ФЕДЕРАЛЬНОЕ АГЕНТСТВО ВОЗДУШНОГО ТРАНСПОРТА
(РОСАВИАЦИЯ)

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ ГРАЖДАНСКОЙ АВИАЦИИ» (МГТУ ГА)

Кафедра основ радиотехники и защиты информации

В.Е. Емельянов

ИССЛЕДОВАНИЕ ОПЕРАЦИЙ

ПРИМЕНЕНИЕ ТЕОРИИ ИГР В ЗАДАЧАХ ЗАЩИТЫ ИНФОРМАЦИИ

Учебное пособие

Утверждено редакционно-издательским советом МГТУ ГА в качестве учебного пособия

Москва
ИД Академии Жуковского
2021

УДК 004.056:519.83
ББК 517.8
Е60

Печатается по решению редакционно-издательского совета
Московского государственного технического университета ГА

Рецензенты:
Лутин Э.А. (МГТУ ГА) – д-р техн. наук, профессор;
Колядов Д.В. (ООО «РОДЕ и ШВАРЦ РУС») – д-р техн. наук

Емельянов В.Е.

Е60 Исследование операций. Применение теории игр в задачах защиты информации [Текст] : учебное пособие / В.Е. Емельянов. – М. : ИД Академии Жуковского, 2021. – 56 с.

ISBN 978-5-907490-11-6

В учебном пособии излагаются особенности информационной защиты, рассматриваются игровые и топологические модели защиты информации в телекоммуникационных системах. Приводятся подходы к решению антагонистических игр, а также модели с двумя противоборствующими сторонами и алгоритмы, которые могут быть использованы для выбора средств защиты информации в информационных системах.

В учебном пособии излагаются некоторые методы теории игр для оптимизации выбора средств защиты информации.

Учебное пособие предназначено для обучающихся по специальности 10.05.02, изучающих дисциплину «Исследование операций».

Рассмотрено и одобрено на заседаниях кафедры 17.06.2021 г. и методического совета 17.06.2021 г.

УДК 004.056:519.83
ББК 517.8
Св. тем. план 2021 г.
поз. 33

ЕМЕЛЬЯНОВ Владимир Евгеньевич

ИССЛЕДОВАНИЕ ОПЕРАЦИЙ.
ПРИМЕНЕНИЕ ТЕОРИИ ИГР В ЗАДАЧАХ ЗАЩИТЫ ИНФОРМАЦИИ

Учебное пособие

В авторской редакции

Подписано в печать 26.10.2021 г.
Формат 60x84/16 Печ. л. 3,5 Усл. печ. л. 3,255
Заказ № 836/1004-УП03 Тираж 30 экз.

Московский государственный технический университет ГА
125993, Москва, Кронштадтский бульвар, д. 20

Издательский дом Академии имени Н. Е. Жуковского
125167, Москва, 8-го Марта 4-я ул., д. 6А
Тел.: (495) 973-45-68 E-mail: zakaz@itsbook.ru

ISBN 978-5-907490-11-6

ВВЕДЕНИЕ

Во многих практических задачах исследования операций в области защиты информации приходится анализировать ситуации, в которых сталкиваются две (реже более) враждующих стороны, преследующие различные цели, причем последствие любого мероприятия каждой из сторон зависит от того, какой образ действий выберет противник. Такие ситуации называются конфликтными ситуациями. Выбор рекомендаций по рациональному образу действий участников конфликта и есть задача теории игр. Каждая непосредственно взятая из практики конфликтная ситуация очень сложна, чтобы сделать возможным математический анализ ситуации, необходимо построить упрощенную, схематизированную модель ситуации. Такую модель и называют игрой.

От реальной конфликтной ситуации игра отличается тем, что ведётся по вполне определенным правилам. Эти правила указывают «права и обязанности» учеников, а также исход игры – выигрыш или проигрыш каждого из участников в зависимости от сложившейся обстановки.

Современное развитие информационных технологий создало ряд проблем, связанных с информационной безопасностью, которая является острой проблемой для всех объектов, использующих современные технологии информационного обмена.

Как отмечено в [1] сложность задачи защиты информации продиктована трудностью её формализации и антагонистической природой самой проблемы.

Материалы данного учебного пособия направлены на повышение эффективности решения вопросов защиты информации обучающимися путём применения методов теории игр.

В пособии рассматриваются различные фазы профессиональной деятельности специалиста в области защиты информации такие как построение моделей информационного обмена, анализ злоумышленных деструктивных воздействий на сети и системы, а также некоторые методы выбора и построения оптимальных комплексных систем защиты информации.

1. Методы тории игр в задачах защиты информации

1.1.Игровые и топологические модели информационной безопасности системы и сетей.

Современные информационные системы представляют собой сложные иерархические системы. Они обеспечивают функционирование всех составляющих взаимодействия государств, организаций, предприятий и физических лиц. Фактически они являются надгосударственной структурой, средством взаимодействия глобального уровня (Интернет и поддерживающие его технические и программные средства). В этой связи мировое сообщество заинтересовано в устойчивости и безопасности этих систем.

Информационные сети можно рассматривать на различных уровнях и в зависимости от поставленных задач. Рассмотрим некоторые из таких проблем.

1. *Надежность и живучесть.* Предполагается, что при нарушениях инфраструктуры системы способны выполнять свои функции, хотя и с потерей качества или с задержками (потеря части информации). Задачи решаются несколькими способами:

а) дублирование оборудования и каналов связи. Особенно эффективно действует на верхних уровнях с большими потоками информации. Например, магистральные линии связи дублируются на разных уровнях;

б) наиболее эффективные в настоящее время оптоволоконные линии связи дублируются дополнительными, включая прокладку кабелей по тем же трассам. Как вариант, прокладывают кабели по другим местам (это дороже);

в) используется избыточность на локальном уровне. Например, все АТС связаны между собой по технологии «каждый с каждым». С точки зрения теории графов используется полный граф, в котором потеря связи по одному из каналов не влияет на качество взаимодействия. Это дорого, поэтому используются промежуточные варианты. Это и является предметом прикладной науки;

г) используются технологии перехода на другие типы каналов связи. Кроме магистральных линий связи применяются радиоканальные системы, причем они могут быть по крайней мере трех типов, в зависимости от диапазона использования: ближнего действия (УКВ-диапазон), глобального наземного действия (КВ-связь), космическая связь. В настоящее время наиболее прогрессивными являются технологии Wi-Fi и Wi-Max. Они позволяют дополнять имеющиеся пробелы в связи существующими линиями связи. Вместе с тем появляются проблемы разделения каналов как по частоте, так и по времени, а также районирования, дублирования каналов.

2. *Обеспечение качества связи*. Понятие качества связи определяется международными стандартами QoS [2] и включает в себя множество разноплановых характеристик: разборчивость и узнаваемость клиентов связи, уровень помехоустойчивости, задержки взаимодействия, потери информации. Повышенное качество связи возможно с использованием мероприятий, приведенных в предыдущем пункте. Кроме того, существующие технологии

цифровых взаимодействий основаны на пакетной передаче информации сетевого уровня. Главными технологиями цифровых взаимодействий являются протоколы IP, причем в настоящее время используются два протокола, IPv4 и IPv6, ориентированные на 32- и 64-разрядные микропроцессоры. К сожалению, в России не предусмотрен переход на новые технологии в рамках государства вследствие недостаточного финансирования на государственном уровне.

Те не менее существующие протоколы взаимодействия ориентированы в основном на один критерий - увеличение потоков информации при существующих ограничениях на существующие каналы связи и их пропускную способность. Протоколы уровней IP и TSP рассчитаны в основном на повторную передачу пакетов при их неполучении приемником или промежуточным коммутационным пунктом, что загружает коммутационное оборудование и приводит к дополнительным задержкам связи. Корректирующие коды используются только на обнаружение, но не на исправление ошибок, причем в качестве корректирующего кода использован только один, принятый за стандартный.

Разгрузка каналов связи использованием других корректирующих кодов и методов декодирования также может быть предметом исследования. Кроме того, появляются задачи синхронизации пакетов при передаче на высокоскоростные каналы уровней SDH и ATM.

3. *Оптимизация трафиков*. Задачу можно назвать *информационной логистикой*. Сформулируем ее следующим образом. Существует сеть клиентов, связанных между собой каналами связи и взаимодействующих между собой в реальном времени. Основные ресурсы -запасы информации в пунктах сети, способы взаимодействия по каналам связи - определяются топологией сети и потоками информации по этим каналам. Необходимо оптимизировать сеть по одному из существующих критериев взаимодействия и при наличии ограничений.

Логистические задачи такого уровня достаточно новы и перспективны. Возможные ограничения - допустимые потоки информации по каналам связи, уровни помех и потерь информации, время задержки, стоимость взаимодействия. Критерии оптимизации - минимум затрат, минимум времени задержки или потерь информации, максимум потоков информации, минимум времени обслуживания и т. д.

Логистические задачи часто сводятся к топологическим (графовым), когда пространство взаимодействия представляется в виде графа или соответствующих ему матриц. Предложенные методы решения и оптимизации таких задач [2, 3] допускают расширение и модернизацию.

4. *Информационная безопасность* — это емкое и многогранное направление, включающее в себя конфиденциальность взаимодействий, обеспечение целостности и отсутствие информационных нарушений. Несмотря на множество технологий и способов защиты информации в этой области существует

множество проблем. Часто они связаны с политическими вопросами, которые затрагивают государственные интересы или вопросы экономической и нравственной этики. Существует конкуренция на различных уровнях. Бороться за информационную безопасность в таких условиях достаточно проблематично.

Несмотря на многообразие технологий и топологий информационных систем и сетей возможно решение множества частных задач, решающих изложенные выше проблемы.

Авторами предложена и доведена до практического применения методика анализа и компьютерного моделирования, основанная на комбинированном применении аппарата теории игр и теории графов. Для конкретизации методики разделим структуру информационных систем на три уровня: глобальный, корпоративный и местный.

Информационные системы и сети местного уровня представляют собой локальные информационные системы, оказывающие информационные услуги частным клиентам. Это прежде всего домашние компьютерные сети, имеющие территориальную ориентацию. Они относятся к классу услуг под названием «мультисервис» и включают в себя цифровые телефонию, телевидение и Интернет. Программное обеспечение, оборудование и способы подключения разработаны достаточно детально и успешно функционируют.

Как правило, домовые сети имеют одну точку сопряжения с выходом на местного провайдера через оптоволокно или радиоканал. Местные пользователи подключаются в основном по схеме «звезда», т. е. не влияют друг на друга.

