Уфа : УГАТУ, 2008 Вестник УГАТУ • Управление, ВТ и И Т. 11, № 1 (28). С. 208–214

УДК 004.7

И. В. МАШКИНА

ИДЕНТИФИКАЦИЯ УГРОЗ НА ОСНОВЕ ПОСТРОЕНИЯ СЕМАНТИЧЕСКОЙ МОДЕЛИ ИНФОРМАЦИОННОЙ СИСТЕМЫ

На основе теоретико-множественного подхода предложено формализованное описание информационной системы, созданной в соответствии с рекомендуемыми в ГОСТ основными принципами архитектуры безопасности. Предложено описание угрозы в виде кортежа, приводится оценка числа путей распространения угроз, анализируется возможность идентификации атаки по индикаторам аномальных событий на пути распространения. *Информационная безопасность*; *информационная система*; *семантическая модель*

Усложнение современных информационных систем (ИС) ведет к появлению в них все большего количества сетевых устройств и разнородных средств защиты информации, генерирующих огромное число событий безопасности, разобраться в которых, сопоставить сигналы о событиях безопасности от разных систем администратору безопасности практически невозможно; в то же время ответные действия на атаки должны быть предприняты немедленно.

Поэтому перед подразделениями, обеспечивающими информационную безопасность (ИБ) организации, ставится задача эффективного управления защитой информации (ЗИ) во все более усложняющейся сетевой среде. Требуются динамические методы, позволяющие оперативно контролировать изменение условий среды функционирования и предотвращать нарушения ИБ, управляя сетевым оборудованием и средствами защиты.

При разработке методов принятия решений по управлению защитой информации необходимо стремиться к наиболее полному и объективному представлению объекта управления — системы защиты информации (СЗИ), описанию ее 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, МСЭ, СОА, серверов, 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, для чего необходимо получить математическое описание структуры сети.

В управлении модели используются для обоснования решений. Такие модели должны обеспечивать как описание, так и объяснение поведения системы в условиях неопределенности воздействия угроз.

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. Известные модели безопасности [1, 2, 3] используются для решения проблемы построения политик безопасности, а не для описания потенциально возможных угроз безопасности информации.

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 [4].

Для представления математических моделей могут использоваться различные формы записи. Инвариантная форма — запись соотношений модели с помощью традиционно-

Контактная информация: (347)273-06-72

го математического языка безотносительно к методу решения уравнений модели [5].

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 в виде кортежа [5]:

$$\Psi =< \{M\}, P_1, P_2, \dots P_n > ,$$

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

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

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.

1. ПОСТАНОВКА ЗАДАЧИ

Примем, что архитектура безопасности ИС создана в соответствии с рекомендуемыми в [6] основными принципами:

• 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 в соответствии с типами изолированных сегментов является легкость осуществления атаки внутри одного сегмента сети.

• 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. В работе ставится задача построения модели информационной инфраструктуры СЗИ на основе теоретико-множественного подхода [7]. Основой построения модели является описание объектов в виде совокупности элементов, связанных между собой определенными отношениями, отображающими семантику предметной области.

Для сети, состоящей из R сегментов, в которых обрабатывается информация с различными уровнями конфиденциальности (критичности):

• описать множество преднамеренных угроз U, внешних $U^{\text{внш}}$ и внутренних $U^{\text{вн}}$,

$$U = U^{\text{вн}} \cup U^{\text{внш}};$$

• выявить возможные источники угроз и объекты атак;

• оценить число потенциально возможных путей распространения атак;

• предложить способ идентификации атаки на основе анализа событий безопасности на пути ее распространения.

2. ФОРМАЛИЗОВАННОЕ ОПИСАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ НА ОСНОВЕ ТЕОРЕТИКО-МНОЖЕСТВЕННОГО ПОДХОДА

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:

$$O = O^{\text{н}} \cup O^{\text{с}} \cup O^{\text{в}},$$

где $O^{\text{н}}$ — множество информационных объектов категории «н»,

$O^{\text{с}}$ — множество информационных объектов категории «с»,

$O^{\text{в}}$ — множество информационных объектов категории «в».

