субъекта сокращаются или значение конфиденциальности объекта понижается.

Важно отметить, что для полного отображения всех условий модели необходимо сгруппировать объекты доступа по двум критериям: по уровню критичности (конфиденциальности) и по принадлежности групп объектов к тем или иным подразделениям компании, организации и т. д., реализующим специфичные для них бизнес-процессы.

Для наглядности процессов реализации несанкционированного доступа и утечки конфиденциальной информации предлагается построение *матриц угроз*, получаемых на основе матриц доступа на уровне сети. В качестве субъектов доступа в матрицах угроз выступают как внутренние несанкционированные процессы и пользователи-нарушители, так и внешние – удаленные пользователи и злоумышленник.

На основе вышеизложенного теоретико-множественного подхода к описанию ИС и построения матриц угроз может быть построена модель угроз в проекции на топологию сети, отражающая процесс реализации угроз на пути их распространения с указанием источника и объекта атаки.

В работе предложено для построения модели угроз и далее для анализа рисков нарушения информационной безопасности использовать нечеткие когнитивные карты (НКК). НКК, построенная в проекции на топологию сети, позволяет *визуализировать пути* распространения возможных угроз от их потенциальных источников – заинтересованных субъектов к критичным информационным ресурсам в сети, представленные кортежами (15)–(21).

Нечеткие когнитивные карты задаются в виде ориентированного графа и представляют моделируемую систему в виде множества концептов$\{K_1, K_2..K_q\}$, существенных для понимания исследуемой проблемы и связанных между собой отношениями влияния, отражающими причинно-следственные связи и показывающими степень влияния одного концепта на другой $w_{ij} \in W$ [5].

Определим путь между входным концептом K_i – источником угрозы и выходным концептом K_y – объектом атаки (информационным ресурсом) нечеткой когнитивной карты следующим образом: $K_i \to K_y$, $(K_i, K_{z_1}, K_{z_2}, K_{z_3} \ldots K_{z_v}, K_y)_j$,

где $j \in [1, J]$ – номер пути между концептами K_i и K_y,

K_{z_v} – промежуточные концепты,

$v \in [1, V]$ – количество промежуточных концептов.

На рис. 1 приведен случай, когда между концептами K_i и K_y могут быть построены J различных путей.

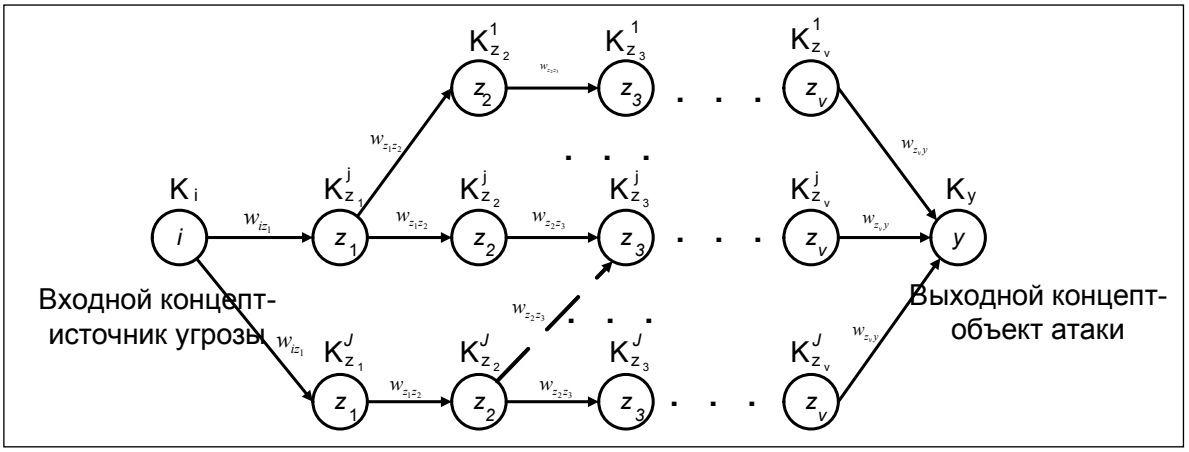

Рис. 1. Множество путей между концептами K_i и K_y

Нечеткие значения выходного концепта могут быть заданы с использованием операции Т-нормы над нечеткими значениями весов влияния входных концептов, характерной для нечеткой логики.

