УДК 004.056

А.А. Петров[1]

[1]*к.т.н., доцент, ВНУ им. Владимира Даля, Луганск*

ВЫЯВЛЕНИЕ И ИДЕНТИФИКАЦИЯ АТАК НА ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНУЮ СРЕДУ НА ОСНОВЕ МАТЕМАТИЧЕСКОЙ МОДЕЛИ СЕТИ

В статье предложено решение задачи выявления и идентификация атак на информационно-вычислительную среду на основе математической модели сети.
Ключевые слова: математическая модель, компьютерная сеть, атака, информационная безопасность.

Введение

При разработке методов принятия решений необходимо стремиться к наиболее полному и объективному представлению объекта управления − системы защиты информации, описанию её внутренней структуры, объясняющей причинно-следственные законы функционирования и позволяющей управлять процессами защиты информации.

Принятие решения по управлению осуществляется на основе реализации *функции контроля* данных с маршрутизаторов, коммутаторов, межсетевых экранов (МСЭ), систем обнаружения аномалий (СОА), серверов, операционных систем (ОС), приложений. При исследовании аномальной активности эффективным способом выявления атаки является анализ *комбинации поведений* в контролируемом пространстве. Поэтому для сопоставления событий в ИС должна быть проведена формализация этого процесса. Прежде всего необходимо получить *математическое описание структуры сети.*

Под математическим моделированием понимают процесс получения некоторого математического объекта − математической модели, соответствующей данному реальному объекту. Любая математическая модель, как и всякая другая, описывает реальную систему с некоторой степенью приближения.

Одним из решений, рассматриваемых в литературе по безопасности, было предложение представлять и использовать для потока информации *модель,* требующую того, чтобы никакая *высокоуровневая* информация никогда *не протекала* на более *низкий* уровень [2]. Известные модели безопасности [3, 4, 5] используются для решения проблемы построения политик безопасности, а не идентификации атак.

Основная часть

Для представления математических моделей могут использоваться различные формы записи. Инвариантная форма − запись соотношений модели с помощью традиционного математического языка безотносительно к методу решения уравнений модели [6].

Модель информационной системы (ИС), в которой реализуется процесс информационного противоборства, может быть представлена в виде кортежа:

$$S_{ИС} = < \psi_П, \psi_С, P_0(\psi_П \psi_С) >, \quad (1)$$

где $\psi_П$ – подмодель, определяющая поведение системы защиты информации; в ней задаются варианты реагирования на определенные информационные воздействия (угрозы);

ψ_C – подмодель, определяющая структуру системы при её внутреннем рассмотрении;

$P_0(\psi_П \psi_C)$ – предикат целостности, определяющий семантику (смысл) моделей $\psi_П$ и ψ_C, семантику преобразования $\psi_П \to \psi_C$.

Наличие предиката целостности позволяет говорить о том, что модель СЗИ – это семантическая модель, имеющая внутреннюю интерпретацию.

В качестве рабочего определения в литературе [6] под системой в общем случае понимается совокупность элементов и связей между ними, обладающая определенной целостностью. Модель системы – есть изоморфизм А в Ψ, где А – множество фиксированных элементов предметной области с исследуемыми связями между этими элементами, Ψ – абстрактное множество, задаваемое виде кортежа:

$$\psi = < \{M\}, P_1, P_2, ...P_n >, \quad (2)$$

где $\{M\}$ – множество элементов модели, соответствующих элементам предметной области, или носитель модели;

$P_1, P_2, ...P_n$ – предикаты, отображающие наличие того или иного отношения между элементами предметной области. Носитель модели является содержательной областью предикатов $P_1, P_2, ...P_n$.

При таком рассмотрении модель отражает семантику предметной области в отличие от неинтерпретированных математических моделей. Этап моделирования является ключевым моментом при разработке системы управления, использующей методы интеллектуальных технологий.

В *управлении* модели используется для *обоснования решений.* Такие модели должны обеспечивать как описание, так и объяснение и предсказание поведения системы.

