Список літератури

1. *Богуш В.М.* Розвідка в інформаційному суспільстві. - К.: МОУ, 2000 750. с.
2. *Богуш В.М., Юдін О.К.* Основи інформаційної безпеки держави. - Харків: "Консум" П, 2004. 510 с.
3. *Богуш В.М., Кривуца В.Г., Кудін А.М.* Інформаційна безпека: термінологічний навчальний довідник. Київ:"Д.В.К.". 2004. 508 с.
4. *Мухачов В.А., Хорошко В.А.* Методи практичної криптографії. Київ 2004. 124 с.
5. Вступ до комп'ютерної інженерії: Методичні рекомендації до самостійної роботи студентів / Уклад. В.М.Богуш, В.В.Богданов - К.: ДУІКТ, 2004 - 40 с.
6. Інформаційна культура: Методичні рекомендації до самостійної роботи студентів / Уклад. В.М. Богуш - К.: ДУІКТ, 2004 - 40 с.
7. Теорія інформації та кодування: Методичні вказівки до самостійної роботи студентів / Уклад. В.М. Астапеня - К.: ДУІКТ, 2003 - 36 с.
8. *Г.А.Максименко, В.А. Хорошко.* Методи виявлення, обробки й ідентифікації сигналів радіозакладних пристроїв. - К.: ТОВ "Поліграфконсалтинг" , 2004. - с.317, іл.
9. Термінологічний словник з питань технічного захисту інформації (Хорошко В.О., Огаркова Й.М., Чирков Д.В. та інші, за ред. проф. В.О. Хорошка.) - 3-є вид., доп. І перераб. - К.: Поліграфконсалтінг, 2003. 286 с. - Бібліогр.: с. 269-270

УДК 004.681

Зыбин С.В.

МОДЕЛЬ ОБЪЕКТА ЗАЩИТЫ ИНФОРМАЦИИ И МОДЕЛИ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

Использование методов моделирования в области обеспечения безопасности привело к разработке большого количества формальных моделей безопасности. Формальные модели используются достаточно широко, потому что только с их помощью можно доказать безопасность системы опираясь при этом на объективные и неопровержимые постулаты математической теории. Основная цель создания политики безопасности информационной системы и описания ее в виде формальной модели – это определение условий, которым должно подчиняться поведение автоматизированной системы, выработка критерия безопасности и проведение формального доказательства соответствия системы этому критерию.

Наиболее общей моделью формального описания систем защиты является модель системы безопасности с полным перекрытием, в которой определяется полный перечень объектов защиты и угроз информации. В модель вводится набор объектов $O=\{o_j\}$, которые нуждаются в защитных мерах, и набор угроз $T=\{\delta_j\}$, каждая из которых направлена на один или несколько защищаемых объектов. Множество отношений угроза-объект образует двухдольный граф, в котором ребро $<\delta,o>$ существует тогда и только тогда, когда угроза δ является способом получения доступа к объекту o. Следует отметить, что угроза δ может быть направлена на несколько объектов и один объект может подвергаться нескольким угрозам. Цель моделируемой системы защиты АС УВД в том чтобы перекрыть все возможные ребра в графе $\{<T,O>\}$, т.е. добиться того, чтобы к каждому объекту не было ни одного не перекрытого пути ни от одной угрозы. Это достигается введением третьего набора $M=\{m_k\}$, который включает способы обеспечения безопасности. В идеальной системе каждый способ m_k, должен устранять, по крайней мере, одно ребро $<\delta,o>$ графа $\{<T,O>\}$. Введение набора M способов обеспечения безопасности преобразует

двухдольный граф в трехдольный граф *{<T,M,O>}*, который содержит дуги вида *<δ,m>* и *<m,o>*. Таким образом, в защищенной системе любое ребро в виде *<δ,o>* определяет незащищенный объект. Один и тот же способ обеспечения безопасности может перекрывать больше одной угрозы и (или) защищать больше одного объекта. При сопоставлении модели с полным перекрытием и общей схемы взаимодействий, очевидно, что модель не учитывает возможностей одновременного существования разных типов угроз, возможностей их взаимодействий и, соответственно, разносторонних способов защиты. Таким образом, развитие модели формального описания систем защиты связан, прежде всего, с введением более общего понятия угроз, а также построения аппарата для моделирования разнообразных видов угроз и их взаимодействий.