Отдельные нечеткие влияния входных концептов, воздействующих на выходной концепт, объединяются на основе S-нормы [6]:

$$w_{iy} = \underset{j=1}{\overset{J}{S}} \; \underset{z \in Z}{T} w_{z,z+1}, \tag{22}$$

где w_{iy} – вес влияния концепта i на концепт y.

Наиболее распространенными разновидностями Т-нормы являются операции минимума и алгебраического произведения, а наиболее распространенной разновидностью S-нормы – операция максимума.

В решаемой задаче веса $w_{z,z+1}$ соответствуют значениям уязвимостей компонентов инфраструктуры – программного обеспечения, коммуникационного оборудования, протоколов связи и сервисов безопасности, представленных в НКК промежуточными концептами K_{z+1}^{j}; $\rho_{акт}$ – вероятность активизации входного концепта; $\rho_{ООИ}$ – характеристика, учитывающая особенности обработки информации на объекте защиты. Тогда вероятность реализации угрозы на j-м пути может быть вычислена по формуле:

$$\rho_j = \rho_{акт} \cdot \rho_{ООИ} \cdot \underset{z \in Z}{T} w_{z,z+1}. \tag{23}$$

Максимальное значение ρ_j между концептами K_i и K_y будет соответствовать вероятности реализации угрозы $P^U(K_i \to K_y)$ на информационный ресурс, представленный концептом K_y, источником атаки:

$$P^U(K_i \to K_y) = \max_{j=1}^{J} P_j. \tag{24}$$

На рис. 2 приведена нечеткая когнитивная карта, показывающая различные пути распространения угроз от источников угроз – входных концептов $K_i^{S_1^{ВНШ}}$, $K_i^{S_2^{ВНШ}}$ и $K_i^{S_1^{СIВ}}$ к подмножеству информационных ресурсов, расположенных в сегменте C_1^B, представленных выходным концептом $K_y^{O_l^B}$.