Примем, что архитектура безопасности ИС создана в соответствии с рекомендуемыми в ISO/IEC 17799:2000 [7] основными принципами:

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. Объяснением такого разделения всех пользователей на три типа изолированных сегментов является легкость осуществления атаки внутри одного сегмента сети.
2. Выделение в отдельный сегмент всех внутренних серверов компании. Эта мера также позволяет изолировать потоки информации между пользователями, имеющими различные уровни доступа.

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 определенными *отношениями*, отображающими семантику предметной области. Модель объекта представляет собой тот информационный контекст, на фоне которого протекают процессы управления. Чем богаче информационная модель объекта и выше возможности манипулирования ею, тем лучше качество принимаемых решений.

Рассмотрим построение модели информационной инфраструктуры СЗИ на основе теоретико-множественного подхода [1].

Зададим три категории конфиденциальности (критичности, важности) информации: низкая («н»), средняя («с») и высокая («в»). Тогда множество информационных объектов О в сети представляет собой *объединение* множеств:

$$O = O^{H} \cup O^{C} \cup O^{B}, \tag{3}$$

где O^{H} − множество информационных объектов категории «н»,

O^{C} − множество информационных объектов категории «с»,

O^{B} − множество информационных объектов категории «в».

Причем

$$\begin{aligned} O^{H} &= \left\{ o_g^{H} : o_g^{H} \in O^{H} \right\}, g \in [1, G], \\ O^{C} &= \left\{ o_f^{C} : o_f^{C} \in O^{C} \right\}, f \in [1, F], \\ O^{B} &= \left\{ o_d^{B} : o_d^{B} \in O^{B} \right\}, d \in [1, D], \\ O^{H} &\subset O, O^{C} \subset O, O^{B} \subset O. \end{aligned} \tag{4}$$

Зададим множество сегментов сети С:

$$C = C^{H} \cup C^{C} \cup C^{B}, \tag{5}$$

где C^{H}, C^{C}, C^{B} − число сегментов, в которых хранится и обрабатывается информация, соответственно, с низким, средним и высоким уровнем конфиденциальности;

$$C^{H} = \left\{ c_n^{H} : c_n^{H} \in C^{H} \right\}, n \in [1, N] \tag{6}$$

где N − число сегментов, в которых хранится и обрабатывается информация категории «н»;

$$C^{C} = \left\{ o_m^{C} : o_m^{C} \in C^{C} \right\}, m \in [1, M], \tag{7}$$

где M − число сегментов, в которых хранится и обрабатывается информация категории «с»;

$$C^{B} = \left\{ c_l^{B} : c_l^{B} \in c^{B} \right\}, l \in [1, L], \tag{8}$$

где L − число сегментов, в которых хранится и обрабатывается информация категории «в»;

$$C^{H} \subset C, C^{C} \subset C, C^{B} \subset C. \tag{9}$$

На хостах хранится и обрабатывается информация с определенным для сегмента уровнем конфиденциальности. Зададим множество хостов в каждом сегменте через *характеристические предикаты:*

$$\begin{aligned} Y_n^{H} &= \left\{ y_{n_i}^{H} : y_{n_i}^{H} - \text{узел в сегменте } C_n^{H} \right\}, i \in [1, I_n], \\ Y_m^{C} &= \left\{ y_{m_j}^{C} : y_{n_j}^{C} - \text{узел в сегменте } C_m^{C} \right\}, j \in [1, J_m], \\ Y_l^{B} &= \left\{ y_{l_k}^{B} : y_{l_k}^{B} - \text{узел в сегменте } C_l^{B} \right\}, k \in [1, K_l]. \end{aligned} \tag{10}$$

Тогда множество узлов в сегментах описывается с помощью объединения множеств:

$$Y^{H} = Y_1^{H} \cup \ldots Y_n^{H} \cup \ldots Y_N^{N}, \tag{11}$$

где Y^{H} – множество узлов в сегментах с уровнем конфиденциальности информации «н»;

$$Y^{C} = Y_1^{C} \cup \ldots Y_m^{C} \cup \ldots Y_M^{C}, \tag{12}$$

где Y^{C} – множество узлов в сегментах с уровнем конфиденциальности информации «с»;

$$Y^{B} = Y_1^{B} \cup \ldots Y_l^{B} \cup \ldots Y_L^{B}, \tag{13}$$

где Y^{B} – множество узлов в сегментах с уровнем конфиденциальности информации «в».