Более сложную топологию имеют информационные сети предприятий, тоже входящие в сети местного уровня. Они имеют достаточно большое количество внутренних взаимодействий (службы, отделы, подразделения), и топология их связей может иметь достаточно сложный характер, как и типы каналов связи.

Корпоративные информационные сети и системы имеют развитую инфраструктуру и топологию. Их главный приоритет - надежность, поэтому топология таких систем приближается к полному графу (соединения типа «каждый с каждым»). Вторая по важности задача -наполняемость сети взаимодействиями, так как клиенты расплачиваются за трафик. На этом уровне наиболее плодотворны задачи логистики, поскольку здесь приоритет имеет тарификация. Оптимизация информационных потоков по критерию максимума прибыли является первоочередной задачей.

Наконец, на верхнем, глобальном уровне также имеет место задача информационной логистики. Проблема живучести приоритетна, и здесь она решается достаточно плодотворно и профессионально.

Приведем некоторые количественные оценки информационных взаимодействий. Прежде всего зададимся величиной *суммарной информационной емкости* $W_{\text{сум}}$ — общего объема памяти:

$$W_{\text{сум}} = \sum_{I=1}^{N} W_I, \tag{1.1}$$

где W_I — емкость I-го элемента памяти; N — количество рассматриваемых объектов взаимодействия. Объемом памяти самих каналов связи можно пренебречь.

Объем фактического информационного ресурса $U_{\text{сум}}$ — это фактический объем информации, находящейся в системе, хранящейся в памяти и передаваемей:

$$U_{\text{сум}} = \sum_{I=1}^{N} U_I. \quad (1.2)$$

Понятно, что $U_{\text{сум}} < W_{\text{сум}}$, причем можно ввести *коэффициент заполнения* $\alpha = U_{\text{сум}}/W_{\text{сум}}$, лежащий в пределах от 0 до 1.

Суммарный трафик $L_{\text{сум}}$ — это общий объем передаваемой информации. Естественно, это функция времени

$$L_{\text{сум}}(t) = \sum_{I=1}^{N} L_I. \quad (1.3)$$

Другие количественные оценки могут быть распространены для решения конкретных сетевых задач. Для их конкретизации рассмотрим простейшую топологию информационной системы, приведённую в виде графа на рис. 1.1. Здесь вершины соответствуют конкретным объектам сети, ребра представляют физические взаимодействия (например, физические линии связи), коэффициенты a_{IJ} (весовые коэффициенты) определяют количественные оценки взаимодействий.

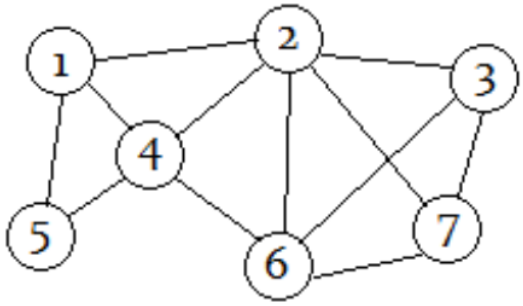

Рис. 1.1 - Граф взаимодействий информационной сети

Приведенный граф может быть применен для любого сегмента информационной трёхуровневой системы и может быть распространен на любую типичную топологию (звезда, дерево, линия, их комбинации).

Плоский граф взаимодействий описывает физические взаимодействия информационной системы в рамках общепринятой модели семейства стандартов

OSI / ISO и родственных им международных рекомендаций. На этой модели можно вводить количественные оценки в зависимости от класса решаемых задач.

Любой плоский граф может быть представлен соответствующей матрицей. Если граф *невзвешенный* [3], то его ребра определяют лишь отношения смежности (если связь между вершинами есть, то $a_{IJ} = 1$, если нет, $a_{IJ} = 0$).

Взвешенный граф имеет возможность варьировать коэффициентами a_{IJ}, причем в зависимости от типа решаемой задачи есть возможность конкретно численно описывать коэффициенты a_{IJ}.

Стратегии защиты информации принципиально зависят от времени суток, дня недели, месяца и т. д. Приведенные задачи могут быть *динамическими*, т. е. могут включать в себя зависимость от этих величин. В таких случаях перечисленные выше величины являются функциями времени.

Приведем некоторые из типичных задач информационных взаимодействий.

1. Задача оптимизации загрузки сети по критерию максимума трафика. Здесь коэффициенты $a_{IJ}(t)$ в зависимости от типа решаемой задачи могут представлять собой

- максимально возможную загрузку данного сегмента сети, например, в Мбит/с;
- стоимость соединения во времени (тарифы услуг зависят и от времени суток, и от дня недели, и от выбранного провайдера);
- вероятности нарушения информации, включая ее потерю или другие ущербы;
- риски клиентов сети в любом варианте (условные вероятности, стоимость, относительные величины).

Сами оценки в прямом измерении могут быть неименованными (кроме зависимости от времени), важно их соотношение с другими вариантами переходов на графе.

2. Задача оптимизации сети по критерию максимальной рентабельности. Коэффициенты $a_{IJ}(t)$ могут иметь те же подсистемы, что и в предыдущем случае. Такие задачи обычно ставятся на двух верхних уровнях.

Рассмотрим более подробно модель описания информационной сети в топологическом пространстве, т. е. с учетом информационных взаимодействий клиентов. Возможны несколько уровней взаимодействия. Первый — непосредственное взаимодействие: после подключения клиент *I* непосредственно подключается к клиенту *J*. В таком варианте коэффициенты $a_{IJ}(t)$ представляют собой стоимость трафика и могут быть представлены в виде обычной двумерной матрицы, в которой они могут иметь, например, одну из перечисленных выше оценок. Вид матрицы представлен на рис. 1.2.

Не обращаясь к деталям получения коэффициентов $a_{IJ}(t)$, отметим возможные пути решения оптимизации трафика, для чего привлечем некоторые определения из теории взвешенных графов [4].

Вес дуги $C_{IJ}(t)$ — количественная оценка перехода по графу из вершины *I* в вершину *J*. В отличие от количественной оценки $a_{IJ}(t)$ может включать в себя множители $R_{IJ}(t)$, которые можно считать *весовыми коэффициентами*, в результате чего матрица, представленная на рис. 1.2, приобретает аналогичный вид, но с коэффициентами $C_{IJ}(t)$:

$$C_{IJ}(t) = R_{IJ} \cdot a_{IJ}(t). \quad (1.4)$$

Отметим, что если между вершинами дуга отсутствует, то коэффициент $C_{IJ}(t) = \infty$.

$$\begin{vmatrix} \alpha_{11}(t) & \alpha_{12}(t) \ldots\ldots\ldots\ldots\ldots & \alpha_{1n}(t) \\ \alpha_{21}(t) & \alpha_{22}(t) \ldots\ldots\ldots\ldots\ldots & \alpha_{2n}(t) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & & \\ \alpha_{n1}(t) & \alpha_{n2}(t) \ldots\ldots\ldots\ldots\ldots & \alpha_{nn}(t) \end{vmatrix}$$

Рис. 1.2 - Матрица информационных взаимодействий

Маршрут на графе — связная последовательность вершин и соединяющих их ребер. Маршрут всегда конечен, т. е. начинается и заканчивается за конечное число шагов (дуг). В этой связи появляется оценка *«вес маршрута»*:

$$S_Q(t) = \sum_{I=1}^{Q} C_{IJ}(t), \quad (1.5)$$

где *Q* — *длина маршрута*, т. е. количество входящих в него дуг.

Вес вершины графа $M_I(t)$ - сумма весов дуг, инцидентных данной вершине:

$$M_I(t) = \sum_{I=1}^{F} C_{IJ}(t), \quad (1.6)$$

где *F* - количество инцидентных дуг.

Минимальный маршрут $S_{QIJ\ min}(t)$ - маршрут, имеющий минимальный вес. Предполагается, что между вершинами *I* и *J* существует несколько маршрутов с различными весами $S_Q(t)$, причем минимальным считается маршрут с наименьшим весом:

$$S_{QIJ\ min}(t) = min_g \cdot S_{QIJ}(t), \quad (1.7)$$

где *g* - текущий номер маршрута.

Задачи такого типа решаются в теории игр и носят название минимаксных [5].

Авторами выполнен достаточно большой объем работ, связанных с количественным описанием информационной безопасности и оперативного мониторинга реальных компьютерных сетей, в том числе с использованием

описанного математического аппарата. Полученные результаты позволили упростить политику управления информационной безопасностью.

1.2. Методы теории игр для решения задач безопасности средств вычислительной техники.

Развитие современных сетевых технологий сопровождается повышением требований к обеспечению приватности обработки информации и, как следствие, предполагает существенную модернизацию нормативно-методологической базы и стандартов управления информационной безопасностью. Между тем в этих документах отмечается, что в ряде случаев методы управления системами защиты информации, ориентированные на применение количественных оценок, все еще не имеют достаточно развитого математического аппарата для их обоснования. В работах [6] прослеживается тенденция расширения имеющихся математических подходов к обоснованию параметров систем защиты за счет применения методов теории игр к решению задач обеспечения безопасности сетевых технологий, в том числе управления информационной безопасностью. Применяемые теоретико-игровые подходы к решению задач информационной безопасности условно можно разделить на 2 класса: один класс (обозначим А) описывает взаимодействие «нападение – защита», предсказывая действия нападающих и определяя ответные действия защиты; второй (В) позволяет получать количественные оценки уровня защиты информационной системы путем предсказания действий нападающих и защиты.

В классе А можно выделить два подкласса игр – А1 и А2: игры подкласса А1 позволяют исследовать взаимодействие «нападение – защита» в общих случаях (игры обычно ведутся двумя игроками – «нападающим» и «защищающимся», и у каждого из них имеются всего по два возможных действия: {«нападать», «не осуществлять никаких действий»} и {«защищаться», «не осуществлять никаких действий»} соответственно); в подклассе А2 рассматриваются более сложные сценарии нападения и защиты, специализированные под конкретные ситуационные параметры (примером таких параметров могут быть свойства сети, в которой осуществляется взаимодействие). Игры подкласса А1 часто являются статическими играми с двумя игроками, или Байесовскими играми, которые хорошо исследованы в «классической» теории игр, и поэтому результаты игры относительно просто получить. Преимущества игр подкласса А2 в их большей реалистичности и лучшем описании динамики взаимодействия «нападающего» и «защищающегося», но получение выводов о «правильном» поведении участников требует значительных объемов вычислений, а решение в ряде случаев может не обладать достаточной точностью.