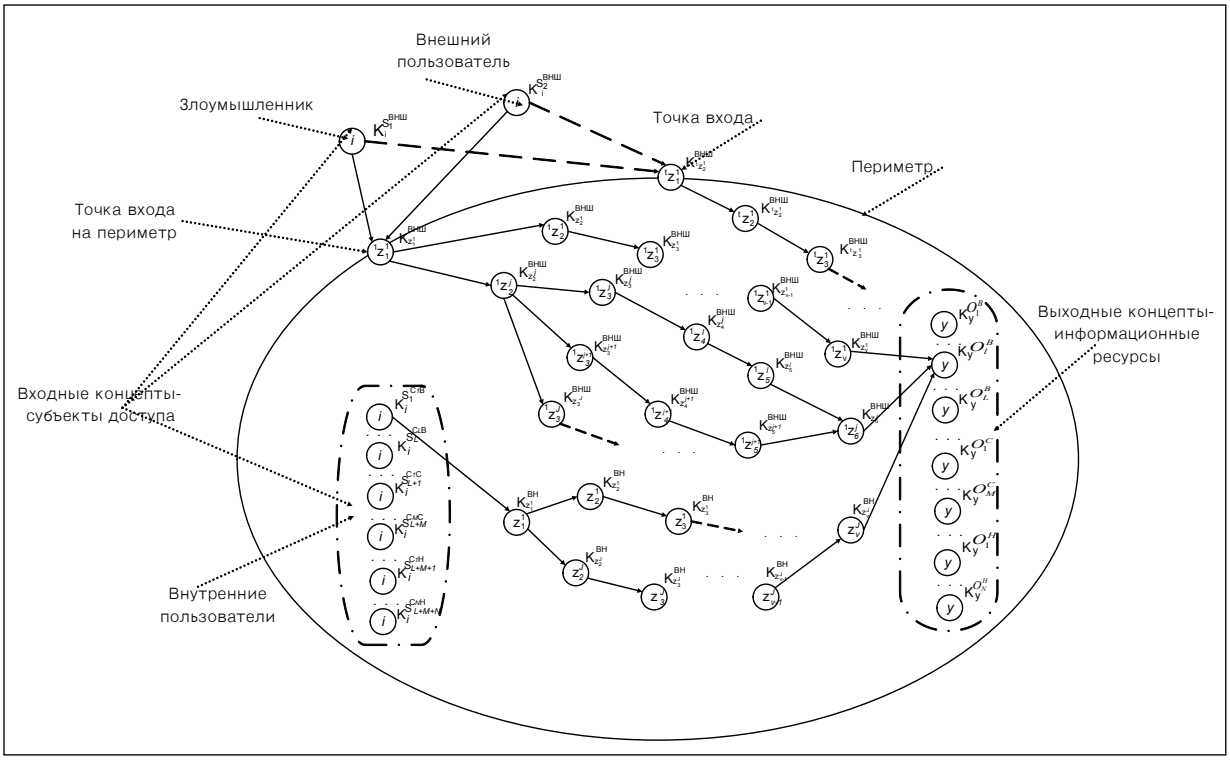

Рис. 2. Нечеткая когнитивная карта – модель угроз

Вероятности реализации угроз на информационные ресурсы с уровнями конфиденциальности «Н», «С», «В» могут быть определены по формулам:

$$P_{C_n H}^{U} = 1 - (1 - P^{U^{ВНШ}}) \cdot (1 - P^{U^{ПВНШ}}), \tag{25}$$

$$P_{C_m C}^{U} = 1 - (1 - P^{U^{ВНШ}}) \cdot (1 - P^{U^{ПВНШ}}) \cdot (1 - P^{U_{m(n)}^{ВН}}) \cdot (1 - P^{U_{m(\mu)}^{ВН}}) \cdot (1 - P^{U_{m(m)}^{ВН}}), \tag{26}$$

$$P_{C_l B}^{U} = 1 - (1 - P^{U^{ВНШ}}) \cdot (1 - P^{U^{ПВНШ}}) \cdot (1 - P^{U_{l(n)}^{ВН}}) \cdot (1 - P^{U_{l(m)}^{ВН}}) \cdot (1 - P^{U_{l(\lambda)}^{ВН}}) \cdot (1 - P^{U_{l(l)}^{ВН}}). \tag{27}$$

Вероятности $P^{U^{ВНШ}}$, $P^{U^{ПВНШ}}$, $P^{U_{m(n)}^{ВН}}$, $P^{U_{l(n)}^{ВН}}$, $P^{U_{l(m)}^{ВН}}$, $P^{U_{m(\mu)}^{ВН}}$, $P^{U_{l(\lambda)}^{ВН}}$, $P^{U_{m(m)}^{ВН}}$, $P^{U_{l(l)}^{ВН}}$ определяются по формуле (23) для соответствующих путей распространения угроз.

Величины относительного риска могут быть определены по формулам:

$$\overline{R_{C^H}} = \sum_{n=1}^{N} P_{C_n^H}^{U} \cdot \frac{Cm_{C_n^H}}{Cm_{\Sigma}}, \tag{28}$$

$$\overline{R_{C^C}} = \sum_{m=1}^{M} P_{C_m^C}^{U} \cdot \frac{Cm_{C_m^C}}{Cm_{\Sigma}}, \tag{29}$$

$$\overline{R_{C^B}} = \sum_{l=1}^{L} P_{C_l^B}^{U} \cdot \frac{Cm_{C_l^B}}{Cm_{\Sigma}}, \tag{30}$$

где $\frac{Cm_{C_n^H}}{Cm_\Sigma}$, $\frac{Cm_{C_m^C}}{Cm_\Sigma}$, $\frac{Cm_{C_l^B}}{Cm_\Sigma}$ – относительные стоимости информационных ресурсов, обрабатываемых в сегменте C_n^H, C_m^C и C_l^B соответственно.

Величина полного относительного риска может быть определена по формуле:

$$\overline{R} = \overline{R_{C^H}} + \overline{R_{C^C}} + \overline{R_{C^B}} \qquad (31)$$

Хотя в работе [7] доказывается, что вопрос определения безопасности компьютерной системы в общем случае неразрешим, т. е. не существует алгоритма, позволяющего определить, будет ли компьютерная система обеспечивать безопасность информации *в общем случае*, в настоящей работе предлагается метод расчета рисков для ИС, топология сети которой построена в соответствии с ГОСТ [1] и является *обобщенной*.

II.

Метод численной оценки риска и программно реализованный алгоритм решения задачи были апробированы для информационной системы, инфраструктура которой построена с учетом рекомендаций ГОСТ [1] и работы [8] к базовой структуре сети.

На рис. 3 приведена топология сети объекта защиты.