На различных узлах в сегментах хранятся и обрабатываются различные наборы информационных объектов. Введем *булеаны* $B(O^{н})$, $B(O^{c})$, $B(O^{в})$:

$$B\left(O^{H}\right) = \left\{H^{H} : H^{H} \subseteq O^{H}\right\}, \tag{14}$$

где H^{H} – подмножество наборов информационных объектов категории «н»,

$$H^{H} = \left\{н_1^{н}, \ldots н_g^{н}, \ldots н_{G_1}^{н}\right\}, G_1 = 2^{G};$$

$$B\left(O^{C}\right) = \left\{H^{C} : H^{C} \subseteq O^{C}\right\}, \tag{15}$$

где H^{C} – подмножества наборов информационных объектов категории «с»,

$$H^{c} = \left\{н_1^{c}, \ldots н_f^{c}, \ldots н_{F_1}^{c}\right\}, F_1 = 2^{F};$$

$$B\left(O^{B}\right) = \left\{H^{B} : H^{B} \subseteq O^{B}\right\}, \tag{16}$$

где H^{B} – подмножество наборов информационных объектов категории «в»,

$$H^{B} = \left\{н_1^{B}, \ldots н_d^{B}, \ldots н_{D_1}^{B}\right\}, D_1 = 2^{D}. \tag{17}$$

Каждому узлу в сегменте соответствует определенный набор информационных объектов, причем могут быть одинаковые наборы на узлах в сегментах одной и той же категории.

Зададим *соответствия* множеств

$$\begin{aligned} \rho &\subseteq B\left(H^{H}\right) \times Y_n^{H}, \\ \tau &\subseteq B\left(H^{H}\right) \times Y_m^{C}, \\ \lambda &\subseteq B\left(H^{B}\right) \times Y_l^{B}. \end{aligned} \tag{18}$$

Соответствие – есть некоторое подмножество декартова произведения:

$$\begin{aligned} H^{H} \times Y_n^{H} &= \left\{\left(н_g^{H}, y_{n_i}^{H}\right) : н_g^{H} \in H^{H} \wedge y_{n_i}^{H} \in Y_n^{H}\right\}, \\ H^{C} \times Y_m^{C} &= \left\{\left(н_f^{C}, y_{m_j}^{C}\right) : н_f^{C} \in H^{C} \wedge y_{m_j}^{C} \in Y_m^{C}\right\}, \\ H^{B} \times Y_l^{B} &= \left\{\left(н_d^{B}, y_{l_k}^{B}\right) : н_d^{B} \in H^{B} \wedge y_{l_k}^{B} \in Y_l^{B}\right\}. \end{aligned} \tag{19}$$

причем *сечения соответствий* $\rho\left(H_g^H\right),\tau\left(H_f^C\right),\lambda\left(H_d^B\right)$, определяют узлы, в которых обрабатываются одинаковые наборы информационных объектов. С помощью соответствия можно задать упорядочение пары (набор информационных объектов, узел в сегменте).

Тогда множество информационных объектов в сегментах определяется с помощью операции объединения множеств:

$$O_n^н = \bigcup_{i=1}^{I_n} H_g^н\left(y_{n_i}^н\right),$$
$$O_m^c = \bigcup_{m=1}^{J_m} H_g^c\left(y_{m_j}^c\right),$$
$$O_l^в = \bigcup_{k=1}^{K_l} H_d^в\left(y_{l_k}^в\right). \tag{20}$$

Обозначим множество субъектов доступа через S. Субъекты доступа − это пользователи или процессы:

$$S = S^{вн} \cup S^{внш}, \tag{21}$$

где $S^{вн}$ − внутренние субъекты доступа;

$S^{внш}$ − внешние субъекты доступа.