Для описания объектов защиты введем наборы:

1. *O={o(δ)}*, описывает содержание защищаемых объектов, *H(o)* - их характеристики;
2. *C={c(i,j)}*, описывает всевозможные связи между элементами объекта (например, *c(i,j)=1* для существующей связи между элементами *o(i)* і *o(j)*, *c(i,j)=0* в противоположном случае), *H(o)* - их характеристики;
3. *EO* - перечень внешних объектов, которые взаимодействуют с защищаемыми объектами, *H(EO)* - их характеристики;
4. *EC* - перечень внешних связей с объектами *EO*, *H(EC)* - их характеристики.

Модель пассивный канал утечки информации

Модель пассивный канал утечки информации предполагает, что нарушитель не предпринимает активных действий. Таким образом, для описания нарушителя достаточно набора *T{δ}*, который описывает такие угрозы. В терминах общей модели такой набор угроз можно обозначить как T_1.

Для описания объекта необходимо учитывать:

1. *O* – отдельные элементы объекта;
2. *C* – информационные связи (обозначим их C_1 в терминах общей модели);
3. *U* – неконтролируемые элементы, т.е. те, которые могут служить источниками информации для угроз T_1 (в общей модели можно ввести обозначение U_1);
4. Предполагается, что все элементы надежны и, соответственно, все другие множества для общей модели являются пустыми;
5. Способы защиты *Z={z}* для простоты предполагается связанными только с элементами модели объекта, т.е. *z=z(o)*.

В этом случае для описания модели пассивный канал утечки информации используем простейшие предикаты:

Объект: *элемент(o)* – если «*o*» принадлежит множеству *O*;

- *инф_связь(o,e)* – если «*o*» и «*e*» принадлежат множеству *O*, а *c(o,e)* множеству C_1;

- *не_контр(o)* – если с элемента «*o*» возможно снятие информации (т.е. нет гарантии, что информация из этого элемента «вытекать» не может), что соответствует множеству U_1 общей модели.

Защита: *защита(o)* – если существуют способы защиты, которые связаны с «*o*»;

- *(защита(o))* – если таких *z* не существует.

Нарушитель: *чтение(o)* – если нарушитель пытается получить информацию из «*o*» (конкретного элемента или элемента, который принадлежит классу (типу) элементов, из которых осуществляется попытка получения информации).

Можно сделать вывод, что модель пассивный канал утечки информации представляет собой множество опасностей $M_1 = \{m\}$.

Используя форму записи предикат, которая принята в языке логического программирования ПРОЛОГ для описания цепей передачи информации через связи, правила выведения F_1 можно представить в рекурсивной форме описания предикат:

$$m(o,\delta) \leftarrow [(элемент(o)) \& (не\_контр(o)) \& (защита(o)) \& (чтение(o))] \cup$$
$$\cup [(элемент(o)) \& (не\_контр(o)) \& (защита(o)) \& (чтение(o))];$$
$$m(o/z,\delta) \leftarrow (элемент(o)) \& [m(e,\delta) \& (инф\_связь(o,e/c)) \& (защита(o))] \cup$$
$$\cup [m(e,\delta) \& c(o,e) \& (защита(o,z))]$$

Если построить независимо от наличия способов защиты *z(o)* цепи информационных связей $c_i(o,e)$, то среди них не может быть двух одинаковых (соответственно, цепь со способами защиты и без них), которые обеспечиваются последовательным использованием предикат *(защита(o,z))* и *(защита(o))* рис.1.