Многие подходы к оценке уровня информационной безопасности (например, риск- ориентированные, то есть применяющие понятие риска как метрику) используют в качестве входных данных предполагаемые стратегии нападающей и защищающейся сторон. Совмещение идей таких подходов с известными теоретико-игровыми методами привело к появлению класса В игр информационной безопасности, ориентированных на получение оценок и анализ уровня защищенности компьютерных систем. К этому классу, например,

относится модель, описывающая, как инвестиции в обеспечение информационной безопасности одной организации могут влиять на безопасность других организаций. В терминах риска можно говорить о том, что такие инвестиции косвенно повышают безопасность других организаций в случае наличия общей сети у этих организаций или, наоборот, снижают чужую безопасность в силу снижения интереса злоумышленников к инвестирующей организации и последующего повышения его к другим организациям. Среди других моделей класса В представляет интерес более глубокое исследование кооперативной игры защищающихся организаций. Под оптимальностью здесь понимается условие, что любая пара уже сформированных коалиций имеет больше позитивных и меньше негативных эффектов, чем в ситуации, когда они создадут одну общую коалицию. Взаимовлияние классов теоретико-игровых моделей информационной безопасности представлено на рис. 1.3.

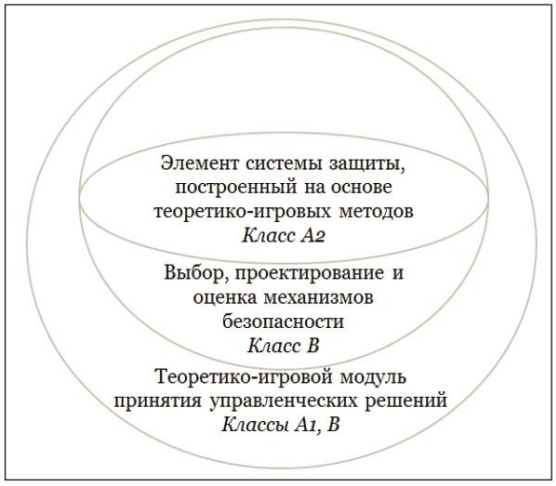

Рис. 1.3. Иерархия классов теоретико-игровых моделей информационной безопасности

Теоретико-игровые методы нашли широкое применение в задачах проектирования систем обнаружения вторжений (СОВ). При этом вопросы противодействия атакам, направленным на саму СОВ, не получили должного исследования с позиции теории игр. В настоящее время к таким атакам относят: сверхстимуляцию – создание большого количества паттернов, генерирующих ложные сигналы системы обнаружения вторжений, что приводит к перегрузке обработчиков событий; DoS-атаку на перегрузку сенсоров или замедление алгоритма, проверяющего паттерны.

Остановимся на узловых системах обнаружения вторжений (пример – BlueBoX). Пусть Ω – множество наблюдаемых объектов, каждому из которых сопоставлено множество отслеживаемых параметров $I_{\omega\in\Omega}$.

Будем рассматривать следующее взаимодействие узловой СОВ и атакующего. Каждую атаку представим в виде некоторой последовательности шагов. Каждый

шаг порождает некоторый вид активности, обнаруживаемый СОВ. После первой активности, которую СОВ распознала как подозрительную, осуществляется попытка предсказать последующие шаги предполагаемого злоумышленника и расширяется множество $I_{\omega\in\Omega}$ наблюдаемых параметров. Далее СОВ наблюдает расширенный список параметров в течение некоторого периода времени t_m. Обозначим $J_{\omega\in\Omega}$ множество дополнительных параметров наблюдения. До выявления подозрительной активности система обнаружения вторжений наблюдает базовый набор критических параметров. Очевидно, что в это время цена системных ресурсов постоянна. Обозначим $S(t)$ – цену дополнительных ресурсов, затрачиваемых на мониторинг множества $J_{\omega\in\Omega}$. Для простоты будем предполагать, что $S(t)$ линейно зависит от t, то есть

$$S(t) = \sum_{\omega\in\Omega}\sum_{j\in J} s(\omega, j, t) = fkt, \tag{1.8}$$

где f – средний весовой коэффициент, определяющий цену одного наблюдаемого параметра, k – количество наблюдаемых пар «объект – параметр».

Для анализа стратегий СОВ и атакующего и оценки эффективности процесса мониторинга рассмотрим некооперативную теоретико-игровую модель с ненулевой суммой и несколькими итерациями. Количество итераций зависит от количества шагов атаки. Предполагается, что СОВ и атакующий взаимно знают стратегии и функции полезности друг друга. Когда СОВ обнаруживает подозрительную активность, она может решить проигнорировать ее или же усилить мониторинг.

В последнем случае количество наблюдаемых параметров будет увеличено. Время мониторинга для дополнительных параметров будет выбрано из информационной базы СОВ согласно сценарию атаки. Атакующий формирует свою стратегию на основе следующего множества действий: {«завершить атаку»; «продолжить без паузы»; «сделать паузу на некоторый период времени»}. Для иллюстрации игры будем использовать несколько типичных периодов подобных пауз.

В случае если узловая СОВ обнаруживает атаку или же злоумышленник решает прекратить нападение, выигрыш для системы обнаружения атаки будет α. В противном случае его значением будет –α.

Атакующий может принадлежать одному из двух типов в зависимости от своих целей: проведение атаки на защищаемую систему или же на саму СОВ.

Первый тип атакующих получает выигрыш β в случае успешной атаки, иначе –β. Обозначим $Z(t)$ – стоимость паузы для атакующего, которую, так же, как и в случае с СОВ, для простоты примем линейно зависящей от времени:

$$Z(t) = gt, \tag{1.10}$$

где g – весовой коэффициент, определяющий стоимость единичного периода паузы.

Таким образом, функция полезности для первого типа нападающих будет:

$$U_{at} = \begin{cases} 0, & NA, \\ \beta - R(t_a), & 0 \le t_m \le t_a, \\ -\beta - R(t_a), & 0 \le t_m \le t_a, \end{cases} \quad (1.10)$$

где t_a – пауза между действиями нападающего, *NA* здесь и далее обозначает выбор злоумышленника завершить атаку.

Соответствующая первому типу атакующих функция полезности СОВ имеет вид

$$U_{mon}^{1} = \begin{cases} \alpha - R(t_m), & 0 \le t_a < t_m, NA, \\ -\alpha - R(t_m), & 0 \le t_m < t_a. \end{cases} \quad (1.11)$$

Для второго типа нападающих примем, что n – количество генерируемых нападающим паттернов. Так как предполагается, что с увеличением количества наблюдаемых объектов и времени их мониторинга, а также величины n вероятность определить тип нападающего возрастает, примем, что если n меньше некоторой величины, зависящей от t_m и k , то атака проходит успешно:

$$U_{ov} = \begin{cases} 0, & NA, \\ \beta + f(n+k)t_m, & n < F(t_m k), \\ -\beta, & n \ge F(t_m k). \end{cases} \quad (1.12)$$

Функция $F(t_m k) = \frac{N}{l^{k t_m}}$ будет использована для упрощения последующих вычислений, где N и l – числовые параметры, задаваемые начальным состоянием системы и особенностями реализации системы обнаружения вторжений. Соответствующая второму типу функция полезности СОВ:

$$U_{mon}^{2} = \begin{cases} \alpha - f(n+k)t_m, & n \ge F(t_m k), NA, \\ -\alpha - f(n+k)t_m, & n < F(t_m k). \end{cases} \quad (1.13)$$

Эта игра не может быть решена с использованием чистых стратегий, поэтому решение будет представлено в смешанных стратегиях. Ожидаемой выплатой для узловой СОВ будет

$$U_T = \sum_a \sum_b U_{mon}(a,b) p(a) p(b), \quad (1.14)$$

где $U_{mon}(a,b)$ – выплата СОВ, когда игроки выбирают стратегии a и b , а $p(a)$ и $q(b)$ – вероятности выбора этих стратегий СОВ и атакующим соответственно.

Для вычисления равновесия Нэша используем Gambit [7]. Рассмотрим пример того, как работает наша модель. СОВ будет осуществлять выбор на множестве из четырех действий: {$a1$ = «игнорировать», $a2$ = «увеличить количество наблюдаемых пар “объект – параметр” на 50, время мониторинга на 100 с», $a3$ = «увеличить количество пар на 100, время мониторинга на 500 с», a_4 = «увеличить количество пар на 200, время мониторинга на 1500 с»}. Атакующий выбирает на множестве: {b_1 = «завершить нападение»,b_2= «продолжить атаку на защищаемый объект без паузы», b_3 = «сделать паузу на 400 с и продолжить атаку на защищаемый объект», b_4 = «сделать паузу на 1000 с и продолжить атаку на защищаемый объект», b_5 = «сформировать 10 паттернов для атаки на СОВ», b_6 = «сформировать 1000 паттернов для атаки на СОВ»}. Кроме того, примем N = 2000, α = 5000, β = 2000 и l =1,0001. В таблице 1.1 представлены результаты одного раунда. Таблицы 1.2 и 1.3 показывают стратегии игроков.

Таблица 1.1. Результаты первой итерации игры

	a_1	a_2	a_3	a_4
b_1	0; 5000	0; 4950	0; 4500	0; 2000
b_2	2000; -5000	-2000; 4950	-2000; 4500	-2000; 2000
b_3	1800; -5000	1800; -5050	-2200; 4500	-2200; 2000
b_4	1500; -5000	1500; -5050	1500; -5500	-2500; 2000
b_5	2000; -5000	2060; -5060	2550; -5550	-2000; 1985
b_6	2000; -5000	3050; -6050	-2000; 4450	-2000; 1985

Таблица 1.2. Стратегия атакующего

b_1	b_2	b_3	b_4	b_5	b_6	Ожидаемая полезность
0.6995816	0.02153313	0.0	0.0	0.2490239	0.02986128	0.0
0.6995493	0.0	0.0	0.0	0.2489484	0.05150225	0.0
0.6995799	0.02040104	0.0	0.0	0.2800189	0.0	0.0
0.6995493	0.0	0.0	0.0	0.3004506	0.0	0.0

Таблица 1.3. Стратегия СОВ

a_1	a_2	a_3	a_4	Ожидаемая полезность
0.5	0.0	0.0	0.5	1995.81672214
0.5	0.0	0.0	0.5	1995.49323986
0.5	0.0	0.0	0.5	1995.79971523
0.5	0.0	0.0	0.5	1995.49323986

В частности, из представленных таблиц видно, что в рассмотренном примере системе обнаружения вторжений следует выбирать с одинаковой вероятностью стратегии a_1 и a_4. В этом случае выплаты игроков будут 1995 и 0 для СОВ и атакующего соответственно.