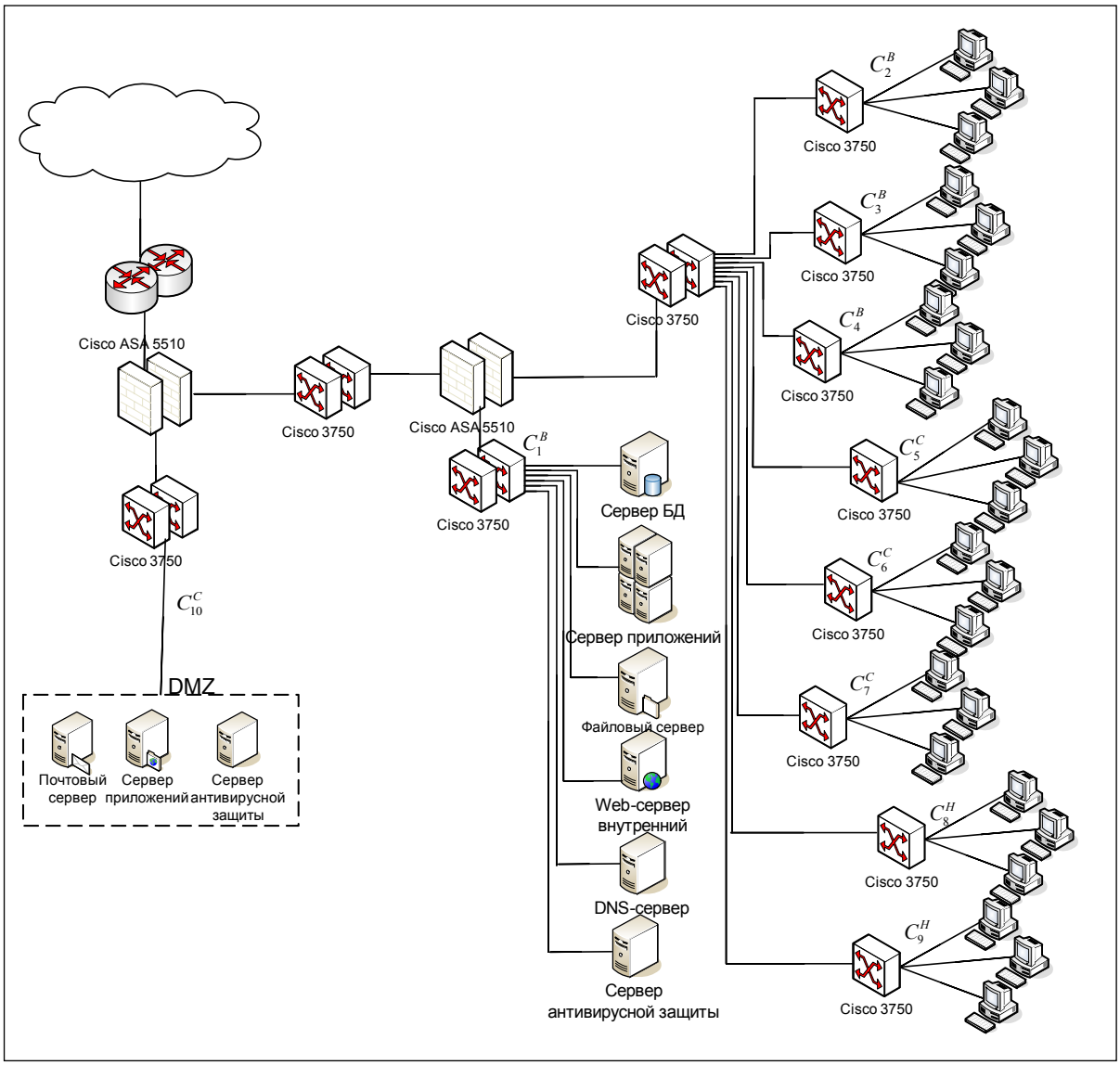

Рис. 3. Топология сети объекта защиты

С учетом существующих на объекте защиты бизнес-процессов и категорирования информации, обрабатываемой в определенных сегментах, сформируем матрицу прав доступа внутренних и удаленных пользователей к информационным ресурсам, приведенную в таблице 1.

Таблица 1.