Множество внутренних субъектов доступа − есть *объединение* множеств

$$S^{вн} = S^н \cup S^c \cup S^в, \tag{22}$$

где $S^н$ − множество пользователей или процессов с уровнем доступа «н»;

S^c − множество пользователей или процессов с уровнем доступа «с»;

$S^в$ − множество пользователей или процессов с уровнем доступа «в»;

Множества задаются через *характеристические предикаты:*

$$\begin{aligned}
&S^н = \bigcup_{n=1}^{N} S_n^н;\\
&S_n^н = \left\{ s_{n_i}^н : s_{n_i}^н - \quad \textit{субъект доступа в n-ом сегменте} \right\},\\
&S^c = \bigcup_{m=1}^{M} S_m^c;\\
&S_m^c = \left\{ s_{m_j}^c : s_{m_j}^c - \quad \textit{субъект доступа m-ом сегменте} \right\},\\
&S^в = \bigcup_{l=1}^{L} S_l^в;\\
&S_l^в = \left\{ s_{l_k}^в : s_{l_k}^в - \quad \textit{субъект доступа l-ом сегменте} \right\}.
\end{aligned} \tag{23}$$

Зададим *отображения* множества узлов в сегментах в множество субъектов доступа:

$$Y_n^н \to S_n^н,$$
$$Y_m^с \to S_m^с,$$
$$Y_l^в \to S_l^в. \quad (24)$$

Множество внешних субъектов доступа — есть объединение множеств

$$S^{внш} = S_r^{п\ внш} \cup S_r^{внш}, r \in [1, R], \quad (25)$$

где $S_r^{п\ внш}$ − внешние пользователи, обладающие правами доступа;

$S_r^{внш}$ − несанкционированный субъект доступа;

R − число точек доступа через периметр.

Множество субъектов доступа, внешних или внутренних, можно рассматривать как *источники угроз,* под которыми понимается атакующая программа или оператор, непосредственно осуществляющий воздействие на вычислительную сеть.

По расположению субъекта доступа относительно атакуемого объекта угрозы подразделяются на внешние и внутренние (внутрисегментные и межсегментные).

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

- злоумышленником с целью проникновения с удаленной машины 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.

Внутренние угрозы связаны с нарушением принятой политики безопасности: нелегальным поведением пользователя на компьютере или сервере, попытками доступа пользователя к информационным ресурсам, уровень конфиденциальности которых превышает его уровень доступа (попытки сетевых соединений, запуска приложений и другое). Любой несанкционированный доступ является реализацией преднамеренной угрозы ИБ и называется *атакой.*

В работе рассматриваются удаленные внешние и внутренние межсегментные атаки, которые представляют гораздо большую опасность, чем внутрисегментные.

Таким образом для описания угрозы как канала несанкционированного доступа, утечки, деструктивных воздействий, необходимо указать субъект доступа, информационный объект, к которому осуществляется несанкционированный доступ, путь распространения угрозы, информационный носитель. Тогда угроза может быть описана кортежем

$$U = \langle S, A, З_с, З_х, П, O(C) \rangle, \quad (26)$$

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

A − оборудование в канале связи (коммутаторы, маршрутизаторы и другое);

$З_С$,$З_Х$ − сервисы безопасности на пути распространения угрозы, соответственно, сетевые и хостовые (МСЭ, СОА, журналы регистрации аномальных сетевых соединений, журналы регистрации операционных систем и другие);

П − протоколы и пакеты;

O − объект доступа (в каком сегменте).