В процессе тестирования модели была создана база знаний СОВ, состоящая из 10 сценариев атаки. Стратегии, основанные на ней, отличаются друг от друга как объектами и параметрами

для мониторинга, так и значением t_m . Каждый сценарий был реализован 100 раз, и результаты отражают средние значения цены и процента обнаружения. Действия СОВ и атакующего выбирались согласно равновесию Нэша. Одновременно в целях сравнения для каждого сценария был подсчитан соответствующий объем ресурсов для традиционной реализации СОВ, обладающей 95-процентной точностью.

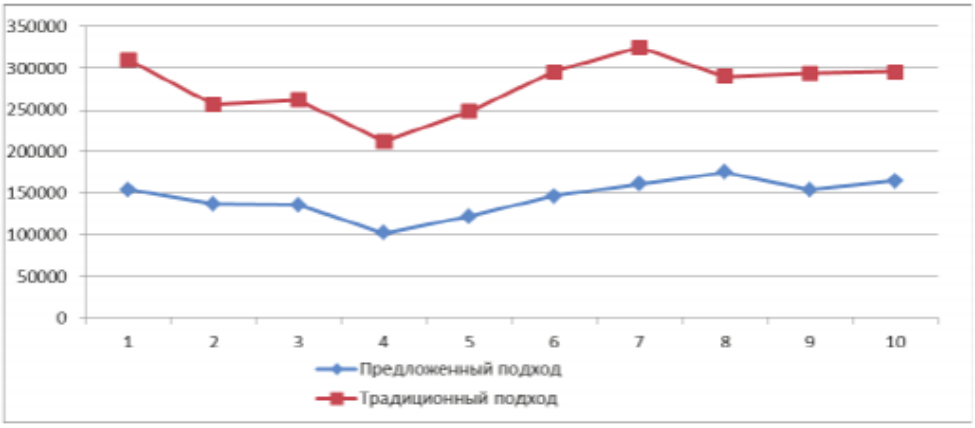

Рис. 1.4 Ценовое сравнение подходов

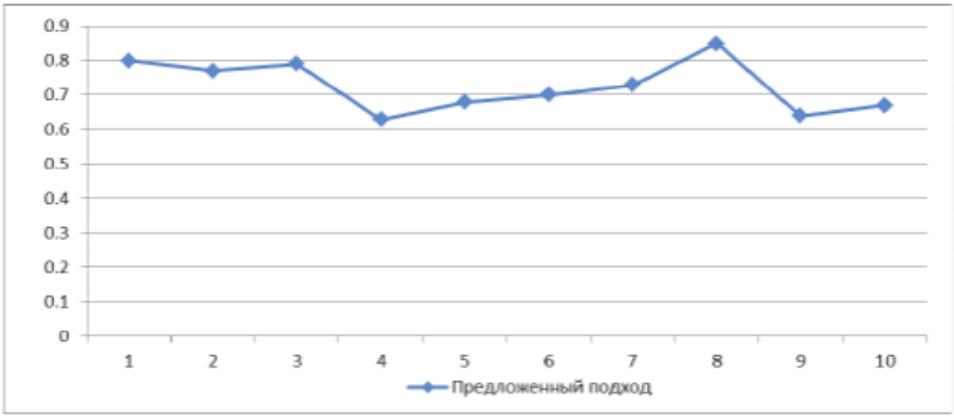

Рис. 1.5 Точность обнаружения предложенного подхода

Результаты представлены на рис. 1.4 и 1.5 Как можно заметить, количество необходимых ресурсов, требуемых для традиционной реализации, во много раз выше предложенного подхода. С другой стороны, точность обнаружения незначительно уступает нормальной реализации, но, тем не менее, оставляет возможным использование подобной теоретико-игровой оптимизации в системах с ограниченными ресурсами.

1.3.Игровой подход к нахождению уязвимостей и оценке рисков в информационных сетях.

Ключевыми задачами при управлении информационной безопасностью (ИБ) [7] являются идентификация угроз, уязвимостей, рисков и их оценка. Важность этих задач обусловлена тем, что результаты их решения служат входными данными для выбора контрмер по обработке рисков. Без объективной оценки рисков нельзя достичь адекватного уровня безопасности и удовлетворить требования безопасности. В литературе [8] упоминается 2 подхода к оценке рисков: качественный и количественный. В рамках сертификации CISSP[3] предлагается количественно оценивать риск, как ожидаемые потери R= L*P , где L- оценка денежных потерь при осуществлении угрозы, P- оценка вероятности осуществления угрозы. При этом в CISSP утверждается, что количественный подход к оценке рисков - это дорогой, сложный процесс, требующий больших затрат человеческих ресурсов и времени.

Например, в данной статье предлагается подход на основе теоретико-игрового понятия ожидаемой полезности и ориентированных графов. Данный подход позволяет автоматизировать процесс оценки рисков и обнаружения наиболее уязвимых мест в системе. Также он позволяет оценивать эффект от различных мер по обработке рисков. Рассмотрим алгоритм информационного поиска A*. Преимуществом предлагаемого подхода по отношению к существующим (напр. Моделирование ИБ на основе байесовских сетей) является вычислительная эффективность, что позволяет применять подход к моделям с большим количеством элементов, и простота задания параметров модели экспертом.

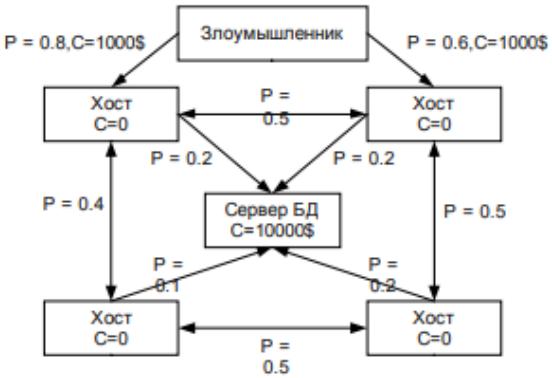

Рис 1.6. Модель информационной системы на основе циклического графа

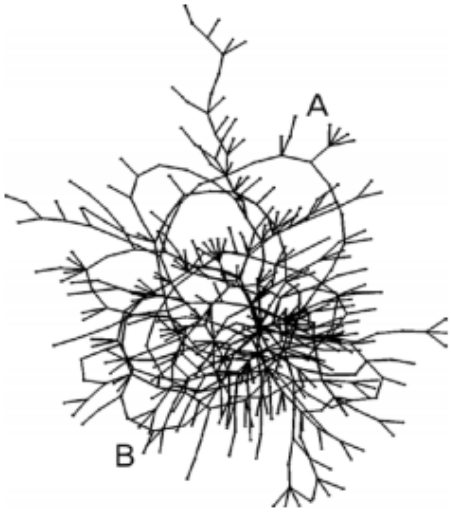

Рис 1.7. Модель широкомасштабной сети на основе случайного графа

Под оптимальностью далее понимается максимизация ожидаемой полезности, т.е. U= M [G− C] , где G – полученная выгода, C – цена, затраченная на проведение атаки, M — математическое ожидание указанной случайной величины.

Рассмотрим на примере (см. рис. 1.8), как можно посчитать это значение для пути из вершины 1 в вершину 4.

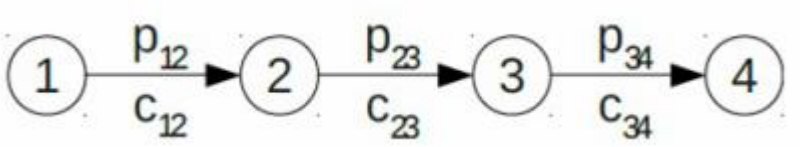

Рис. 1.8 Пример вычисления стоимости некоторого пути

Допустим атака начинается из вершины 1. Предпринимаем атаку на вершину 2 и платим за неё цену c12, с вероятностью p12 мы получаем награду c2, далее платим c23 за атаку и т.д. Получаем

$$u(v_1 \dots v_4) = c_1 - c_{12} + p_{12}(c_2 - c_{23} + p_{23}(c_3 - c_{34} + p_{34}\, c_4))$$

Или, обобщая,

$$u(v_1 \dots v_n) = c_1 - c_{12} + p_{12} u(v_2 \dots v_4)$$
$$u(v_i\, v_i) = c_i\,, \qquad (1.15)$$

Заметим, в общем случае может существовать несколько рёбер (т. е. несколько атак) между вершинами, петли и циклы. На вершинах определены премии c_i за компрометацию вершины.

На рёбрах определены цены c_{ij} атаки по ребру. Следующим моментом, который необходимо обсудить для уточнения модели, является работа с рёбрами относительно времени. Возможны следующие варианты:

1. выбираем 1 атакуемое ребро на каждом шаге, т.е. осуществляем атаки последовательно;
2. выбираем K атакуемых рёбер на шаге, число K позволяет моделировать доступные нам ресурсы;
3. все рёбра обрабатываются одновременно, при этом каждой вершине сопоставлено некоторое состояние в текущий момент времени. Это наиболее общий случай.

В наиболее общей постановке задача сложна с вычислительной точки зрения, т.к. за счёт циклов может потребоваться большое количество итераций до наступления состояния равновесия. По структуре она аналогична задаче моделирования работы многослойной нейронной сети с обратными связями (либо цепи Маркова).

Далее рассмотрим частный случай, где отсутствуют циклы и выбирается 1 ребро за шаг.

Поиск оптимальной атаки

К сожалению, введённый функционал качества (1.15) не обладает свойством оптимальности подзадач, т.е. путь в графе, максимизирующий эту функцию, не обязательно состоит из подпутей, так же максимизирующих её. Проще всего это видеть на примере (см. рис. 1.9).

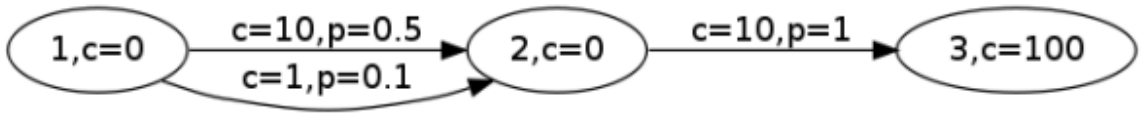

Рис. 1.9 Пример нарушающий свойство оптимальности подзадач

Из 1 в 3 есть 2 пути, цена первого: -10+0,5 (-10+100)=35, цена второго: -1+0,1(-10+100) = 8. Первый путь лучше, однако он содержит путь из 1 в 2, который не является локально оптимальным.

Из-за этого быстрые алгоритмы, базирующиеся на динамическом программировании (алгоритмы Дейкстры, Беллмана), оказываются неприменимы.

С другой стороны, полный перебор всех возможных путей невозможен, т.к. их может быть экспоненциальное число от количества вершин входного графа.

