УДК 519.72:004.056

А.А. Барышников, И.А. Исаев

МОДЕЛИРОВАНИЕ ВЕРОЯТНОСТИ ВЗЛОМА СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (СИСТЕМНО-ИНТЕГРАЛЬНЫЙ ПОДХОД)

Рассмотрен системно-интегральный подход в решении задач информационной безопасности. Моделируется вероятность взлома информационно-управляющей системы и получается интегральная экспертная оценка несанкционированного доступа в систему методом составления логической функции.
Ключевые слова: информационная безопасность, системно-интегральный подход, вероятность взлома системы, структурная схема.

Проблема обеспечения безопасности в широком смысле как физических, так и юридических лиц, но в особенности, всевозможной информационной собственности, в условиях окружающего нас современного мира, с каждым годом становится вес актуальнее и сложнее.

Вследствие внедрения в нашу жизнь новых информационных технологий, в том числе сетевых, в условиях массового использования персональных

Компьютеров, общедоступных каналов связи, большего количества субъектов, имеющих доступ к системе защиты объекта, наличие технического оборудования от разных производителей, постоянный рост объема и сложности программного обеспечения, его многоуравненности, рост степени распределенности систем и пр., это далеко не полный перечень факторов, провоцирующих вероятность незаконного проникновения в любой объект (систему), в том числе, в систему информационной безопасности объекта.

Традиционно считается, что большинство задач инженерно-технологической защиты являются слабо формализируемыми задачами, когда формальное получение оптимального решения крайне затруднительно в силу наличия большого числа факторов самой разнообразной природы, в очень малой степени поддающихся точному учету и корректному описанию из-за отсутствия достоверных количественных данных об этих факторах.

Однако если попытаться выделить отдельную группу каналов утечки информации, наиболее характерных для какого-либо конкретного объекта и попытаться объединить эти каналы в виде структурной схемы (блок-схемы) некоторой системы, то может быть синтезирована система информационной безопасности какого-либо объекта, имитирующая конечное число способов незаконного проникновения в систему информационной безопасности, или в систему информации объекта.

С помощью структурной схемы такой системы может быть рассчитан такой важный показатель качества системы безопасности, как вероятность несанкционированного доступа в данную систему безопасности, или вероятность "взлома" этой системы, рассматриваемой как единое целое.

Очевидно, что вводимый таким образом показатель (обозначим его L) носит интегральный характер и находится целиком в рамках интегрального подхода к проблеме защиты информации, в рамках концепции интегральной безопасности. Известно, что интегральная безопасность характеризует такое физическое состояние функционирующего объекта, циркулирующей в нём информации и человеческого фактура, при котором они надежно защищены от всех возможных видов угроз несанкционированного доступа в процессе решения поставленных задач.

Интегральная безопасность, в пределе, должна аккумулировать в себе как все необходимые для решения данной задачи на объекте виды безопасности (охранная, пожарная, электрическая, экологическая, информационная и т.д.), так и перечень большинства каналов утечки рассматриваемого объекта (акустического, электрического, электромагнитного и т.д.) для их блокировки.

В настоящее время считается общепризнанным фактом, что, оставаясь в рамках концепции интегральной защиты, интегральной безопасности объекта, эффективность создаваемой системы информационной безопасности этого объекта может быть существенно повышена.

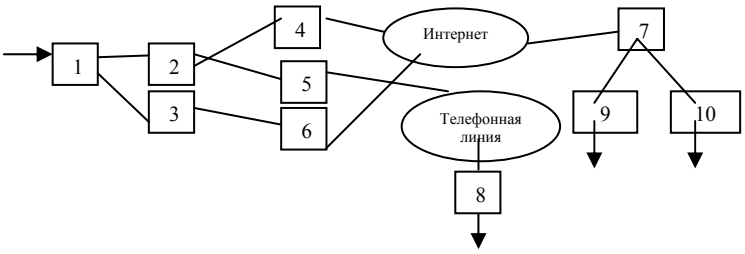
Вводимый интегральный показатель L находится полностью в рамках системного подхода к рассматриваемой в статье задаче оценивания вероятности взлома системы защиты информации, поскольку этот показатель рассчитывается на основе наиболее универсальной модели объектно-структурной схемы системы информационной безопасности.

Система – как самый высокий уровень описания объекта исследования - порождает системный подход, а последний, как известно, аккумулирует в себе некоторый алгоритм описания процесса функционирования объекта с помощью модели, называемой системой. Как известно система – это целенаправленное множество взаимосвязанных элементов любой природы. В рассматриваемой нами задаче – моделировании процессов взлома системы информационной безопасности – в качестве элементов такой системы естественно рассматривать возможные каналы утечки информации, представляемые в виде блоков структурной схемы, соединенных последовательно, параллельно, треугольником, звездой и другими стандартными способами.