В настоящее время подавляющее число угроз информационной безопасности принципиально могут быть реализованы только в процессе функционирования ИС [76],

при этом логическое вторжение является наиболее результативным для злоумышленника. В рамках логического вторжения обычно выделяют внутрисистемное и удаленное. При внутрисистемном вторжении предполагается, что нарушитель уже имеет учетную запись в системе как пользователь с невысокими привилегиями и совершает атаку на систему для получения дополнительных привилегий. Удаленное вторжение заключается в попытке проникновения в систему (например, через сеть Интернет) с удаленной машины. Это атаки, выполняемые при постоянном участии человека и атаки, выполняемые специальными программами: атаки на информацию, хранящуюся на внешних запоминающих устройствах, атаки на информацию, передаваемую по линиям связи, атаки на информацию, обрабатываемую в памяти компьютера.

Основная цель практически любой атаки − получение несанкционированного доступа к информации: перехват и искажение. Возможность искажения информации означает либо полный контроль над информационными потоками, либо возможность передачи сообщений от имени другого объекта.

Множество угроз включает в себя подмножества внешних и внутренних угроз:

$$U = U^{вн} \cup U^{внш} \tag{27}$$

В свою очередь подмножество внутренних угроз включает в себя подмножества $U^{вн}_{l(m)}$ и $U^{вн}_{l\ m(n)}$

$$U^{вн}_{l(m)} = \left\langle S^{с}, A, З_{с}, З_{х}, П, O^{в}\left(C^{в}\right)\right\rangle, \tag{28}$$

где $U^{вн}_{l(m)}$ − угроза информационным объектам категории «в» в случае, когда нарушитель имеет учетную запись в системе как пользователь с правами доступа к информации с уровнем конфиденциальности «с», обрабатываемой в сегментах $C^{с}_{m}$, и пытается превысить свои привилегии,

$$U^{вн}_{l\ m(n)} = \left\langle S^{н}, A, З_{с}, З_{х}, П, O^{в}\left(C^{в}\right) \cup O^{с}\left(C^{с}\right)\right\rangle, \tag{29}$$

где $U^{вн}_{l\ m(n)}$ − информационным объектом категории «в» и «с» в случае, когда нарушитель имеет учетную запись в системе как пользователь с правами доступа к информации с уровнем конфиденциальности «н», обрабатываемой в сегментах $C^{с}_{n}$, и пытается превысить свои привилегии.

Внешняя угроза связана с внешним субъектом доступа и описывается кортежем

$$U^{внш} = \left\langle S^{внш}, A, З_{с}, З_{х}, П, O(C)\right\rangle. \tag{30}$$

Таким образом, источниками внутренних угроз являются субъекты и процессы, описываемые множествами S^{H}, S^{C}, источниками внешних угроз − субъекты и процессы, описываемые множеством $S^{внш}$.

На информационные объекты множества O^{B}_{l} в сегментах C^{B}_{l} воздействует множество угроз U_{l}

$$U_l = U^{вн}_{l(m)} \cup U^{вн}_{l(n)} \cup U^{внш}. \quad (31)$$

На информационные объекты множества $O^{с}_{m}$ в сегментах $C^{с}_{m}$ воздействует множество угроз

$$U_m = U^{вн}_{m(n)} \cup U^{внш}. \quad (32)$$

На информационные объекты множества $O^{н}_{n}$ воздействует множество внешних угроз

$$U_n = U^{внш}. \quad (33)$$

Построим далее композиции соответствий

$$\begin{aligned} &\sigma \subseteq U_l \times C^{в} \text{ и } \xi \subseteq C^{в} \times Y^{в}_{l}, \\ &\nu \subseteq U_m \times C^{с} \text{ и } \pi \subseteq C^{с} \times Y^{с}_{m}, \\ &\varphi \subseteq U_n \times C^{н} \text{ и } \mu \subseteq C^{н} \times Y^{н}_{n}. \end{aligned} \quad (34)$$