Если ввести подходящую эвристику, то эту проблему можно решить, применяя метод информированного поиска по алгоритму SMA* (Simplified Memory-bounded A*)[9].

В качестве эвристики для оценки функционала качества пути между вершинами v1 и vn возьмём сумму неотрицательных цен вершин и рёбер на пути.

$$\hat{u}(v_1 \dots v_n) = \max(c_n, 0) + \sum_{i=1}^{n-1} (\max(c_i, 0) + \max(-c_{i,i+1}, 0)) \quad (1.16)$$

Если предположить неотрицательность цен вершин (т. е. нас не штрафуют за компрометацию вершины) и рёбер (т. е. мы не получаем выгоду за сам факт атаки), то выражение (3) можно упростить до суммы цен вершин на пути:

$$\hat{u}(v_1 \dots v_n) = \sum_{i=1}^{n} c_i \quad (1.17)$$

Однако, сделанные такие предположения существенно ограничивают применимость модели, поэтому далее мы будем пользоваться выражением (2).

Эвристика (1.16) не занижает стоимость пути, следовательно является допустимой. Также (1.16) удовлетворяет неравенству треугольника $\hat{u}(v_1 \dots v_n) \leq \hat{u}(v_n \dots v_k) + \hat{u}(v_1 \dots v_k)$, где v_k потомок v_n, следовательно является преемственной. В соответствии с [9], поиск A* на основе такой эвристики является полным и оптимальным.

Чтобы вычислить значения эвристики во всех вершинах, можно использовать алгоритм Беллмана-Форда.

Далее обозначим $h(x) = \hat{u}(v_1, \dots, v_n - 1, x)$ – оценка цены пути из текущего состояния x в целевое (1.16), g(x) - цена достижения состояния x из начального

(1.15). f(x) = g(x) + h(x) – оценка стоимости достижения целевого состояния по пути через вершину x.

Алгоритм: *нахождение оптимального пути*
Вход: *Граф G, начальный узел start, конечный узел end*
Выход: *оптимальный путь*
O = множество рассмотренных путей
n = количество рассмотренный путей
поместить start в O
n := 1
цикл:
находим наиболее перспективный узел из уже рассмотренных
best := argmax {x из O | f(x)}
если best = end, то завершить вернув best
next := следующий возможный узел в пути best
f(next) := min(f(best), g(next) + h(next))
если просмотрены все потомки узла best, то backup(best)
если все потомки best в памяти, то удалить best из O
n := n + 1
если n > maxN то
удалить наименее глубокий узел с мин. значением f из O
удалить этот узел из списка последующих узлов для его родителя
добавить его родителя в O, если необходимо.
n := n — 1
добавить next в O

function backup(n):
если n полностью обработан и имеет родительский узел, то
f(n) := argmax {x потомок n | f(x)}
если f(n) изменилось, то backup(parent(n))

Результатом предложенного подхода является наиболее привлекательный для злоумышленника путь атаки на рассматриваемую информационную систему (в предположении, что используемые нами оценки выгоды и затрат совпадают с используемыми злоумышленником). Это позволяет, во-первых, выявить наиболее слабое место в системе, вовторых, зная путь можно перемножить вероятности реализации угроз, соответствующих рёбрам пути, и получить вероятность реализации данной атаки для её дальнейшего использования в количественных методах оценки риска.

Поиск атаки при ограниченном количестве ресурсов

В предыдущем разделе была рассмотрена задача поиска оптимальной атаки на заданный объект в системе. Сейчас рассмотрим, как можно использовать предложенный подход для оценки вероятности атаки на систему, когда целевой объект атаки неизвестен, при условии, что ресурсы злоумышленника

ограничены некоторым известным значением (предполагаем, что это значение входит в используемую модель нарушителя).

В данном случае, задачей злоумышленника является не выбор оптимального пути к целевой вершине, а выбор такого подмножества рёбер и вершин, содержащего заданную начальную вершину, что ожидаемая полезность максимальна.

Рассмотрим для каждой вершины 2 числа: c_i — математическое ожидание цены пути, ведущего от начальной вершины в данную, g_i — мат. ожидание выгоды этого пути (т.е. ожидаемая полезность, рассмотренная ранее, разделяется на 2 части).

Данная задача может быть сведена к задаче о рюкзаке (knapsack problem), если рассмотреть c_i как вес предмета, а g_i как цену предмета. Известно, что задача о рюкзаке является NP-полной, однако, если предположить, что веса целочисленные, то она допускает точное псевдо-полиномиальное решение, с помощью динамического программирования [8], которое на практике работает достаточно хорошо.

Однако это решение не будет точным для рассматриваемой задачи, т. к. после выбора одного пути цены других изменяются за счёт возможности повторно использовать выбранный путь. Так что решение, полученное в результате решения задачи о рюкзаке, переоценивает стоимость проведение атаки.

Для уточнения решения используется следующий подход:

1. Решаем задачу о рюкзаке.
2. Выбираем один из путей в качестве начального, например, максимизируя $g_i - c_i$.
3. Пересчитываем ci и gi для остальных путей, используя в качестве начальной вершины все вершины из выбранного в пункте 2 пути и выбирая оптимальные значения, запоминаем полученный путь.
4. Выбираем следующий путь в пункте 2 из оставшихся и повторяем пункт 3.

В результате такой жадной стратегии, мы получаем более точную оценку стоимости проведения выбранной атаки.

Контрольные вопросы:

1. *Раскройте понятия надежности и живучести информационных систем.*
2. *В чем заключается обеспечение качества информационного обмена?*
3. *Каковы особенности оптимизации тарифов?*
4. *Приведите характеристики плоского графа топологической модели информационной системы.*
5. *Раскройте сущность оптимизации сети по критерию максимума трафика.*
6. *Приведите задачу оптимизации сети по критерию максимальной рентабельности.*
7. *В чем смысл классов теоретико-игровых подходов к задачам информационной безопасности?*
8. *Приведите модель взаимодействия СОВ и атакующего.*
9. *Приведите модель выбора СОВ из 4-х действий.*
10. *Как оценивается функционал качества пути между вершинами?*

2. Методы выбора средств защиты информации

2.1. Модель выбора оборудования интегрированной системы безопасности.

Для поиска наиболее оптимальных стратегий защиты информационных ресурсов можно предложить математическую игру двух сторон, одной из которых является система защиты - ИСБ, а с другой - возможные действия нарушителей. В этом случае выигрыш злоумышленников будет равен проигрышу специалистов по информационной безопасности (ИБ) и можно получить матрицу для игры двух лиц с нулевой суммой. При этом строки Ai(i=1,…,n) некоторой матрицы будут приниматься в качестве стратегий нарушителей, а в качестве стратегий специалистов ИБ - её столбцы Bj(j =1,…, m). К стратегиям нарушителей можно отнести различные типовые сценарии (угрозы) действий нарушителей, которые могут привести к ущербу для Предприятия (несанкционированное проникновение на объект, хищение информации, теракт, пожар и т.д.), к стратегиям специалистов ИБ – различные технические средства охраны, предназначенные для защиты.

Таблица 2.1 - Таблица матричной игры

A_i / B_j		B_1	B_2	. . .	B_m
A_1	$p(x_1)$	a_{11}	a_{12}	. . .	a_{1m}
A_2	$p(x_2)$	a_{21}	a_{22}	. . .	a_{2m}
. . .	. . .	. . .	. . .	. . .	. . .
A_n	$p(x_n)$	a_{n1}	a_{n2}	. . .	a_{nm}

Анализ выбранного оборудования позволяет каждому техническому средству охраны сопоставить возможность и устранить определенные угрозы. Для проведения на компьютере игры надо также знать результаты игры при каждой паре стратегий A_i и B_j (например, a_{ij} - причинённый нарушителем материальный ущерб) и вероятности реализации сценария угрозы нарушителем $p(x_i)$ при выбранной стратегии x_i. Вероятности реализации угроз $p(x_i)$ берутся из сети Интернет, по результатам статистических исследований, используя на кафедре интегрированную систему безопасности «Интеллект». Если вероятности неизвестны, то можно предположить, что все они равновероятны, т. е. $p(x_i)=1/n$. В качестве коэффициентов a_{ij} матрицы игры рассматривать годовые потери для всех вариантов комбинаций $A_i(i= 1, …,n)$ и $B_j(j=1,…,m)$. Для этого сопоставить каждый типовой сценарий действий нарушителей с каждым методом защиты и определить ущерб, который может быть при этом нанесён. Покупка, установка и использование средств защиты требуют дополнительных затрат, что нужно вносить в ущерб при расчётах. Построив игровую матрицу (см. таблица 2.1) и проанализировав её, оцениваются затраты для каждого решения и выбираются наиболее эффективные варианты оборудования для всего диапазона сценариев действий нарушителей. Если построена такая игровая матрица, то наилучшей в условиях имеющейся информации будет стратегия системы защиты

компьютерной информации Bj, при которой будут минимальны средние потери, т. е. будет минимальна сумма:

$$\sum_{i=1}^{n} a_{ij} p(x_i).$$

Для выбора наиболее оптимального набора оборудования в качестве стратегий используются различные сочетания сценариев действий нарушителей и видов оборудования. Прекращение использования или добавление нового средства можно рассматривать как переход от одной стратегии к другой. Поэтому разумное поведение игроков в матричной игре должно основываться на следующих рассуждениях.

Пусть нарушитель выбирает некоторую свою стратегию A_i. Тогда в наихудшем случае (в теории игр игроки предполагаются весьма осторожными и рассчитывают на наименее благоприятный поворот событий; такое положение дел для стратегий нарушителей может наступить, например, в случае, когда стратегия A_i станет известной специалисту ИБ) и он получит выигрыш $\min a_{ij}$. Поэтому нарушитель должен выбрать свою стратегию A_{i0} (см. формулу 1) так, чтобы максимизировать этот свой минимальный выигрыш:

$$\min_j a_{i0j} = \max_i \min_j a_{ij} \qquad (2.1)$$

Значит, стоящий в правой части написанного равенства «максимин» является гарантированным выигрышем нарушителя. Аналогичные рассуждения, проводимые специалистом ИБ, показывают в формуле 2, что он должен выбирать такую свою стратегию B_{j0}, что

$$\min_i a_{ij0} = \min_j \max_i a_{ij} \qquad (2.2)$$

Здесь стоящий справа «минимакс» является тем выигрышем нарушителя, больше которого он при правильных действиях специалиста ИБ получить не может. Поэтому фактический выигрыш нарушителя должен при разумных действиях специалистов ИБ лежать между правыми частями формул (2.1) и (2.2).