Матрица разграничения прав доступа

	S_1 (C_2^B)	S_2 (C_3^B)	S_3 (C_4^B)	S_4 (C_5^C)	S_5 (C_6^C)	S_6 (C_7^C)	S_7 (C_8^H)	S_8 (C_9^H)	$S_t^{\text{ПВНШ}}$
O_1^B	rw	rw	rw	rw	rw	rw	rw	rw	–
O_2^B	rw	–	–	w	–	–	–	–	–
O_3^B	–	rw	–	–	w	–	w	–	–
O_4^B	–	–	rw	–	–	w	–	w	–
O_5^C	r	–	–	rw	–	–	–	–	–
O_6^C	–	r	–	–	rw	–	w	–	–
O_7^C	–	–	r	–	–	rw	–	w	–
O_{10}^C	rw	rw	rw	rw	rw	rw	–	–	rw
O_8^H	–	r	–	–	r	–	rw	–	–
O_9^H	–	–	r	–	–	r	–	rw	–

Матрицы НСД и утечки строятся на основе матрицы разграничения прав доступа.

В таблицах 2, 3 приведены матрицы, отражающие возможные процессы несанкционированного доступа и утечки информации соответственно.

Таблица 2.

Матрица НСД к информационным объектам

	S_1 (C_2^B)	S_2 (C_3^B)	S_3 (C_4^B)	S_4 (C_5^C)	S_5 (C_6^C)	S_6 (C_7^C)	S_7 (C_8^H)	S_8 (C_9^H)	$S_t^{\text{ПВНШ}}$	$S_t^{\text{ВНШ}}$
O_1^B	1	1	1	1	1	1	1	1	1	1
O_2^B	–	1	1	1	1	1	1	1	1	1
O_3^B	1	–	1	1	1	1	1	1	1	1
O_4^B	1	1	–	1	1	1	1	1	1	1
O_5^C	–	–	–	–	1	1	1	1	1	1
O_6^C	–	–	–	1	–	1	1	1	1	1
O_7^C	–	–	–	1	1	–	1	1	1	1
O_{10}^C	–	–	–	1	1	1	1	1	–	1
O_8^H	–	–	–	–	–	–	–	–	1	1
O_9^H	–	–	–	–	–	–	–	–	1	1

Формат матрицы утечки предлагается следующим: столбцы характеризуют линейно упорядоченные множества пользователей-нарушителей S, а строки – информационные объекты, созданные пользователем. Для осуществления угрозы утечки, т. е. распространения защищаемой информации через периметр сети к злоумышленнику пользователем с высоким уровнем доступа, необходимо предварительно понизить уровень конфиденциальности интересующего его информационного объекта.

Таблица 3.

Матрица утечек

	$S_1 (C_2^B)$	$S_2 (C_3^B)$	$S_3 (C_4^B)$	$S_4 (C_5^C)$	$S_5 (C_6^C)$	$S_6 (C_7^C)$	$S_7 (C_8^H)$	$S_8 (C_9^H)$
O_1^B	–	–	–	–	–	–	–	–
O_2^B	–	–	–	–	–	–	–	–
O_3^B	–	–	–	–	–	–	–	–
O_4^B	–	–	–	–	–	–	–	–
O_5^C	1	1	1	–	–	–	–	–
O_6^C	1	1	1	–	–	–	–	–
O_7^C	1	1	1	–	–	–	–	–
O_{10}^C	1	1	1	–	–	–	–	–
O_8^H	1	1	1	1	1	1	–	–
O_9^H	1	1	1	1	1	1	–	–

Матрицы угроз являются исходными данными для построения НКК, задавая входные и выходные концепты карты.

Нечеткая когнитивная карта *отражает* процесс реализации угроз *через используемые уязвимости* программного обеспечения, коммуникационного оборудования, протоколов связи и сервисов безопасности.

НКК, представляющая схему НСД удаленного пользователя – нарушителя и злоумышленника на информационные ресурсы, в проекции на топологию сети приведена на рис. 4.