Причем

$$O^{\text{н}} = \left\{o_g^{\text{н}} : o_g^{\text{н}} \in O^{\text{н}}\right\},\ g \in [1, G],$$
$$O^{c} = \left\{o_f^{c} : o_f^{c} \in O^{c}\right\},\ f \in [1, F],$$
$$O^{\text{в}} = \left\{o_d^{\text{в}} : o_d^{\text{в}} \in O^{\text{в}}\right\},\ d \in [1, D],$$
$$O^{\text{н}} \subset O, \quad O^{\text{с}} \subset O, \quad O^{\text{в}} \subset O.$$

Зададим множество C сегментов сети:

$$C = C^{\text{н}} \cup C^{c} \cup C^{\text{в}},$$

где $C^{\text{н}}$, $C^{\text{с}}$, $C^{\text{в}}$ — подмножества сегментов, в которых хранится и обрабатывается информация, соответственно, с низким, средним и высоким уровнем конфиденциальности;

$$C^{\text{н}} = \left\{c_n^{\text{н}} : c_n^{\text{н}} \in C^{\text{н}}\right\},\ n \in [1, N],$$

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

$$C^{\text{с}} = \{c_m^{\text{с}} : c_m^c \in C^c\}\ ,\ m \in [1, M]\ ,$$

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

$$C^{\text{в}} = \{\text{с}_l^{\text{в}} : c_l^{\text{в}} \in \text{С}^{\text{в}}\}\ ,\ l \in [1, L]\ ,$$

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

$$C^{\text{н}} \subset C\,,\quad C^{\text{с}} \subset C\,,\quad C^{\text{в}} \subset C\,.$$

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

$$Y_n^{\text{н}} = \left\{y_{n_i}^{\text{н}} : y_{n_i}^{\text{н}} - \text{узел в сегменте } C_n^{\text{н}}\right\}\ ,$$
$$i \in [1, I_n]\ ;$$
$$Y_m^{\text{с}} = \left\{y_{m_j}^c : y_{m_j}^c - \text{узел в сегменте } C_m^c\right\}\ ,$$
$$j \in [1, J_m]\ ;$$
$$Y_l^{\text{в}} = \left\{y_{l_k}^{\text{в}} : y_{l_k}^{\text{в}} - \text{узел в сегменте} C_l^{\text{в}}\right\}\ ,$$
$$k \in [1, K_l]\ .$$

Тогда множество узлов в сегментах описывается с помощью объединения множеств:

$$Y^{\text{н}} = Y_1^{\text{н}} \cup \ldots Y_n^{\text{н}} \cup \ldots Y_N^{\text{н}}\,,$$

где $Y^{\text{н}}$ — множество узлов в сегментах с уровнем конфиденциальности информации «н»;

$$Y^{\text{с}} = Y_1^{\text{с}} \cup \ldots Y_m^c \cup \ldots Y_M^c\,,$$

где $Y^{\text{с}}$ — множество узлов в сегментах с уровнем конфиденциальности информации «с»;

$$Y^{\text{в}} = Y_1^{\text{в}} \cup \ldots Y_l^{\text{в}} \cup \ldots Y_L^{\text{в}}\,,$$

где $Y^{\text{в}}$ — множество узлов в сегментах с уровнем конфиденциальности информации «в».

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

$$B(O^{\text{н}}) = \{\text{Н}^{\text{н}} : \text{Н}^{\text{н}} \subseteq O^{\text{н}}\}\ ,$$

где $H^{\text{н}}$ — подмножество наборов информационных объектов категории «н»,

$$\text{Н}^{\text{н}} = \left\{\text{н}_1^{\text{н}}, \ldots \text{н}_g^{\text{н}}, \ldots \text{н}_{G_1}^{\text{н}}\right\}\ ,\ G_1 = 2^G\,;$$

$$B(O^c) = \{\text{Н}^{\text{с}} : \text{Н}^{\text{с}} \subseteq O^{\text{с}}\}\ ,$$

где $\text{Н}^{\text{с}}$ — подмножество наборов информационных объектов категории «с»,

$$\text{Н}^{\text{с}} = \left\{\text{н}_1^{\text{с}}, \ldots \text{н}_f^c, \ldots \text{н}_{F_1}^c\right\}\ ,\quad F_1 = 2^F\,;$$
$$B(O^{\text{в}}) = \{\text{Н}^{\text{в}} : H^{\text{в}} \subseteq O^{\text{в}}\}\ ,$$

где $\text{Н}^{\text{в}}$ — подмножество наборов информационных объектов категории «в»,

$$\text{Н}^{\text{в}} = \left\{\text{н}_1^{\text{в}}, \ldots \text{н}_d^{\text{в}}, \ldots \text{н}_{D_1}^{\text{в}}\right\}\ ,\ D_1 = 2^D\,.$$

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

$$\rho \subseteq B(\text{Н}^{\text{н}}) \times Y_n^{\text{н}}\,,$$
$$\tau \subseteq B(\text{Н}^{\text{н}}) \times Y_m^c\,,$$
$$\lambda \subseteq B(\text{Н}^{\text{в}}) \times Y_l^{\text{в}}\,.$$