Расчет ущерба складывается из величин ущерба D_1, который может быть нанесён при реализации текущей стратегии нарушителем, если система не была защищена от неё техническими средствами охраны из текущей стратегии специалиста ИБ; и из общей стоимости D_2 всех технических средств охраны из текущей стратегии специалиста ИБ. Для подсчета общей стоимости нужных технических средств охраны D_2 сопоставляется текущий набор средств и все имеющиеся средства и суммируются величины стоимости тех средств, которые присутствуют в первом наборе. Подсчет ущерба от реализации угроз D_1

вычисляется в два этапа. Сначала текущая стратегия злоумышленника сопоставляется с каждым из технических средств охраны из текущей стратегии специалиста ИБ, и если средство защищает от каких-то угроз из текущего набора, то данные угрозы удаляются из набора. Сопоставив текущий набор угроз со всеми средствами из текущей стратегии специалиста ИБ, получаем некоторое количество угроз, от которых система в данном случае не защищена. Полученные угрозы нужно сопоставить со всеми имеющимися угрозами и суммировать величины ущерба тех угроз, что присутствуют в полученном наборе. Далее эти две суммы D1 и D2 складываются и получается ущерб при применении текущей пары стратегий нарушителя и специалиста ИБ.

Для вычисления оптимальной стратегии необходимо в качестве основы для расчетов использовать формулу (2.2). Для начала составляется матрица, строками которой являются стратегии нарушителя, а столбцами – стратегии специалиста ИБ. На пересечении стратегий ставятся максимальные величины ущерба, рассчитанные по алгоритму. Таким образом, для каждой стратегии специалиста ИБ вычисляется максимально возможный ущерб. Теперь из всех полученных максимальных величин ущерба выбрать минимальное значение, т.е. min max $\{D_1+D_2\}$. Стратегия, соответствующая данному значению, и будет искомой оптимальной стратегией.

Рекомендуется разработать программу, которая по введённым значениям стоимости оборудования и величины ущерба и в результате применения всех пар угроза-средство защиты вычисляет оптимальный набор из базы технических средств охраны. Результатом вычислений будет комплекс оптимального оборудования для интегрированной системы безопасности, общая стоимость оборудования и максимальный ущерб, который можно получить, при использовании данного комплекса. При выборе оборудования предпочтение отдаётся более дешёвым аналогам. В результате специалист ИБ может сначала получить оптимальный комплекс технических средств охраны, а потом изменять его исходя из величины максимального ущерба. В дальнейшем при подготовки программы желательно применять веб-приложение с использованием HTML, CSS, языка JavaScript, JVM и с возможностью его запуска в браузере. Применение программного продукта и данной модели даст возможность специалисту ИБ выбрать наиболее оптимальный комплекс оборудования для построения на его основе интегрированной системы безопасности объекта информатизации.

2.2 Оптимизация выбора средств защиты информации

Телекоммуникационные системы, активно развивающиеся в последнее время, являются артериями современных глобальных информационных систем. Информация, циркулирующая в таких системах, представляет существенную ценность и поэтому является уязвимой к различного рода нарушениям и злоупотреблениям. Развитие сетевых технологий сопровождается повышением требований к информационной безопасности.

Несмотря на значительные успехи в сфере информационной безопасности, до сих пор существуют трудности предотвращения удаленных атак. Анализ сетевых атак показывает, что действия по защите чаще всего принимаются после того, как уже имеется снижение производительности сервиса. Происходит это вследствие сложности оценивания будущего масштаба атаки и использования соответствующей меры защиты. Некоторые воздействия (например, Бо8-атаки) отличает спонтанный характер, то есть они могут начинаться и закачиваться в случайные моменты времени, что в свою очередь также добавляет сложности выработки своевременной реакции на атаку.

Для выявления фактов неавторизованного доступа в систему, а также для других типов вредоносной активности, которые могут нарушить безопасность информационной системы, используются системы обнаружения вторжений. Система обнаружения вторжений обычно включает:

- сенсорную систему, предназначенную для сбора событий, связанных с безопасностью защищаемой системы;
- подсистему анализа, предназначенную для выявления подозрительных действий и атак на основе данных сенсоров;
- хранилище данных, необходимое для накопления первичных событий и результатов анализа;
- подсистему управления и представления результатов анализа, позволяющую конфигурировать систему обнаружения вторжений и наблюдать за состоянием защищаемой системы.

Наиболее сложной и «математизированной» частью системы обнаружения вторжений является блок анализа. Входными данными для блока анализа является информация, полученная от сенсоров. В большинстве современных систем такого рода для анализа применяется комбинация нескольких математических методов.

Для повышения точности предсказания и обнаружения атак система обнаружения вторжений должна собирать разнородную информацию о работе защищаемой системы, а также хранить и обрабатывать большой объем данных. Использование системы фильтрации в отсутствии атаки влечет за собой снижение производительности сервера и возможное ложное срабатывание фильтра. Достаточно часто создание эффективной системы защиты сталкивается с нехваткой вычислительной мощности. Таким образом, возникает задача

оптимизации ресурсов, затрачиваемых на поддержание работоспособности системы защиты от сетевых атак на высоком уровне.

Одним из вариантов решения указанной проблемы является минимизация ресурсов, затрачиваемых на поддержание информационной безопасности в те моменты времени, когда активность атакующей стороны незначительна. С этой целью система обнаружения вторжений должна использовать динамические методы, позволяющие оперативно обнаруживать и предотвращать нарушения безопасности. То есть в системе защиты информации должна быть использована математическая модель, позволяющая в каждый момент времени выбрать необходимый набор средств защиты, обеспечивающий надежную защиту и при этом требующий минимального количества ресурсов.

В отечественных и зарубежных работах последних лет наблюдается тенденция расширения имеющихся математических подходов к выбору параметров системы защиты информации. Так, например, различные авторы предлагают следующие математические методы для анализа и оптимизации системы защиты информации [10]:

- методы математической статистики;
- методы, основанные на использовании сетей Петри;
- математический аппарат теории случайных процессов;
- методы, основанные на использовании теории автоматов;
- методы на основе теории нечетких множеств;
- методы, основанные на использовании нейронных сетей;
- методы экспертных систем;
- математический аппарат теории игр.

Статистические методы обнаружения вторжений используют хорошо зарекомендовавший себя аппарат математической статистики к поведению субъектов анализируемой системы. Вначале для всех субъектов формируются статистические профили. Составными элементами такого профиля могут быть различные параметры, например, общий трафик в единицу времени, количество отказов в обслуживании, отношение входящего трафика к исходящему, количество уникальных запросов к системе и др. Любое отклонение используемого профиля от эталонного считается нарушением безопасности. Основными недостатками данного подхода являются следующие моменты. Во-первых, системы обнаружения вторжений на основе статистических методов не чувствительны к порядку следования событий в защищаемой системе: в некоторых ситуациях одни и те же события в зависимости от порядка их следования могут быть характерны для аномальной или нормальной деятельности. Во-вторых, в некоторых случаях бывает трудно задать пороговые значения отслеживаемых характеристик для идентификации аномальной деятельности. Занижение порога приводит к ложному срабатыванию, а завышение - к пропуску вторжений. Кроме того, часто атакующая сторона

использует индивидуальные подходы для каждой системы защиты, что делает использование статистических методов менее эффективными [10].

Любую систему обработки информации, состоящую из различных аппаратных и программных средств, можно рассматривать как уникальный комплекс со своими особенностями. Именно это является объяснением возможности пропуска специфичных для защищаемой системы вторжений теми системами обнаружения вторжений, которые используют один и тот же набор параметров оценки. Следовательно, более предпочтительным решением будет определение необходимых параметров мониторинга в процессе работы системы. Трудность эффективного динамического формирования параметров наблюдения состоит в том, что размер области поиска экспоненциально зависит от мощности начального множества наблюдаемых параметров. Для формирования множества наблюдаемых параметров в системах обнаружения вторжений могут использоваться различные интеллектуальные методы.

Многие исследователи предлагают использовать в качестве математической основы при построении и анализе систем защиты информации аппарат теории игр. Теория игр является формальным подходом, предназначенным для анализа взаимодействий между несколькими участниками процесса, имеющими разные интересы и принимающими решения. В любой системе защиты информации предполагаются две стороны: сторона нападения и сторона защиты (система защиты информации), имеющие противоположные интересы. В подразделе 2.3 рассмотрен математический аппарат теории игр для решения задачи выбора средств защиты от несанкционированного доступа к информации в автоматизированной системе. Там же выполнена математическая постановка задачи в виде задачи линейного программирования с булевыми переменными. В математической постановке введен показатель стоимости средств защиты. Ограничения задачи учитывают требования классов защищенности от несанкционированного доступа в автоматизированных системах.

В [11] проводится обзор теоретико-игровых методов, используемых при решении задач информационной безопасности. В работе рассматривается подход к проектированию систем обнаружения вторжений с использованием математического аппарата матричных игр для двух игроков. В предлагаемой модели учитывается стоимость системных ресурсов для организации защиты.

В работе [12] рассматриваются возможности использования многошаговых игр с неполной информацией при построении систем защиты от DoS атак. Предлагается представить задачу в виде игры двух сторон: обороняющейся (A) и атакующей (B). Задачей обороняющейся стороны является минимизация собственных потерь вследствие действий атакующей стороны. Задача стороны *B* – получение максимальной прибыли. В статье указывается, что главной особенностью такой игры является то, что в качестве стратегий используются функции, описывающие поведение сторон в краткосрочной перспективе (под краткосрочной перспективой понимается такой промежуток времени, в котором

поведение участников игры можно представить детерминировано). Множество функций предлагается подбирать для каждой задачи индивидуально, исходя из статистических данных, внешних ограничений и здравого смысла.

При анализе вопросов защиты от различных угроз безопасности целесообразно рассматривать действия двух сторон: стороны защиты (информационной системы) и стороны нарушителя. В качестве нарушителя можно рассматривать всю совокупность угроз безопасности: действия отдельных лиц, преследующих различные цели, крупномасштабные спланированные атаки, а также случайные воздействия на систему. Подобные модели, когда существуют две или более противоборствующие стороны. Если известны варианты действий (стратегии) каждой из сторон, а также выигрыш (или проигрыш) от каждого из вариантов действий, то имеется возможность сформулировать математическую модель ситуации в виде модели бескоалиционной антагонистической игры (например, матричной). На основе сформулированной модели можно получить оптимальные стратегии стороны нападения и стороны защиты, требующие минимума ресурсов.