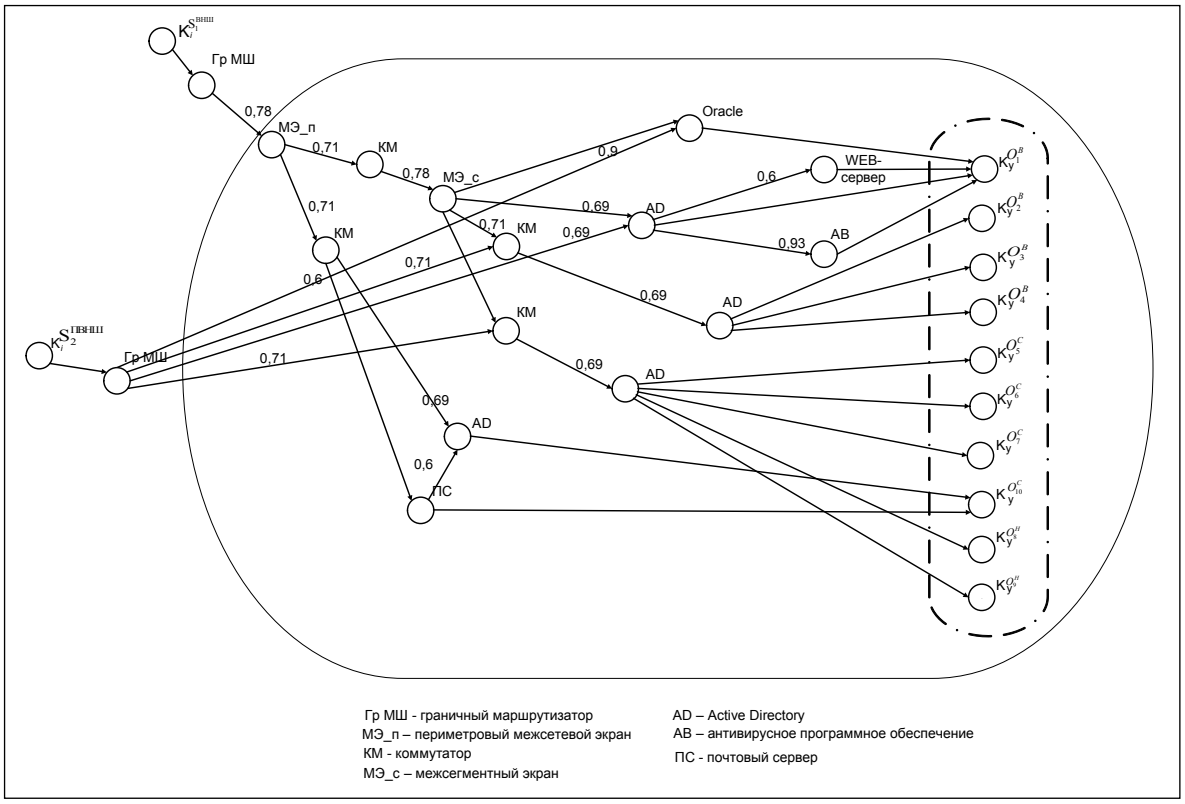

Рис. 4. Нечеткая когнитивная карта – модель угроз НСД, реализуемых удаленным пользователем и злоумышленником, через периметр

На рис. 5 приведена НКК – модель угроз, источниками которых выступают внутренние пользователи-нарушители.

