

*Левченков Александр Николаевич*

канд. тех. наук, доцент

*Хаджи Ризгар Омер Хаджи*

магистрант

ФГБОУ ВО «Донской государственной  
технический университет»

г. Ростов-на-Дону, Ростовская область

## МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОГО ПОТОКА

*Аннотация:* статья посвящена одному из подходов к разработке графовой модели угрозы безопасности информационных потоков. Рассмотрена структура множеств объектов (информация), источников (часть среды информационного потока) и точек приложения (уязвимости) и предложены правила обработки информации в виде логических выражений и предикатов.

*Ключевые слова:* граф, информационный поток, источники угроз, угрозы безопасности информации, уязвимость информации, предикат.

Рассмотрим совокупность информационных потоков в автоматизированной системе. Каждый информационный поток исходит из какого-либо узла и заканчивается в каком-либо узле. Представим эти потоки в виде графа

$$G = \{V, E\} \quad (1)$$

где  $V$  – множество вершин графа, соответствующих узлам;

$E$  – множество ребер графа, соответствующих информационным потокам.

Поскольку каждый поток имеет определенное начало и конец, то граф  $G$  является ориентированным графом.

Среди множества информационных узлов выделим те узлы, которые принадлежат внешней среде автоматизированной системы. Назовем такие узлы внешними, а соответствующие им вершины графа  $G$  – внешними вершинами.

$$V = V_I \cup V_O, \quad (2)$$

где  $V_I$  – внутренние вершины графа;

$V_O$  – внешние вершины.

Зададим функцию

$$I_V : V \rightarrow N, \quad (3)$$

которая ставит в соответствие каждой вершине некоторое натуральное число, являющееся ее идентификатором.

Зададим функцию

$$L_V : V \rightarrow N_L \subset N, \quad (4)$$

где  $N_L$  – подмножество натуральных чисел, обозначающих уровни доступа (или грифы секретности). Функция  $L_V$  ставит в соответствие каждой вершине ее уровень доступа.

Зададим функцию

$$I_E : E \rightarrow N, \quad (5)$$

которая ставит в соответствие каждому ребру некоторое натуральное число, являющееся идентификатором соответствующего информационного потока.

Зададим функцию

$$L_E : E \rightarrow N_L, \quad (6)$$

которая определяет для каждого ребра уровень доступа, определенный для соответствующего информационного потока. Уровень доступа информационного потока и его идентификатор равны уровню доступа и идентификатору обрабатываемого в этом потоке информационного объекта.

Функции  $I_V, L_V, I_E$  и  $L_E$  предназначены для идентификации вершин и ребер и назначения им уровней доступа. Эти идентификаторы и метки уровней доступа используются для отражения в модели различных методов разграничения полномочий (мандатного и дискреционного).

Принятая для автоматизированной системы политика безопасности определяет правила взаимодействия информационных потоков с информационными объектами и узлами.

Под угрозой безопасности информации понимаются любые обстоятельства или события, которые могут являться причиной нанесения ущерба системе в

форме разрушения, раскрытия или модификации данных, или отказа в обслуживании. Анализ различных угроз позволяет выявить некоторые общие черты. Во-первых любая угроза направлена на какое-то определенное множество информационных объектов. Это могут быть данные пользователей, служебная информация, данные операционной системы и т. д. Во-вторых, угроза всегда исходит от какого-либо источника. В различных случаях в качестве источника, от которого исходит угроза, может выступать злоумышленник, пользователь системы, нарушающий правила работы, случайные события, такие как сбой в сети электропитания и т. д. В-третьих, всякая угроза реализуется, используя некоторые недостатки или уязвимости автоматизированной системы или информационной технологии [1]. Их еще можно назвать точками приложения угрозы. Это могут быть недостатки в организации вычислительного процесса, сбои и отказы аппаратных средств, ошибки и уязвимости программного обеспечения. Таким образом, угрозу  $T$  можно представить в виде тройки множеств:

- множество объектов  $O$ ;
- множество источников  $S$ ;
- множество точек приложения  $P$ ;

$$T = \{O, S, P\} \quad (7)$$

Рассмотрим структуру этих множеств более подробно.