Рассмотрим взаимодействие сторон (нарушителя и системы обнаружения вторжений) как бескоалиционную конечную игру. Пусть сторона защиты А и нарушитель В имеют конечное число стратегий n_A и n_B что соответствует реальности, так как сторона защиты всегда имеет ограничение по числу возможных вариантов реагирования, а сторона нападения по числу вариантов организации атаки. Например, для стороны защиты можно использовать стратегии {«игнорировать подозрительную активность», «усилить мониторинг»}, а для стороны нападения можно рассматривать множество стратегий {«завершить атаку», «продолжить без паузы», «сделать паузу в атаке»}. Набора стратегий игроков $s = (s_A, s_B), s_A \in S_A, s_B \in S_B$, называется ситуацией. Функции w_A и w_B выигрышей игроков определены на множестве ситуаций $S = S_A \times S_B$.

Решением бескоалиционной игры являются ситуации равновесия, но не обязательно в чистых стратегиях. Как известно, каждая конечная антагонистическая игра имеет хотя бы одну ситуацию равновесия в смешанных стратегиях. Смешанные стратегии при анализе систем защиты информации имеет смысл рассматривать при допущении, что работа системы продолжается значительное время, то есть итерации атаки и защиты повторяются многократно. При этом стратегии используются сторонами с некоторой недетерминированной закономерностью и затраты/доходы накапливаются с течением времени. Смешанной стратегией игроков А и В будем называть полный набор вероятностей применения их чистых стратегий:

$$P_A = \{p_{A1}, p_{A2}, \dots, p_{An}\}, P_B = \{p_{B1}, p_{B2}, \dots, p_{Bn}\}$$

В бескоалиционной игре каждый игрок использует свои чистые стратегии независимо от другого участника процесса, поэтому в смешанной ситуации p= $\{P_A , P_B\}$ вероятность $p(s)$ появления ситуации AB $s = (s_A, s_B)$, равна произведению вероятностей использования обоими игроками своих чистых стратегий, то есть

$$p(s) = p(s_A, s_B) = p_A, s_A \cdot p_{B1}, s_B$$

Найдем средний выигрыш (проигрыш) игроков. В общем случае математическое ожидание выигрыша игрока А в смешанной ситуации p= $\{P_A , P_B\}$ определяется следующим образом:

$$\overline{W_A(p)}=\overline{w_A}(P_A , P_B)= \sum_{s\in S} w_A(s)p(s)= \sum_{s1\in SA} \sum_{s2\in SB} w_A(s_1, s_2) \cdot p_A, s_A \cdot p_{B1}, s_B,$$

где P_A , P_B – множества возможных ситуаций игроков А и В соответственно, w_A – функция выигрыша (а на самом деле – проигрыша или расходов) системы защиты информации, если система защиты информации выбрала стратегию s_1, а нарушитель – стратегию s_2.

Выигрыш игрока В (нарушителя системы защиты информации) в общем случае определяется аналогично.

Каким образом можно определить выигрыши игроков в данном случае? Система обнаружения вторжений S в каждый момент времени наблюдает множество параметров M_Sс помощью сенсоров. Каждую атаку можно представить в виде последовательности итераций. После каждого шага система обнаружения вторжений пытается «предсказать» следующие шаги нарушителя. Каждый шаг нарушителя порождает некоторый вид активности, который обнаруживается датчиками системы. Если блок анализа распознает активность как подозрительную, множество базовых наблюдаемых параметров M_S должно быть расширено. Пусть множество дополнительных параметров наблюдения будет $M_{S\text{доп}}$ ={x_1, x_2, ... , x_n}, а стоимость дополнительных ресурсов, затрачиваемых на их наблюдение в течение времени t – C_A (t). Предположим, затраты на наблюдение прямо пропорциональны времени наблюдения. Если мониторинг расширенного множества параметров производится в течение времени t_m, то стоимость дополнительных затрат на наблюдение будет равен

$$C_A\ (t) = \sum_{i=1}^{n} c_i t_m,$$

где n – количество дополнительных параметров наблюдения, c_i – затраты на мониторинг i-го параметра. При принятии решения игнорировать возможную атаку система защиты информации не несет затрат на дополнительный мониторинг.

Оценим затраты нарушителя системы защиты информации. В случае принятия решения о прекращении атаки нарушитель не несет дополнительных затрат, а в случае принятия решения о продолжении атаки затраты атакующей стороны зависят от количества k генерируемых запросов к защищаемой системе: $C_B = gk$, где g – стоимость генерации одного запроса.

В случае успешной атаки система защиты информации несет убытки c_A^*, а нарушитель получает некоторый выигрыш c_B^*.

Затраты системы защиты информации при реализации каждой из возможных стратегий складываются из затрат на организацию защиты от $C_A(t)$ и убытков от возможных нарушений безопасности c_A^*. Аналогично выигрыш нарушителя складывается из выигрыша от нарушения работы системы защиты информации c_B^* и из затрат на проведение атак C_B.

Для рассматриваемой системы обнаружения вторжений предполагается, что с увеличением дополнительных параметров наблюдения возрастает вероятность верного определения атаки. Однако определение точной зависимости успешного обнаружения атаки от количества и набора параметров мониторинга, а также от времени наблюдения требует экспериментального исследования для каждого типа систем защиты информации.

Как уже отмечалось, каждая конечная бескоалиционная игра имеет хотя бы одну ситуацию равновесия в смешанных стратегиях Ситуацию равновесия можно найти стандартными методами теории игр.

Хотелось бы отметить некоторые особенности применения данной методики применительно к системам защиты информации.

Прежде всего, выигрыши игроков в смешанной ситуации были определены равными математическим ожиданиям их выигрышей. Это предполагает, что игроки являются нейтральными к риску при многократном повторении игровой ситуации. Однако в случае рассмотрения систем защиты информации это не совсем оправдано. Если нарушителя можно считать нейтральным к риску участником игры, то сторону защиты – скорее всего, нет. Даже однократное нарушение безопасности защищаемой системы может быть критичным для нее, выводя из работоспособного состояния на длительное время.

Во-вторых, модель может использовать те или иные данные в качестве входных параметров. При этом возможности получения различных данных могут быть задачами разной степени сложности. Так, например, если модель использует в качестве входных параметров вероятности использования атакующей стороной отдельных стратегий, характеристики средств защиты, уязвимостей, барьеров и т.д., то оценить все указанные параметры и определить взаимосвязи между ними достаточно сложно, что осложнит практическое применение методики в системе обнаружения вторжений.

Далее, известно, что в обнаружении сетевых вторжений очень значительную роль играет множество параметров оценки. Поэтому в обнаружении аномалий

одной из главных задач является выбор оптимального множества параметров оценки, что невозможно выполнить методами теории игр. Поэтому целесообразно применять различные комплексные математические методы при построении систем защиты информации, в частности, систем обнаружения вторжений.

В целом, математический аппарат теории игр может быть применен для анализа ситуаций с повторяющейся антагонистической природой, что является типичным для задач защиты информации. Предлагаемые методы дают возможность выбрать на начальном этапе работы системы обнаружения вторжений стратегии действий и снизить вычислительные затраты на обработку данных в системе защиты информации.

2.3. Выбор средств защиты информации в телекоммуникационных системах на основе модели антагонистической игры.

При защите от различных угроз безопасности присутствуют две стороны: сторона нарушителя или сторона нападения, которая преследует свои цели, в качестве нарушителя можно рассматривать и «природу» («игра с природой»), в этом случае у нарушителя нет целей, рассматриваются различные случайные воздействия на систему, и сторона защиты от возможных реализаций этих угроз безопасности. Подобные модели принятия решения, когда существуют две или более противоборствующих сторон, рассматриваются в теории «игр» [7]. Для выбора средств защиты от DDoS-атак используем матричную игру двух игроков с нулевой суммой. Решение по различным критериям оптимальности искалось на платежной матрице игры, но если число средств защиты и число возможных атак велико, то платежная матрица будет иметь большую размерность, искать решения напрямую на такой матрице затруднительно.

Будем считать, что исходными данными являются следующие:

1. A = $\{a_1, a_2, \dots, a_n\}$ – множество возможных угроз безопасности или средств проведения атак, которыми может воспользоваться нарушитель, N = {1, 2, … , n}– множество индексов этих угроз (средств). В качестве возможных угроз здесь можно рассматривать конкретные технические, программные или организационные средства, которые может задействовать сторона нападения.
2. B = $\{b_1, b_2, \dots, b_m\}$ – множество средств защиты информации от угроз безопасности, M = {1, 2, … , m} – множество индексов средств защиты соответственно.
3. $u_i \forall \in N$ – средний ущерб от непредотвращения i-ой угрозы за заданный период времени.
4. $c_i^{(н)} \geq 0, \forall i \in N$ – стоимость реализации i-ой угрозы стороной нападения;
5. $c_j^{(з)} \geq 0, \forall j \in M$ – стоимость j-го средства защиты;
6. $p_{ij} \in [0, 1]$, $\forall i \in N$, $\forall j \in M$ – возможность, описываемая в рамках теории нечетких множеств, или вероятность (если есть статистика) предотвращения последствий i-ой угрозы с помощью j-го средства защиты, параметры образуют матрицу P = $\|p_{ij}\|$, размерности n × m.

Для стороны защиты введем булеву переменную $x_j \in \{0, 1\}$, $\forall j \in M$.

$-x_j = 1$, если j-ое средство защиты будет применяться в автоматизированной системе для защиты от тех или иных угроз;

$-x_j = 0$в противном случае, то есть если j- ое средство не будет применяться. Тогда $\vec{X}$ - вектор булевых переменных x_j . По аналогии для стороны нападения введем булеву переменную $y_i \in \{0, 1\}$, $\forall i \in N$:

$-y_i = 1$, если сторона нападения будет использовать i-ое средство атаки (реализовывать i-ую угрозу);
$-y_i = 0$ в противном случае.

Тогда $\vec{Y}$ - вектор булевых переменных y_i .

Ущерб от реализации атак без применения средств защиты для стороны защиты или максимально возможный ущерб определяется как:

$$U^{(max)}(\vec{Y}) = \sum_{i \in N} u_i y_i \ .$$

При использовании средств защиты некоторая часть этого ущерба будет предотвращена, предотвращенный ущерб в общем случае может быть описан:

$$U^{(\text{пред})}(\vec{X}, \vec{Y}) = \sum_{i \in N} u_i y_i \, F_i(P, \vec{X}) \ ,$$

где $F_i(P, \vec{X})$, $\forall i \in N$ – функции, определяющие степени предотвращения ущерба от каждой из угроз.

В качестве таких функций будем использовать:

$$F_i(P, \vec{X}) = max_{j \in M}\{p_{ij} x_i\}, \forall i \in N.$$

Содержательно функция задает то, что для предотвращения ущерба учитывается только одно выбранное средство защиты, имеющее максимальную возможность (вероятность) предотвращения для i-ой угрозы. В этой функции не учитывается суммарный эффект от совместного использования двух или более средств защиты для предотвращения угрозы.