Получим упорядоченные множества, элементами которых являются пары (угроза, узел) в соответствующих сегментах:

$$\begin{aligned} &\sigma \circ \xi = \left\{ (u_{l_q}, y^{в}_{l_k}) : (\exists c^{в}_{l} \in C^{в})((u_{l_q} c^{в}_{l}) \in \sigma) \wedge ((c^{в}_{l}, y^{в}_{l_k}) \in \xi) \right\}, \\ &q \in [1, Q^{в}], \\ &\nu \circ \pi = \left\{ (u_{m_q}, y^{с}_{m_j}) : (\exists c^{с}_{m} \in C^{с})((u_{m_q} c^{с}_{m}) \in \nu) \wedge ((c^{с}_{m}, y^{с}_{m_j}) \in \pi) \right\}, \\ &q \in [1, Q^{с}], \\ &\varphi \circ \mu = \left\{ (u_{n_q}, y^{н}_{n_i}) : (\exists c^{н}_{n} \in C^{н})((u_{n_q} c^{н}_{n}) \in \nu) \wedge ((c^{н}_{n}, y^{н}_{n_i}) \in \mu) \right\}, \\ &q \in [1, Q^{н}] \end{aligned} \quad (35)$$

где $Q^{в}, Q^{с}, Q^{н}$ – число путей распространения атак к узлам в сегментах, в которых хранится и обрабатывается информация с уровнем конфиденциальности, соответственно, «в», «с», «н».

Число путей равно:

$$\begin{aligned} Q^{в} &= N + M + R, \\ Q^{с} &= N + R, \\ Q^{н} &= R. \end{aligned} \quad (36)$$

Обнаружение пассивных атак затруднено из-за отсутствия непосредственного влияния на работу системы. Активное воздействие нарушает принятую в ней политику безопасности; в результате осуществления такой атаки в системе происходят определенные изменения, которые могут быть зарегистрированы.

Источниками информации о состоянии информационной среды являются маршрутизаторы и коммутаторы, другое сетевое оборудование, межсетевые экраны, сетевые и хостовые системы обнаружения аномалий, VPN устройства, журналы регистрации операционных систем, аномальных сетевых соединений, приложений и другие. События, зафиксированные различными источниками, необходимо сопоставить с возмож-

ными путями распространения атаки.

Введем множество функциональных индикаторов И – значений контролируемых параметров, с помощью которых фиксируются отдельные события информационной безопасности. Функциональные индикаторы отражают результаты *контроля:*

- изменений правил МСЭ;
- соответствия настроек других сервисов безопасности политике безопасности;
- изменений привилегий пользователей;
- системных вызовов;
- попыток доступа;
- состояния соединений;
- обращений ОС.

Поскольку единственным эффективным способом идентифицировать атаку является анализ комбинаций поведений, в работе предлагается сопоставить множеству возможных путей распространения атаки множество индикаторов. Очевидно, тогда, что *вероятность* того, что подозрительная активность, является атакой может быть оценена числом индикаторов на пути распространения атаки. Для идентификации внутренних атак предлагается использовать два типа индикаторов: системные и сетевые (хостовые), для идентификации внешних вторжений дополнительно использовать индикаторы, отображающие аномальные события на периметре сети.

Зададим множество путей распространения атак с помощью характеристического предиката:

$$P = \{p_i : p_i - \text{путь распределения атаки}\}, i \in [1, \mathrm{I_p}],$$
$$\mathrm{I_p} = \mathrm{Q^в} + \mathrm{Q^с} + \mathrm{Q^н}. \tag{37}$$

Множество индикаторов включает в себя:

$$\mathrm{И} = \mathrm{И}^{\mathrm{с}}_{(\mathrm{n})} \cup \mathrm{И}^{\mathrm{в}}_{(\mathrm{n})} \cup \mathrm{И}^{\mathrm{в}}_{(\mathrm{m})} \cup \mathrm{И}_{\mathrm{пер}}, \tag{38}$$

где $\mathrm{И}^{\mathrm{с}}_{(\mathrm{n})}$ − подмножество индикаторов, фиксирующих попытку доступа субъекта с уровнем ограничения доступа «н» к объекту с уровнем конфиденциальности «с»;