Множество объектов  $O$ , на которые направлены угрозы безопасности, состоит из информационных объектов, представляющих собой порции информации и правила их обработки. Собственно, угроза безопасности информации состоит в доступе или модификации с нарушением этих правил. Правила обработки информации можно представить в виде логических выражений или предикатов, определяющих разрешенные действия над информационными объектами. Т.е. информационный процесс  $IP$  может выполнить операцию  $Op$  над информационным объектом  $O$  только в том случае, если предикаты  $Preds \in O$  принимают значения ИСТИНА для  $Op$  и  $IP$ .

Кроме правил, определяющих разрешенные операции так же существуют предикаты, которые описывают внутренние свойства информации, например, ее

целостность и непротиворечивость. Эти правила задаются при проектировании информационной технологии и отражаются в документации и спецификациях на информационные массивы и программное обеспечение. При информационных узлах все предикаты должны иметь значение «истина». Внутри потоков правила могут нарушаться, так как обработка информации выполняется последовательно и невозможно обеспечить целостность информации при выполнении программ ее обработки.

Контроль за выполнением правил обработки информации осуществляется выделенной группой информационных процессов, называемых ядром безопасности. Они работают с информационными объектами, называемыми дескрипторами защиты и представляющими собой предикаты других информационных объектов. Предикаты, описывающие правила работы с дескрипторами задаются при проектировании информационной технологии и остаются неизменными в течение всего времени ее использования. Таким образом, в модели выделяются две группы процессов – обычные и относящиеся к ядру безопасности. Первые выполняют функциональные задачи информационной системы, а вторые обеспечивают безопасность обрабатываемой информации [2].

Множество источников угроз  $S$  представляет собой причины нарушений безопасности информации. Такими источниками могут быть случайные факторы внешней среды или самой системы, а так же злоумышленники. В данном случае важен не их субъективный или объективный характер, а то, что эти источники инициируют процесс реализации угрозы.

Точки приложения  $P$  – это уязвимости, на использовании которых основана конкретная угроза безопасности информации. К их числу относятся недостатки организационного характера, ошибки, сбои и отказы аппаратуры, уязвимости программного обеспечения.

В предлагаемой модели информационной технологии объект  $O$  – это информация, источник – часть среды информационного потока, точка приложения – свойство информационного потока.

Рассмотрим, в чем проявляется реализация угрозы безопасности информации на графовой модели информационных потоков. Нарушение безопасности информации выражается в невыполнении предикатов информационного объекта при нахождении его в информационных узлах. Кроме того, раскрытие может произойти при попадании информационного объекта в информационный поток, заканчивающийся на внешнем информационном узле, не имеющем требуемого уровня полномочий. Пусть информационный поток  $IP$  начинается в узле  $IN1$  и заканчивается в узле  $IN2$ . В нашей модели ему соответствует дуга  $e \in E$  и вершины  $v_1, v_2 \in V$ , соответствующие начальному и конечному узлам. Предположим, что в потоке находится информационный объект  $O$ , обозначим функцию, соответствующую логическому произведению его предикатов  $O.pred()$ . Тогда нарушение безопасности имеет место, когда

$$O.pred(v_2)=false. \quad (8)$$

Таким образом, для противодействия угрозам безопасности информации необходимо не допускать ситуаций, при которых выполняется (8). Такие ситуации могут возникнуть в следующих случаях:

- в результате преобразования информации в информационном потоке;
- в результате перемещения защищаемой информации информационным потоком.