В случае отсутствия необходимой структурной схемы, процедура моделирования начинается с выделения некоторого конечного числа каналов утечки, например: электрического, акустического, электромагнитного, кабельной сети и двух компьютеров (с их материнскими платами). Можно предложить, например, следующую словесную формулировку процедуры несанкционированного проникновения в систему информационной безопасности.

Рассмотрим распределенную ИУС состоящую из центра управления *1*, сервера обработки почты *2*, связи через телефонную линию и интернет, удаленного сервера *7, 8*, рабочие станции конечных пользователей *9, 10*, шлюз *4*, вспомогательный шлюз *5*, Intranet сервер *3*, File server *6*.

Из литературных данных [3] нами были взяты следующие каналы утечки для блоков (1-10) и оценки для соответствующих вероятностей несанкционированного доступа в систему по средством этих каналов.



Блок 1 – электрический канал утечки P≅0.1

Блоки 2,6,7,8 – использование вирусных программ для несанкционированного доступа в систему P≅0.08

Блок 3 – электромагнитный канал утечки P≅0.18

Блоки 4,5 – электрический канал утечки P≅0.15

Блок 9,10 – использование вирусных программ для несанкционированного доступа в систему P≅0.3

Телефонная линия – акустический канал утечки P≅0.45

Интернет линия – электромагнитный канал утечки P≅0.35

Для получения интегральной экспертной оценки несанкционированного доступа в систему составляем логическую функцию работоспособности рассматриваемой системы:

L_{Σ}=P(1)*P(2)*P(4)*P(int)*P(7)*P(9) V P(1)*P(2)*P(4)*P(int)*P(7)*P(10) V P(1)*P(2)*P(5)*P(tel)*P(8) V P(1)*P(3)*P(6)*P(int)*P(7)*P(9) V P(1)*P(3)*P(6)*P(int)*P(7)*P(10)

L_{Σ}= P(1)*P(2)*P(4)*P(int)*P(7)*(P(9)VP(10)) V P(1)*P(2)*P(5)*P(tel)*P(8) V P(1)*P(3)*P(6)*P(int)*P(7)*(P(9)VP(10))

Для упрощения вида выражения примем:

A_1= P(1)*P(2)*P(4)*P(int)*P(7)

A_2= P(1)*P(2)*P(5)*P(tel)*P(8)

A_3= P(1)*P(3)*P(6)*P(int)*P(7)

Переходя к арифметической логической функции:

$L_a = A_1*(P(9)VP(10)) + A_{2+} A_3*(P(9)VP(10)) - A_1* A_2*(P(9)VP(10)) - A_2* A_3*(P(9)VP(10)) - A_1* A_3*(P(9)VP(10))^2 + A_1* A_2*A_3*(P(9)VP(10))^2$

Таким образом:

A_1= 0,1*0,08*0,15*0.35*0,08=0,0000336

A_2= 0,1*0,08*0,15*0.45*0,08=0,0000432

A_3= 0,1*0,18*0,08*0,35*0.08=0,0004032

L_a = 0,0000336*(0,3+0,3-0,09) + 0,0000432 + 0,0004032* (0,3+0,3-0,09) - 0,0000336*0,0000432*(0,3+0,3-0,09) - 0,0000432*0,0004032*(0,3+0,3-0,09) - 0,0000336*0,0004032*(0,3+0,3-0,09) ^{2} + 0,0000336*0,0000432*0,0004032* (0,3+0,3-0,09) ^{2} ≅0,000266

Итак, не следует переоценивать малую вероятность «взлома» всей системы, так как метод её расчёта учитывает все количество вариантов несанкционированного доступа в данную, конкретную систему, и в логической функции в явном виде присутствуют вероятности «взлома» каждого из элементов информационной системы. Вводимый показатель является важнейшим показателем, характеризующим качество системы информационной безопасности и обязательно должен учитываться при аттестации этой системы.

СПИСОК ЛИТЕРАТУРЫ

1. *Исаев А.Б.* Современные технические методы и средства защиты информации. Учебное пособие – М., РУДН, 2008., 258 с. ГИАБ

Коротко об авторах

Барышников А.А. – аспирант кафедры кибернетики и мехатроники инженерного факультета Российского университета дружбы народов,
Исаев И.А. – магистр кафедры высшей математики факультета физико-математических и естественных наук Российского университета дружбы народов
aspirant@office.rudn.ru

ДИССЕРТАЦИИ

ТЕКУЩАЯ ИНФОРМАЦИЯ О ЗАЩИТАХ ДИССЕРТАЦИЙ ПО ГОРНОМУ ДЕЛУ И СМЕЖНЫМ ВОПРОСАМ

Автор	*Название работы*	*Специальность*	*Ученая степень*
РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НЕФТИ И ГАЗА им. И.М. ГУБКИНА			
ЯСАШИН Виталий Анатольевич	Конструкторские и технологические методы повышения эффективности работы буровых шарошечных долот большого диаметра	05.02.13	д.т.н.
ШУТЬ Константин Федорович	Предупреждение осыпей и обвалов кристаллических пород во время бурения скважин	25.00.15	к.т.н.