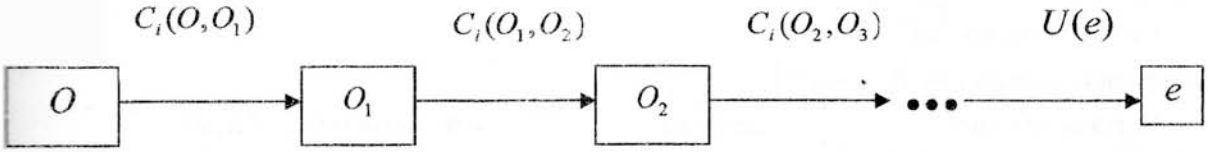

Рис. 1. Схема реализации угроз в модели пассивный канал утечки информации

Так как каждому предикату *«m»*, который описывает «опасность», сопоставляются множества $\{o\}$, $\{c\}$, $\{z\}$, $\{u\}$, $\{v\}$, также угроза «δ», при которых данный предикат является истинным, то для определения характеристик опасности *h(m)* необходимо агрегировать выходные оценочные данные – характеристики всех составляющих.

Модель активный канал утечки информации

В модели активный канал утечки информации предполагается, что нарушитель занимается сбором и съемом информации всеми возможными способами. Таким образом, для описания нарушителя достаточен набор $T=\{\delta\}$, который описывает подобные угрозы. В терминах общей модели такой набор угроз можно обозначить как T_1.

Для описания объекта необходимо учитывать:

1. O – отдельные элементы объекта;
2. C – информационные связи (обозначим C_1 в терминах общей модели);
3. U – неконтролируемые элементы, т.е. те, которые могут служить источниками информации для угроз T_1 (обозначим их U_1 в терминах общей модели);
4. V – внутренние воздействия, в большинстве аналогичные T_1, которые направлены на установление возможных нетехнологичных связей (v,u), и которые для простоты (как указывалось в общем описании объекта) могут быть объединены в отдельное множество C_{nt} или C_2. Таким образом, в описании объекта уже не предполагается надежность всех элементов.
5. Способы защиты $Z=\{z\}$ для упрощения предполагается связанными только с элементами модели объекта, т.е. $z=z(o)$.

В этом случае для описания модели активный канал утечки информации используем простейшие предикаты (в расширенной форме записи):

Объект: *элемент(o)* – если «*o*» принадлежит множеству *O*;

- *инф_связь(o,e/c)* – если «*o*» и «*e*» принадлежат множеству *O*, а *c(o,e)* множеству C_1;

- *не_контр(о/и)* – если с элемента «*о*» возможно снятие информации (т.е. нет гарантии, что информация из этого элемента «вытекать» не может), что соответствует множеству U_1 общей модели;

- *вн_чтение(о/v)* – если элемент «*о*» может активизироваться для образования нетехнологичного информационного канала целенаправленно или случайно (V_1).

Защита: *защита(о/z)* – если существуют способы защиты *z*, которые связаны с «*о*»;

- *(защита(о))* – если таких *z* не существует.

Нарушитель: *чтение(о/δ)* – если нарушитель пытается получить информацию из «*о*» (конкретного элемента или элемента, который принадлежит классу (типу) элементов, из которых осуществляется попытка получения информации).

Можно сделать вывод, что модель активный канал утечки информации будет состоять из развития описания объекта через введение понятия «нетехнологическая связь» в виде:

$$нт\_связь(o,e/u,v) \leftarrow (элемент(o)) \& (элемент(e)) \& (вн\_чтение(e/v) \& (не\_контр(o/u)$$

и множества опасностей $M_2 = \{m\}$.

Использование предикат $нт\_связь(o,e/u,v)$ и $[((инф\_связь(o,e/c)) \cup (нт\_связь(o,e/u,v))]$ позволяет в модели активный канал утечки информации сформировать цепи передачи информации, которые состоят как из технологичных $c_i(o,e)$, так и из нетехнологичных связей $c_{нт}(o,e)$ (возможных информационных взаимодействий).

При этом среди этих цепей (по сути, это множество M_2) так же как в M_1 не может быть двух одинаковых связей.

Модель несанкционированного доступа с целью снятия информации

Модель несанкционированного доступа с целью снятия информации или «активная утечка информации» предполагает, что нарушитель прилагает активные действия – осуществляет несанкционированного доступа (проникновение в систему) для воздействия на ее элементы с целю их активизации по получению информации (т.е. могут возникнуть новые «наведенные» внутренние воздействия для построения новых нетехнологических каналов передачи информации или изменения существующих характеристик). Таким образом, для описания нарушителя достаточно списка $T = [T_1, T_2]$, где T_1 - угрозы по съему информации, а T_2 - угрозы несанкционированного доступа.