Соответствие — есть некоторое подмножество декартова произведения:

$$\text{Н}^{\text{н}} \times Y_n^{\text{н}} = \left\{(\text{н}_g^{\text{н}}, y_{n_i}^{\text{н}}) : \text{н}_g^{\text{н}} \in \text{Н}^{\text{н}} \wedge y_{n_i}^{\text{н}} \in Y_n^{\text{н}}\right\}\ ,$$
$$\text{Н}^{\text{с}} \times Y_m^{\text{с}} = \left\{(\text{н}_f^{\text{с}}, y_{m_j}^{\text{с}}) : \text{н}_f^{\text{с}} \in \text{Н}^{\text{с}} \wedge y_{m_j}^{\text{с}} \in Y_m^{\text{с}}\right\}\ ,$$
$$\text{Н}^{\text{в}} \times Y_l^{\text{в}} = \left\{(\text{н}_d^{\text{в}}, y_{l_k}^{\text{в}}) : \text{н}_d^{\text{в}} \in \text{Н}^{\text{в}} \wedge y_{l_k}^{\text{в}} \in Y_l^{\text{в}}\right\}\ ,$$

причем *сечения соответствий* $\rho(\text{н}_g^{\text{н}})$, $\tau(\text{н}_f^c)$, $\lambda(\text{н}_d^{\text{в}})$ 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:

$$O_n^{\text{н}} = \bigcup_{i=1}^{I_n} \text{н}_g^{\text{н}}(y_{n_i}^{\text{н}})\,,$$
$$O_m^c = \bigcup_{m=1}^{J_m} \text{н}_f^c(y_{m_j}^{\text{с}})\,,$$
$$O_l^{\text{в}} = \bigcup_{k=1}^{K_l} \text{н}_d^{\text{в}}(y_{l_k}^{\text{в}})\,.$$

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

$$S = S^{\text{вн}} \cup S^{\text{внш}}\,,$$

где $S^{\text{вн}}$ — внутренние субъекты доступа,

$S^{\text{внш}}$ — внешние субъекты доступа.

Множество внутренних субъектов доступа есть объединение множеств

$$S^{\text{вн}} = S^{\text{н}} \cup S^{\text{с}} \cup S^{\text{в}} ,$$

где $S^{\text{н}}$ — множество пользователей или процессов с уровнем доступа «н»,

$S^{\text{с}}$ — множество пользователей или процессов с уровнем доступа «с»,

$S^{\text{в}}$ — множество пользователей или процессов с уровнем доступа «в».

Множества задаются через характеристические предикаты:

$$S^{\text{н}} = \bigcup_{n=1}^{N} S_n^{\text{н}} ;$$
$$S_n^{\text{н}} = \left\{ s_{n_i}^{\text{н}} : s_{n_i}^{\text{н}} \right\} ,$$
$$S^{\text{с}} = \bigcup_{m=1}^{M} S_m^{c} ;$$
$$S_m^{c} = \left\{ s_{m_j}^{\text{с}} : s_{m_j}^{\text{с}} \right\} ,$$
$$S^{\text{в}} = \bigcup_{l=1}^{L} S_l^{\text{в}} ;$$
$$S_l^{\text{в}} = \left\{ s_{l_k}^{\text{в}} : s_{l_k}^{\text{в}} \right\} ,$$

где $s_{n_i}^{\text{н}}$ — субъект доступа в n-м сегменте, $s_{m_j}^{\text{с}}$ — субъект доступа в m-м сегменте, $s_{l_k}^{\text{в}}$ — субъект доступа в l-м сегменте.

Зададим отображения множества узлов в сегментах в множество субъектов доступа:

$$Y_n^{\text{н}} \to S_n^{\text{н}} ,$$
$$Y_m^{\text{с}} \to S_m^{\text{с}} ,$$
$$Y_l^{\text{в}} \to S_l^{\text{в}} .$$

Множество внешних субъектов доступа есть объединение множеств

$$S^{\text{внш}} = S_r^{\text{п внш}} \cup S_r^{\text{внш}} , \; r \in [1, R] ,$$

где $S^{\text{п внш}}$ — внешние пользователи, обладающие правами доступа,

$S^{\text{внш}}$ — 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).