$\mathrm{И}^{\mathrm{в}}_{(\mathrm{n})}$ − подмножество индикаторов, фиксирующих попытку доступа субъекта с уровнем ограничения доступа «н» к объекту с уровнем конфиденциальности «в»;

$\mathrm{И}^{\mathrm{в}}_{(\mathrm{m})}$ − подмножество индикаторов, фиксирующих попытку доступа субъекта с уровнем ограничения доступа «с» к объекту с уровнем конфиденциальности «в»;

$\mathrm{И}_{\mathrm{пер}}$ − подмножество индикаторов, фиксирующих попытки проникновения на периметре.

Множество И можно описать с помощью характеристического предиката

$$\mathrm{И} = \{\mathrm{и_j} : \mathrm{и_j} - \text{индикатор сетевой, хостов или периметровый}\},$$
$$\mathrm{j} \in [1, \mathrm{J_н}]. \tag{39}$$

Зададим соответствие множества путей атак множеству индикаторов

$$\tau_a \subseteq \text{Р} \times \text{И} = \{(p_i, и_j) : p_i \in \text{Р} \wedge и_j \in \text{И}\}. \quad (40)$$

Тогда *сечение соответствия* по $\tau_a(p_i)$ определяет набор индикаторов, соответствующий реализации угрозы на данном пути.

$$\tau_a(p_i) = \{(и_{p_i} : и_{p_i} \text{ - индикатор одного события ИБ на пути атаки})\} \quad (41)$$

Выводы

В условиях информационного противоборства для принятия решения о варианте реагирования на изменение среды функционирования, то есть для формирования командной информации для реализации управления в реальном времени, необходим регулярный контроль и оперативный анализ данных о подозрительной активности, которую можно идентифицировать как атаку, и *численная оценка вероятности* того, что эта активность является атакой.

Литература

1. *Куликов, В. В.* Дискретная математика: учеб. пособие / В. В. Куликов. - М.: РИОР, 2007. - 174 с.
2. *Корт, С. С.* Теоретические основы защиты информации: учеб. пособие. М.: Гелиос АРВ, 2004. - 240 с.
3. *Bella Padula, L., Bell, D.* Secure Computer System: Mathematical Foundation, ESD-TR-73-278, V. I, MITRE Corporation.
4. *Bella Padula, L., Bell, D.* Secure Computer Systems: A Mathematical Model, ESD-TR-73-278, V. II, MITRE Corporation.
5. *John, McLean.* A comment of the «Basic Security Teorem» of the Bell and La Padula, Information Processing Letters. 1985.
6. *Анфилатов, В.* С. Системный анализ в управлении: учеб. пособие / В.С Анфилатов, А. А. Емельянов, А. А. Кукушкин; под ред. А.А. Емельянова. - М.: Финансы и статистика, 2006. — 368 с.
7. ISO/IEC 17799:2000. Information technology – Code of practice for information security management.

Надійшла до редколегії 23.06.2013 р.

Рецензент: д.т.н., проф. Хорошко В.О.

Petrov A.A.

DETECTION AND IDENTIFICATION OF ATTACKS ON INFORMATION AND COMPUTING ENVIRONMENT BASED ON A MATHEMATICAL MODEL OF THE NETWORK

This article provides a solution to the problem of identifying and identification of attacks on information and computing environment based on a mathematical model of the network.

Keyword: mathematical model, computer network, attack, information security.

Петров А.О.

ВИЯВЛЕННЯ ТА ІДЕНТИФІКАЦІЯ АТАК НА ІНФОРМАЦІЙНО-ОБЧИСЛЮВАЛЬНУ СЕРЕДУ НА ОСНОВІ МАТЕМАТИЧНОЇ МОДЕЛІ МЕРЕЖІ

У статті запропоновано вирішення завдання виявлення та ідентифікація атак на інформаційно-обчислювальну середу на основі математичної моделі мережі.

Ключові слова: математична модель, комп'ютерна мережа, атака, інформаційна безпека.