Для описания объекта необходимо учитывать:

1. O – отдельные элементы объекта;
2. C_1 – информационные связи (C_1);
3. C_k - связи управления (C_3);
4. U_1 – неконтролированные элементы, т.е. те, которые могут служить источниками информации для угроз T_1;
5. U_2 – неконтролированные элементы, т.е. те, которые могут служить предметом несанкционированного доступа для угроз T_2;
6. V_1 – внутренние воздействия, в большинстве аналогичные T_1, которые направлены на установление возможных нетехнологичных связей (v_1, u_1), и которые могут быть объединены в отдельное множество $C_{нт}$ или C_2.

7. V_2 – внутренние воздействия, в большинстве аналогичные T_2, которые направлены на установление возможных нетехнологичных связей (v_2, u_2), и которые для простоты могут быть объединены в отдельное множество C_{nk} (или C_4). Таким образом, в описании объекта, как и в модели АКУИ, уже не предполагается надежность всех элементов.

8. Способы защиты *Z={z}*, как и в модели активный канал утечки информации, предполагается связанными только с элементами модели объекта *z=z(o)* и не взаимодействуют с другими элементами модели и внешними объектами, т.е. неуязвимы и надежны.

Объект:

- *элемент(o)* – если «*o*» принадлежит множеству *O*;
- *инф_связь*$(o, e / c_1)$ – если «*o*» и «*e*» принадлежат множеству *O*, а *c(o,e)* множеству C_1;
- *упр_связь*$(o, e / c_2)$ – если «*o*» и «*e*» принадлежат множеству *O*, а *c(o,e)* множеству C_k;
- *не_контр*(o / u_1) – если с элемента «*o*» возможен съем информации (т.е. нет гарантии, что информация из этого элемента не сможет «вытечь»), что соответствует множеству U_1 общей модели;
- *доступный*(o / u_2) – если к элементу «*o*» возможен доступ для изменения режима его работы, что соответствует множеству U_2 общей модели;
- *вн_чтение*(o / v_1) – если элемент «*o*» может активизироваться для образования нетехнологичного информационного канала целенаправленно или случайно (V_1).
- *вн_нсд*(o / v_2) – если элемент «*o*» может активизироваться для образования нетехнологичного управляющего воздействия целенаправленно или случайно (V_2).

Защита:

- *защита*(o / z_1) – если существуют способы защиты, которые связаны с «*o*»;
- *(защита(o))* – если таких *z* не существует;
- *нсд_защ*(o / z_2) – если существуют способы защиты от несанкционированного доступа, которые связаны с «*o*»;
- *(нсд_защ(o))* – если способов защиты от несанкционированного доступа не существует;

Нарушитель:

- *чтение*(o / δ_1) – если нарушитель пытается получить информацию из «*o*» (конкретного элемента или элемента, который принадлежит классу (типу) элементов, из которых осуществляется попытка получения информации);
- *нсд*(o / δ_2) – если нарушитель пытается получить доступ к «*o*» (конкретному элементу или элементу, который принадлежит классу (типу) элементов, к которым осуществляется попытка несанкционированного доступа).

Таким образом, модель несанкционированного доступа, будет состоять из развития описания объекта посредством введения новых понятий