Первый случай касается угроз нарушения целостности, модификации и отказа в доступе, второй случай охватывает угрозы, связанные с разглашением информации ограниченного доступа. Для противодействия угрозам, относящимся к первому случаю существует ряд методов, связанных с контролем в начальных и конечных узлах информационных потоков, который осуществляется ядром безопасности. Это методы контрольного суммирования, проверки полномочий доступа, управления списком разрешенных действий и т. д. Ситуации, возникающие во втором случае, связаны с наличием в автоматизированных системах внешних информационных узлов, которые имеют непосредственную связь с внешней средой. В качестве наиболее характерного примера следует привести

наличие в системе отчуждаемых носителей информации, таких как дискеты, распечатки, магнитные ленты и т. д. Важной особенностью внешних узлов является то, что на них начинаются информационные потоки во внешнюю среду, которые реализуются вне вычислительных машин и не подпадают под контроль ядра безопасности. Уровень доступа и идентификатор внешнего информационного узла определяются уровнем доступа и идентификатором носителя информации, используемого в нем и очень часто у ядра безопасности нет технической возможности проконтролировать его. Например, ядро безопасности ПЭВМ не может определить учтенная или не учтенная бумага используется в принтере.

Таким образом, необходимо контролировать внешние информационные узлы и маршруты информационных потоков, заканчивающиеся в них. Рассмотрим некоторый информационный объект  $O$ . Разобьем множество внутренних вершин на два подмножества  $V_1$  и  $V_2$ , такие, что

$$V_I = V_1 \cup V_2, \quad (9)$$

$$V_1 = \{v \mid v \in V_I, O.pred(v) = true\}, \quad (10)$$

$$V_2 = \{v \mid v \in V_I, O.pred(v) = false\}. \quad (11)$$

В первое множество входят вершины, которые соответствуют тем узлам, в которых, согласно политики безопасности, может находиться информационный объект  $O$ , а ко второму – те, которые соответствуют узлам, попадание в которые объекта  $O$  означает нарушение безопасности информации. В соответствии с этим разобьем множество дуг.

$$E = E_1 \cup E_2, \quad (12)$$

$$E_1 = \{e = (v_1, v_2) \mid (v_1 \in V_1 \vee v_1 \in V_0) \wedge (v_2 \in V_1 \vee v_2 \in V_0)\}, \quad (13)$$

$$E_2 = \{e = (v_1, v_2) \mid v_1 \notin V_1 \vee v_2 \notin V_1\}. \quad (14)$$

Такое разбиение приводит к тому, что граф информационных потоков (1) распадается на два подграфа