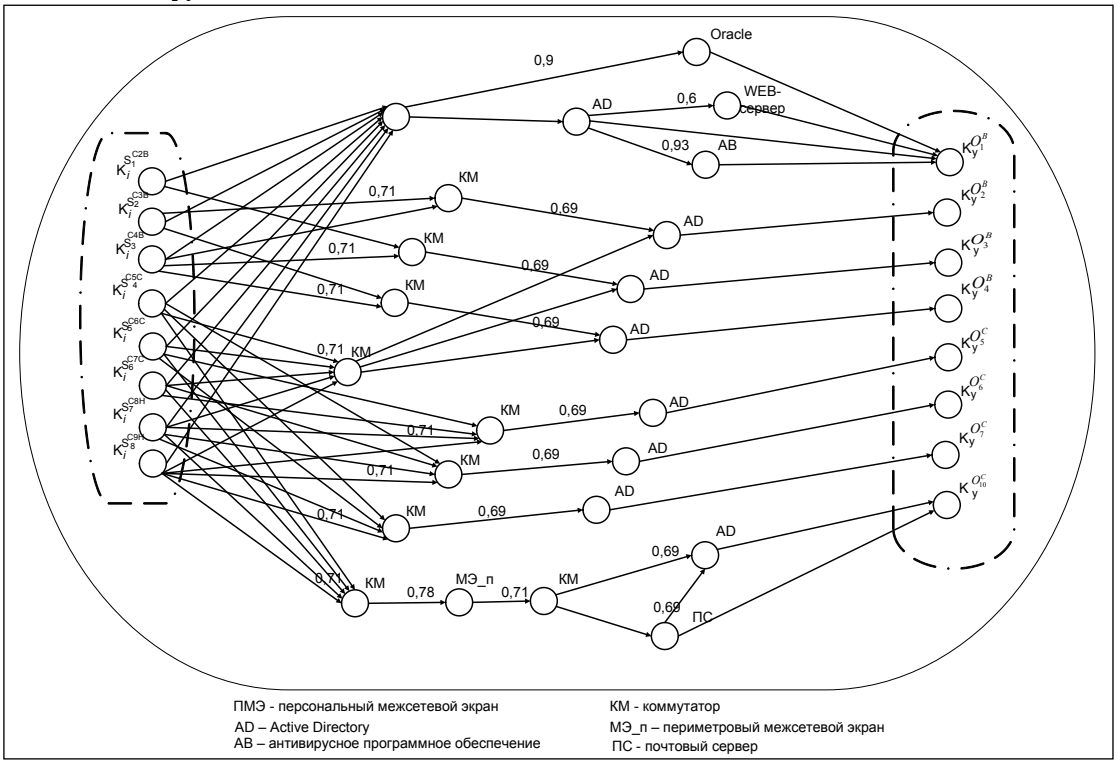

Рис. 5. Нечеткая когнитивная карта – модель угроз, реализуемых внутренними пользователями

Нечеткая когнитивная карта, отображающая процесс реализации угрозы утечки конфиденциальной информации, передаваемой через периметр пользователем-нарушителем с высоким уровнем доступа несанкционированному получателю, приведена на рис. 6.

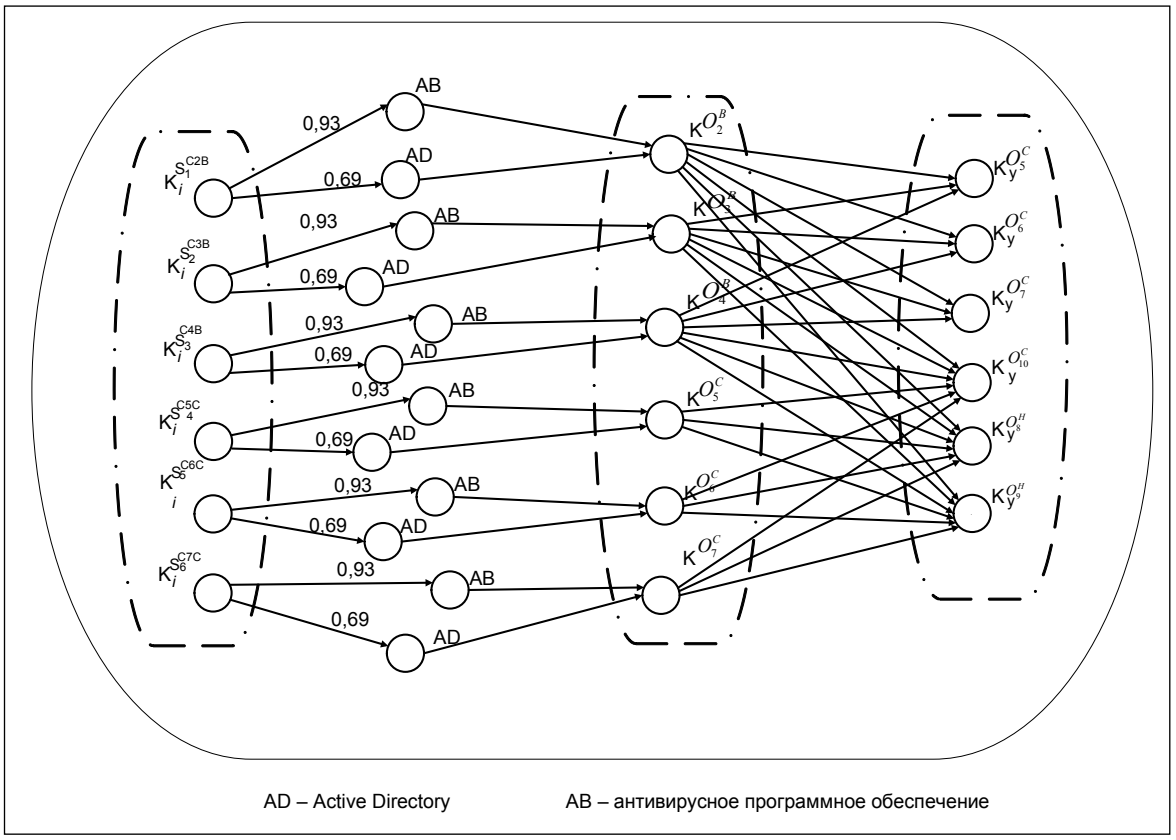

Рис. 6. Нечеткая когнитивная карта – модель угроз утечки конфиденциальной информации