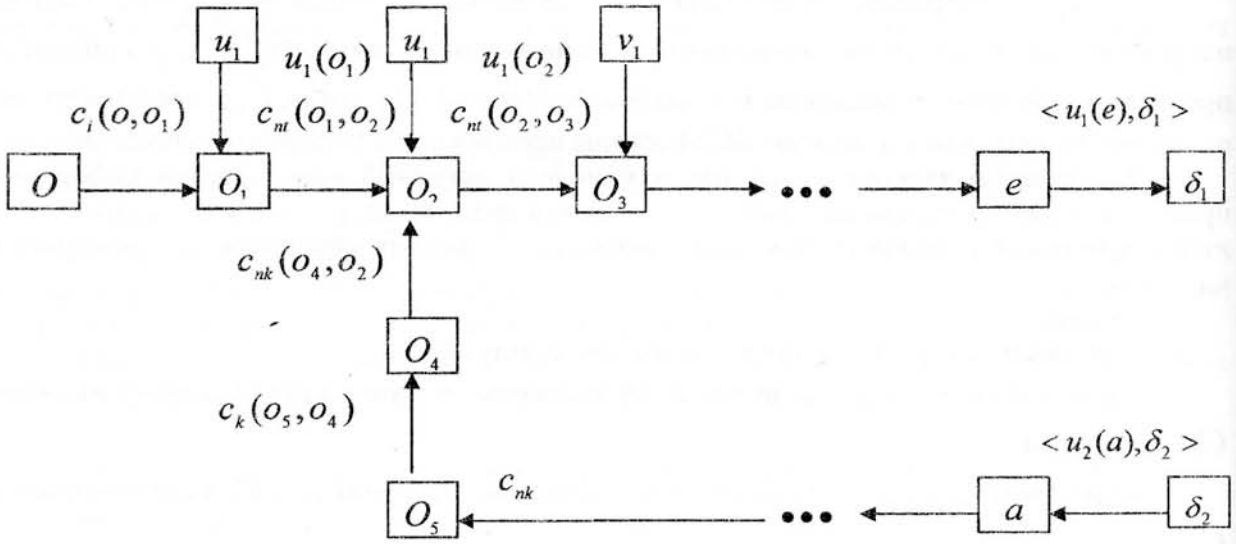

Рис.2. Структура угроз в модели несанкционированного доступа с учетом нетехнологических управляющих связей

а) «нетехнологичная управляющая (несанкционированная) связь»:

нс _ связь $(o, e / u_2, v_2) \leftarrow$ (*элемент* (o)) & (*элемент* (e)) & *вн _ нсд* (o / v_2) & *доступный* (e, u_2);

б) «несанкционированное управляющее воздействие»;

в) «информационная нетехнологичная связь».

Структура угроз в модели несанкционированного доступа с учетом нетехнологических управляющих связей изображена на рисунке 2, а с учетом несанкционированных управляющих связей – на рис. 3.

Рассмотренные примеры показывают, с одной стороны, возможности предложенного аппарата для формального описания моделей разного вида и наглядности их представления, а с другой стороны, сложность моделирования каждой непосредственной системы защиты.