$$G = G_1 \cup G_2, \quad (15)$$

где

$$G = \{V, E\}, \quad (16)$$

$$G_1 = \{V_1, E_1\}, \quad (17)$$

$$G_2 = \{V_2, E_2\}. \quad (18)$$

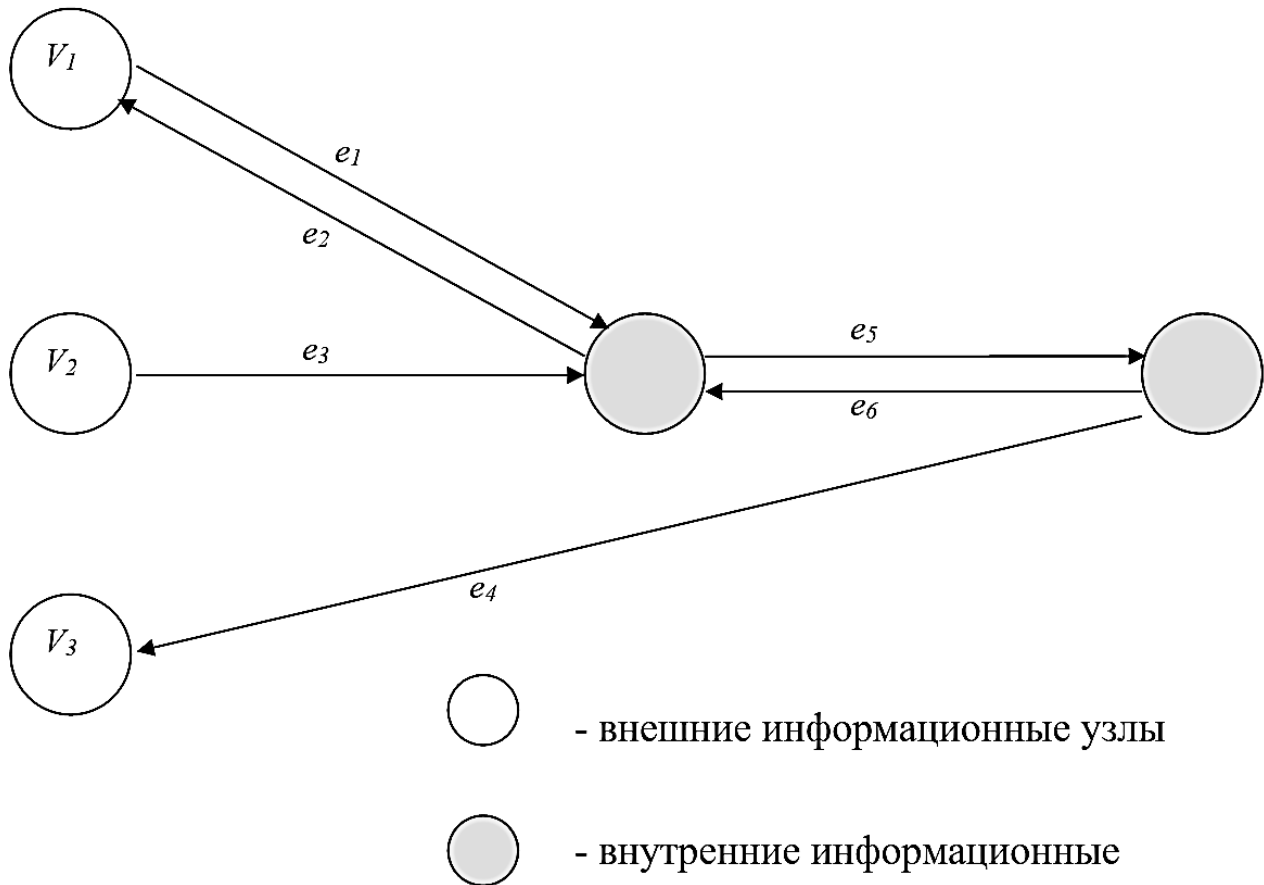


Рис. 1. Пример графовой модели информационных потоков

Граф (17) на рисунке 1 представляет собой схему информационных потоков и узлов, которые являются для объекта  $O$  разрешенными политикой безопасности. За техническую реализацию разбиения (15) в информационной системе отвечает ядро безопасности.

Пусть в некоторый момент времени информационный объект  $O$  находится в информационном узле, которому соответствует вершина  $v \in G_1$ . Рассмотрим вершину  $v' \in V_O$ . Если в графе  $G_1$  существует ориентированный маршрут  $M$ , начальная вершина которого есть  $v$ , а конечная –  $v'$ , то существует угроза

$$T = \{O, S, P\}, \quad (19)$$

где  $P$  – уязвимость, заключающаяся в возможности утечки информации через информационный узел, которому соответствует вершина  $v'$ .

Таким образом, в настоящее время актуальной проблемой является возможность раскрытия информации при записи ее на отчуждаемые носители. Для решения этой проблемы необходимо разработать и реализовать комплекс механизмов и средств, выявляющих и перекрывающих маршруты, по которым информационные объекты могут попадать на внешние информационные узлы и отчуждаемые носители информации.

### *Список литературы*

1. Левченков А.Н. Критерии оценки безопасности программного обеспечения / А.Н. Левченков, А.Н. Бабарицкий // Известия ТРТУ. – 2003. – №4.
2. Negnivitsky M. Artificial Intelligence: A Guide to Intelligent systems? England? Harlow: Addison Wesley, 2002.