Значения весов влияния в НКК получены на основе нормализации оценок уязвимостей, приведенных в [9].

Значение риска информационной безопасности рассчитывалось для случая, когда все источники угроз активизируются одновременно с равной вероятностью.

Характеристика $\rho_{ООИ}$, учитывающая особенности обработки информации на объекте защиты, – вероятность наличия защищаемой информации в трафике, в рамках данной статьи принимается как частота использования канала связи для передачи конфиденциальной информации.

В расчетах принято, что при передаче информации через периметр $\rho_{ООИ} = \frac{1}{24}$, через границы сегмента $\rho_{ООИ} = \frac{1}{8}$.

В расчетах приняты значения относительных стоимостей информационных ресурсов, обрабатываемых в сегментах сети компании, приведенные в таблице 4.

Таблица 4.

Значения относительных стоимостей информационных ресурсов

Наименование сегмента	Значения относительных стоимостей
Сегменты 8, 9 с категорией конфиденциальности «Н»	0,025
Сегменты 5, 6, 7 с категорией конфиденциальности «С»	0,04

Сегмент 10 внешней экранированной подсети «С»	0,07
Сегменты 2, 3, 4 с категорией конфиденциальности «В»	0,07
Серверный сегмент 1 с уровнем конфиденциальности «В»	0,55

Расчетное значение полного относительного риска $\overline{R}$ в соответствии с формулами (28)–(31) составило 0,120345.

При установке дополнительных СрЗ на путях реализации угроз: персональных межсетевых экранов перед рабочими станциями с уровнями доступа «С» и «В» и серверами, систем предотвращения вторжений Cisco IPS 4270 и программного продукта, предназначенного для защиты данных от утечек, InfoWatch Data Control – значение полного относительного риска уменьшилось более чем в 3 раза и составило $\overline{R}$ = 0,038151.

Вычислительный эксперимент показывает адекватность предложенного метода моделирования угроз для оценки уровня риска информационной безопасности информационных систем с различными наборами средств защиты.

Метод применим на стадии проектирования СЗИ для сравнения различных наборов средств защиты.

Работа выполнена при поддержке гранта НШ-65497.2010.9.

СПИСОК ЛИТЕРАТУРЫ:

1. ГОСТ Р ИСО/МЭК 17799 – 2005. URL: http://sec7x24.net/std/17799-2005.html.
2. *Машкина И. В.* Идентификация угроз на основе построения семантической модели информационной системы // Вестник УГАТУ. Серия «Управление, вычислительная техника и информатика». 2008. Т. 11. № 1 (28). С. 208–214.
3. ГОСТ Р 50.1.053.2005 «Информационные технологии. Основные термины и определения». URL: http://www.gosthelp.ru/text/R5010532005Informacionnye.html.
4. *Бабенко Л. К., Басан А. С., Журкин И. Г, Макаревич О. Б.* Защита данных геоинформационных систем: учеб. пособие для студентов вузов / Под ред. И. Г. Журкина. М.: Гелиос АРВ, 2010. – 336 с.
5. *Васильев В. И.* Интеллектуальные системы защиты информации: учеб. пособие. М.: Машиностроение, 2010. – 152 с.
6. *Борисов В. В., Круглов В. В., Федулов А. С.* Нечеткие модели и сети. М.: Горячая линия – Телеком, 2007. – 283 с.: ил.
7. *Корт С. С.* Теоретические основы защиты информации: Учебное пособие. М.: Гелиос АРВ, 2004. – 240 с.
8. *Брег Р., Родс-Оусли М., Страссберг К.* Безопасность сетей. Полное руководство. Пер. с англ. М.: Эком, 2006. – 912 с.
9. National Vulnerability Database (NVD) Search Common Platform Enumeration. URL: http://web.nvd.nist.gov/view/cpe/search.