3. ОПИСАНИЕ УГРОЗ КАК КАНАЛОВ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА, УТЕЧКИ, ДЕСТРУКТИВНЫХ ВОЗДЕЙСТВИЙ, И ОПРЕДЕЛЕНИЕ ПУТЕЙ УГРОЗ

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

$$U = \langle S, A, З_{\text{с}}, З_{\text{х}}, \Pi, \text{О(С)} \rangle ,$$

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

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

$З_{\text{с}}$, $З_{\text{х}}$ — сервисы безопасности на пути распространения угрозы, соответственно се-

тевые и хостовые (МСЭ, СОА, журналы регистрации аномальных сетевых соединений, журналы регистрации операционных систем и другие);

П — протоколы и пакеты;

О — объект доступа (в каком сегменте).

В настоящее время подавляющее число угроз информационной безопасности принципиально может быть реализовано только в процессе функционирования ИС [8], 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:

$$U = U^{\text{вн}} \cup U^{\text{внш}}.$$

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

$$U^{\text{вн}}_{l(m)} = \langle S^c, A, З_с, З_х, П, О^{\text{в}}(C^{\text{в}})\rangle,$$

где $U^{\text{вн}}_{l(m)}$ — 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 $С^{\text{с}}_m$, и пытается превысить свои привилегии,

$$U^{\text{вн}}_{lm(n)} = \langle S^{\text{н}}, А, З_с, З_х, П, О^{\text{в}}(C^{\text{в}}) \cup O^{\text{с}}(C^{\text{с}})\rangle,$$

$U^{\text{вн}}_{lm(n)}$ — угроза информационным объектам 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 $С^{\text{н}}_n$, и пытается превысить свои привилегии.

Внешняя угроза связана с внешним субъектом доступа и описывается кортежем

$$U^{\text{внш}} = \langle S^{\text{внш}}, А, З_с, З_х, Н, О(C)\rangle.$$

Таким образом, источниками внутренних угроз являются субъекты и процессы, описываемые множествами $S^{\text{н}}$, $S^{\text{с}}$, источниками внешних угроз — субъекты и процессы, описываемые множеством $S^{\text{внш}}$.

На информационные объекты множества $O^{\text{в}}_l$ в сегментах $С^{\text{в}}_l$ воздействует множество угроз U_l:

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

На информационные объекты множества $O^{\text{с}}_m$ в сегментах $C^{\text{с}}_m$ воздействует множество угроз

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

На информационные объекты множества $O^{\text{н}}_n$ воздействует множество внешних угроз

$$U_n = U^{\text{внш}}.$$

Построим далее композиции соответствий:

$$\sigma \subseteq U_l \times С^{\text{в}} \text{ и } \xi \subseteq С^{\text{в}} \times Y^{\text{в}}_l,$$
$$\nu \subseteq U_m \times C^c \text{ и } \pi \subseteq C^c \times Y^c_m,$$
$$\varphi \subseteq U^{\times}_n С^{\text{н}} \text{ и } \mu \subseteq С^{\text{н}} \times Y^{\text{н}}_n.$$

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

$$\sigma \circ \xi = \left\{(u_{l_q}, y^{\text{в}}_{l_k}) : (\exists c^{\text{в}}_l \in С^{\text{в}})((u_{l_q} c^{\text{в}}_l) \in \sigma) \wedge ((c^{\text{в}}_l, y^{\text{в}}_{l_k}) \in \xi)\right\},$$
$$q \in [1, Q^{\text{в}}],$$
$$\nu \circ \pi = \left\{(u_{m_q}, y^c_{m_j}) : (\exists c^{\text{с}}_m \in С^c)((u_{m_q} c^{\text{с}}_m) \in \nu) \wedge ((c^{\text{с}}_m, y^{\text{с}}_{m_j}) \in \pi)\right\};$$
$$q \in [1, Q^{\text{с}}],$$
$$\varphi \circ \mu = \left\{(u_{n_q}, y^{\text{н}}_{n_i}) : (\exists c^{\text{н}}_n \in С^{\text{н}})((u_{n_q} c^{\text{н}}_n) \in \varphi) \wedge ((c^{\text{н}}_n, y^{\text{н}}_{n_i}) \in \mu)\right\};$$
$$q \in [1, Q^{\text{н}}],$$

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

Число путей равно:

$$Q^{\text{в}} = N + M + R,$$
$$Q^{\text{с}} = N + R,$$
$$Q^{\text{н}} = R.$$

4. СПОСОБ ИДЕНТИФИКАЦИИ АТАКИ – АНАЛИЗ СОВОКУПНОСТИ АНОМАЛЬНЫХ СОБЫТИЙ

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 возможными 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. 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:

$$P = \{p_i : p_i\}\ ,\ i \in [1, I_p]\ ,$$
$$I_p = Q^{\text{в}} + Q^{\text{с}} + Q^{\text{н}}\ ,$$

где p_i — путь распространения атаки.