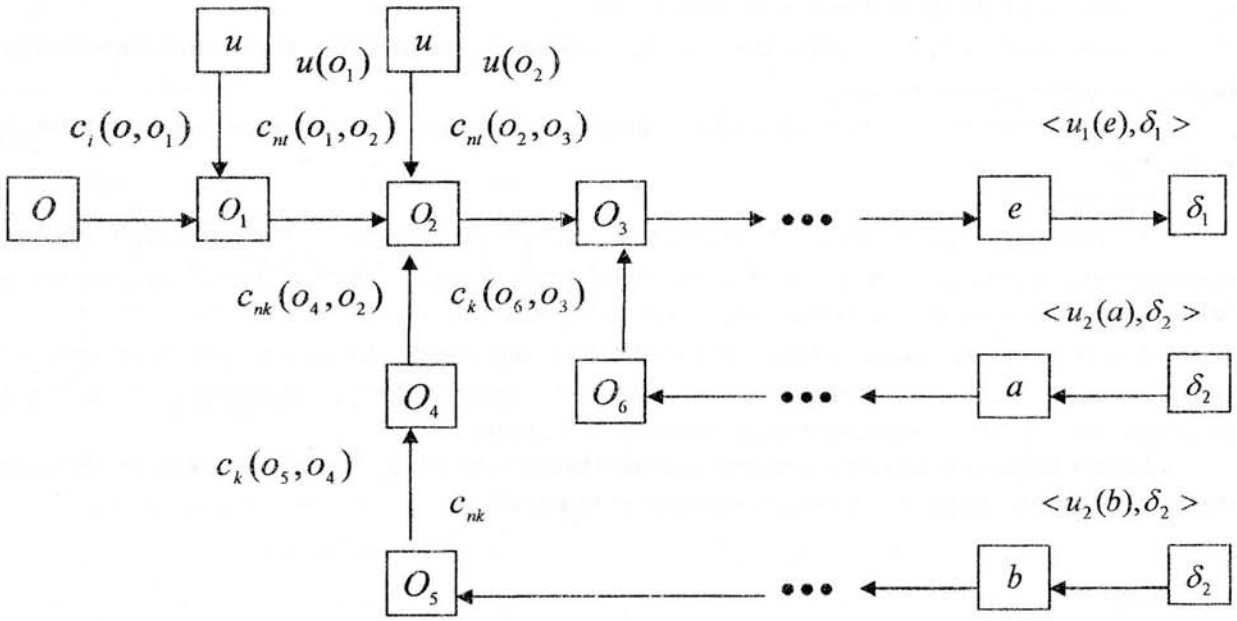

Рис. 3. Структура угроз в модели несанкционированного доступа с учетом несанкционированных управляющих связей

Предложенная модель объекта защиты информации позволяет описать различные связи между элементами. Это позволяет анализировать сеть в произвольном описании и является общим, в тоже время позволяет учитывать особенности каждого объекта.

УДК 004.681

Хорошко В.А., Чередниченко В.С.

КАТЕГОРИИ И ВИДЫ ИНФОРМАЦИОННЫХ ВОЗДЕЙСТВИЙ

В настоящее время различным аспектам информационной борьбы (противоборства, воздействий, угрозы войны) уделяется большое внимание в средствах массовой информации и научных изданиях. Проведенный анализ позволяет сделать вывод, что при общности взглядов на информационную борьбу существуют различные подходы к определению целей, объектов воздействия, способов воздействия и средств информационной борьбы.[1,2].

С точки зрения Украины источником информационных воздействий, по их происхождениям и внутренней природе можно разделить на три категории.[2].

К первой категории – относятся источники внешней угрозы:
- наличие информационных атак из вне;
- заинтересованность в изменении информационных потоков как из вне, так и внутренних;
- заинтересованность в ослаблении политической, экономической и военной роли Украины в регионе, на континенте и в мире;
- поддержка и позитивное отношение к действиям дестабилизирующих сил в Украине;
- заинтересованность в информационных ресурсах Украины, в установлении контроля над ее информационными ресурсами.

Вторая категория составляет источники,
- которые образуются объективными внешними условиями: действуют или существуют за границами Украины и не имеют прямых признаков информационных угроз для Украины;
- стойкое увеличение затрат на информационную борьбу;
- внутренняя социально-политическая нестабильность.

К третьей категории относятся источники внутреннего происхождения, которые, так или иначе, влияют на уровень информационной небезопасности для Украины:
- неудовлетворительное состояние информационной безопасности;
- недостаточное финансирование из государственного бюджета Украины на нужды информационной безопасности;
- проявление социально-политического и морально-психологического кризиса в отношении к информационной борьбе.

Все эти категории воздействия в большей или меньшей степени влияют на безопасность информации в государстве, а, следовательно, усугубляют условия информационной борьбы.

Процесс разработки теоретических основ информационной борьбы и воздействий затруднен тем, что не существует однозначного определения и всеми принятого понятия – «информация». Так, Закон Российской Федерации «Об информации, и защите информации» трактует это понятие, как сведения о лицах, фактах, событиях, явлениях и процессах, независимо от формы их представления. А Закон Украины «Об информации», – определяет как документированные или публично оглашенные сведения о событиях и явлениях, происходящих в обществе, государстве и окружающей среде. В тоже время философское определение понятия «информация» звучит, как система идеальных (субъективных) образов объектов, процессов и явлений окружающего нас мира в сознании человека, а так же множество признаков, присущих материи и формирующих идеальные образы. Исходя из приведенных понятий, можно сделать вывод, что они не позволяют рассматривать «информацию» как объект воздействия и сужает сферу информационной борьбы и воздействий.