Множество индикаторов включает в себя:

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

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

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

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

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

Множество И можно описать с помощью характеристического предиката

$$\text{И} = \{\text{и}_j : \text{и}_j\},$$
$$j \in [1, J_{\text{н}}]\ ,$$

где и_j — индикатор сетевой, хостовой или периметровый.

Зададим соответствие множества путей атак множеству индикаторов

$$\tau_a \subseteq P \times \text{И} = \{(p_i, \text{и}_j) : p_i \in P \wedge \text{ и } j \in \text{И}\}\ .$$

Тогда сечение соответствия по $\tau_{\text{a}}(p_i)$ определяет набор индикаторов, соответствующий реализации угрозы на данном пути.

$$\tau_a(p_i) = \{(\text{и}_{p_i} : \text{и}_{p_i}\}\ ,$$

где и_{p_i} — индикатор одного события ИБ на пути атаки.

Регулярный контроль и оперативный анализ данных о подозрительной активности, которую можно идентифицировать как атаку, в условиях информационного противоборства позволит принимать обоснованные решения

о варианте реагирования на изменение среды функционирования, то есть формировать командную информацию для реализации управления в реальном времени.

Для путей распространения угроз разработаны модели, реализованные в модуле системы интеллектуальной поддержки принятия решений, что позволяет после установления пути распространения атаки выбирать типовые решений из базы моделей, вырабатывать оперативную командную информацию по рациональному управлению в условиях сложной обстановки информационного противоборства. Разработанные модели и метод принятия решений по оперативному управлению защитой информации на основе идентификации атаки по индикаторам на пути ее распространения описаны в [9], приведены численные примеры.

ЗАКЛЮЧЕНИЕ

На основе теоретико-множественного подхода построена математическая модель информационной системы, представляющей собой сегментированную сеть, в виде совокупности элементов, связанных между собой определенными отношениями, отображающими семантику предметной области (информационных объектов трех уровней конфиденциальности, узлов, сегментов, субъектов доступа), что позволяет определить множество источников угроз, внешних и внутренних, защищаемым информационным активам.

На основе семантической модели информационной системы предложено описание множества внешних удаленных и внутренних межсегментных угроз в виде кортежей, для каждого узла в соответствующем сегменте определены пути угроз, получена в количественном выражении оценка числа путей распространения угроз к узлам в сегментах, что позволяет внести в рассмотрение множество функциональных индикаторов, определять наборы индикаторов, соответствующих реализации атаки на каждом пути, и сопоставлять события в сети для принятия обоснованных решений по оперативному управлению.

СПИСОК ЛИТЕРАТУРЫ

1. **La Padula, L.** Secure computer system : mathematical foundation / L. La Padula, D. Bell. ESD-TR-73-278, V. I, MITRE Corporation.
2. **La Padula, L.** Secure Computer Systems : a mathematical model / L. La Padula, D. Bell. ESD-TR-73-278, V. II, MITRE Corporation.
3. **McLean, J.** A comment of the «Basic Security Theorem» of the Bell and La Padula / J. McLean. Information Processing Letters, 1985.
4. **Корт, С. С.** Теоретические основы защиты информации : учеб. пособие / С. С. Корт. М. : Гелиос АРВ, 2004. 240 с.
5. **Анфилатов, В. С.** Системный анализ в управлении : учеб. пособие / В. С. Анфилатов, А. А. Емельянов, А. А. Кукушкин. М. : Финансы и статистика, 2006. 368 с.
6. **ГОСТ ИСО/МЭК** 17799 [Электронный ресурс] (http://it4business.ru/itsec/ NormativnajaBazaRossijjskojjFederaciiPoBezopasnosti?v=14t8).
7. **Куликов, В. В.** Дискретная математика : учеб. пособие / В. В. Куликов. М. : РИОР, 2007. 174 с.
8. **Кузнецов, Н. А.** Информационная безопасность систем организационного управления. Теоретические основы / Н. А. Кузнецов. Ин-т проблем передачи информации РАН. М. : Наука, 2006.
9. **Машкина, И. В.** Модели и метод принятия решений по оперативному управлению защитой информации / И. В. Машкина // Системы управления и информационные технологии. 2008. № 32. С. 98–104.

ОБ АВТОРЕ

Машкина Ирина Владимировна, доц. каф. выч. техн. и защиты информации. Дипл. инж.-электромех. по авиац. приборостроению (УАИ, 1974). Канд. техн. наук по системам управления силов. установками летат. аппаратов (УАИ, 1989). Иссл. в обл. информ. безопасности.