Тогда реальный ущерб для стороны защиты:

$$\begin{aligned} U(\vec{X}, \vec{Y}) &= U^{(max)}(\vec{Y}) - U^{(\text{пред})}(\vec{X}, \vec{Y}) = \\ &= \sum_{i \in N} u_i y_i - \sum_{i \in N} u_i y_i \, max_{j \in M}\{p_{ij} x_i\} \end{aligned} \qquad (23)$$

Данный показатель определяет реальный возможный ущерб для стороны защиты при использовании СЗИ. Сторона защиты старается этот ущерб минимизировать, а сторона нападения старается максимизировать, таким образом, получаем игру двух игроков с нулевой суммой.

При этом сторона защиты ограничена в средствах и может потратить на защиту информации некоторую максимальную сумму $C_{max}^{(з)}$. Тогда ограничения на максимальную стоимость средств защиты определяется неравенством:

$$\sum_{i \in M} c_j^{(з)} x_j \leq C_{max}^{(з)} \ . \qquad (24)$$

По аналогии для стороны нападения введем ограничения на максимальную стоимость используемых для атак ресурсов:

$$\sum_{i \in N} c_j^{(н)} y_i \leq C_{max}^{(н)} \quad (2.5)$$

где $C_{max}^{(н)}$ - максимальная стоимость ресурсов, которые может выделить для проведения атак нарушитель.

Сторона защиты или первый игрок решает задачу минимизации показателя (2.3) с ограничениями (2.4):

$$U(\vec{X}, \vec{Y}) = \sum_{i \in N} u_i y_i - \sum_{i \in N} u_i y_i \, max_{j \in M} \{p_{ij} x_i\} \rightarrow min_{\vec{X} \in \Delta_x^{(доп)}}, \quad (2.7)$$

$$\Delta_x^{(доп)}: \sum_{i \in M} c_j^{(з)} x_j \leq C_{max}^{(з)}$$

где $\Delta_x^{(доп)}$ – множество допустимых альтернатив (значений компонент неизвестного вектора $\vec{X}$) для первого игрока. При фиксированных значениях компонент вектора $\vec{Y}$ получаем задачу булевого программирования.

Сторона нападения или второй игрок решает задачу максимизации показателя (2.3) с ограничениями (2.5):

$$U(\vec{X}, \vec{Y}) = \sum_{i \in N} u_i y_i - \sum_{i \in N} u_i y_i \, max_{j \in M} \{p_{ij} x_i\} \rightarrow max_{\vec{Y} \in \Delta_y^{(доп)}}, \quad (2.8)$$

$$\Delta_y^{(доп)}: \sum_{i \in N} c_j^{(н)} y_i \leq C_{max}^{(н)}$$

где $\Delta_y^{(доп)}$ - множество допустимых альтернатив (значений компонент неизвестного вектора $\vec{Y}$) для второго игрока. При фиксированных значениях компонент вектора $\vec{X}$ получаем задачу булевого программирования.

Представленную модель игры можно свести к игре, заданной платежной матрицей [13]. Проблема в том, что размерность этой матрицы может быть достаточно велика: число строк будет равно числу допустимых значений вектора $\vec{X}$, удовлетворяющих ограничению (2.5), а число столбцов будет равно числу допустимых значений вектора $\vec{Y}$, удовлетворяющих ограничению (2.6). В случае использования платежной матрицы часто ищут седловую точку в чистых стратегиях или, если ее не существует, в смешанных стратегиях [13]. При большой размерности платежной матрицы это затруднительно.

Можно использовать различные критерии оптимальности, такие как критерии Лапласа, Вальда, Гурвица или Сэвиджа. С точки зрения обеспечения состояния защищенности информации чаще всего для стороны защиты используют критерий Вальда, так как при проектировании системы защиты необходимо обеспечить гарантированный результат в любых условиях. Критерий Вальда обеспечивает выбор осторожной или пессимистической стратегии, т.е. обеспечивает гарантированный результат при самых худших условиях. Из-за

того, что при выборе средств защиты решается защита минимизации возможного ущерба, данный критерий превращается в минимаксный критерий:

$$min_{\vec{X}\in\Delta_x^{(\text{доп})}} max_{\vec{Y}\in\Delta_y^{(\text{доп})}} U(\vec{X},\vec{Y}) \qquad (2.9)$$

При решении задачи максимизации показателя $U(\vec{X},\vec{Y})$ по вектору $\vec{Y}\in\Delta_y^{(\text{доп})}$ при фиксированных значениях вектора $\vec{X}$ или задачи минимизации показателя $U(\vec{X},\vec{Y})$ по вектору $\vec{X}\in\Delta_x^{(\text{доп})}$ при фиксированных значениях вектора $\vec{Y}$ решаются задачи булевого программирования с линейным ограничением (2.3) или (2.4) и нелинейным показателем качества (2.3). Эти задачи относятся к классу NP-полных задач оптимизации. Точное решение для таких задач может быть получено алгоритмом с экспоненциальной трудоемкостью. Рассмотрим некоторые точные и приближенные алгоритмы, подходящие для решения задачи по критерию (2.9).

Среди точных методов в булевом программировании всегда можно выделить метод полного перебора. Другие точные методы позволяют сократить некоторым образом полный перебор. Рассмотрим один из методов, который можно применить к данной задаче, – метод неявного перебора на векторной решетке.

Идея метода следующая: между булевыми векторами $\vec{X}$ (или $\vec{Y}$), имеющими различ- ные значения компонент можно ввести отложение доминирования. Отношение доминиро- вания устанавливается между любыми двумя векторами, отличающимися только значением одного элемента. Можно ввести данное отношение двумя способами: значение 0 доминирует значение 1 или наоборот – 1 доминирует 0. На первом уровне решетки располагается недоминируемый вектор, состоящий из всех 0 (или всех 1), на втором уровне – вектора, доминируемые лишь вектором первого уровня и не доминируемые никакими другими векторами и т.д. Для векторов из трех булевых переменных решетка по правилу «0 доминирует 1» представлена на рис. 2.3.1, а решетка по правилу «1 доминирует 0» представлена на рис. 2.3.2. Решетка является отношением частичного порядка.

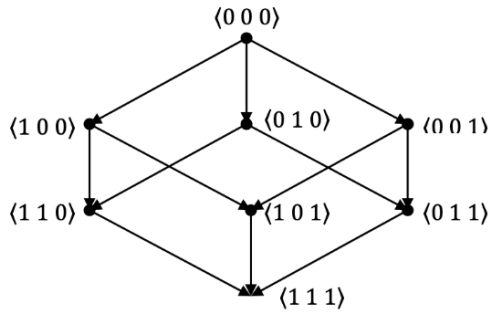

Рис. 2.1. Пример решетки по правилу «0 доминирует 1»

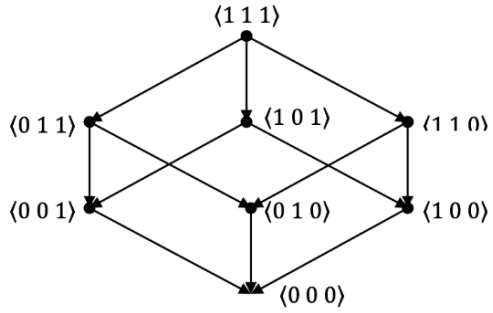

Рис. 2.2. Пример решетки по правилу «1 доминирует 0»

Правило 1 получения новых векторов следующего уровня решетки в цикле: для всех последних элементов вектора, равных 0, до первой 1 (или до начала вектора, если вектор состоит из всех 0) последовательно, по одному, значение 0 превращаем в 1 в направлении от начала к концу вектора, каждый раз получаем новый вектор следующего уровня, если в векторе последний элемент 1, то векторов следующего уровня для элемента не существует.

Например, для вектора $\|101000\|^T$ элементами следующего уровня решетки, которые не были получены при рассмотрении предшествующих решений, являются вектора:

$$\|101100\|^T, \|101010\|^T, \|101001\|^T.$$

Если используется правило «1 доминирует 0», то для получения новых векторов следующего уровня для любого элемента используется правило 2 (обратное правилу 1).

Правило 2 получения новых векторов следующего уровня решетки в цикле: для всех последних элементов вектора, равных 1, до первого 0 (или до начала вектора, если вектор состоит из всех 1) последовательно, по одному, значение 1 превращаем в 0 в направлении от начала к концу вектора, каждый раз получаем новый вектор следующего уровня, если в векторе последний элемент 0, то векторов следующего уровня для элемента не существует.

Процесс получения новых векторов нижнего уровня для текущего вектора (решения) будем называть зондированием этого вектора (решения).

Решетчатое упорядочивание позволяет, учитывая специфику задачи, не осуществлять полный перебор всех элементов. Если используется правило «0

доминирует 1», то элемент решетки, который не удовлетворяет ограничениям (2) или (3) в зависимости от решаемой задачи, можно далее не зондировать, так как эти вектора также будут недопустимыми. Это связано с тем, что коэффициенты в ограничениях (2) и (3) неотрицательные, и максимальная стоимость также неотрицательная (добавление в вектор новой единицы может только увеличить общую стоимость).

Если используется правило «1 доминирует 0», то элемент решетки, который удовлетворяет ограничениям (2) или (3) в зависимости от решаемой задачи, можно далее не зондировать, так как эти вектора будут иметь значение целевой функции (1) не лучше, чем полученное. Это связано с тем, что превращение в векторе 1 в 0, означает то, что некоторое средство (защиты или нападения, в зависимости от решаемой задачи) не будет применено, что не улучшит выигрыш соответствующего игрока. Для реализации алгоритмов перебора на решетке удобно использовать рекурсивные алгоритмы. Рассмотрим два алгоритма поиска решения на решетке.

Алгоритм неявного перебора на решетке, построенной по правилу «0 доминирует 1»

Стартовый алгоритм метода неявного перебора на решетке, построенной по правилу «0 доминирует 1», имеет следующие шаги:

1. Задаем начальное решение, состоящее из всех нулей $\vec{X} = ||0, 0, \dots, 0||^T$ (в программе массив X размерности m), полагаем UMinMax= ∞.

2. Выполнение рекурсивного алгоритма зондирования решения $\vec{X}$ по правилу «0 до- минирует 1».

3. После работы алгоритма зондирования значение показателя для первого игрока, осуществляющего выбор средств защиты, haqденное по критерию минимакс (6), будет равно UMinMax, полученное решение будет записано в массиве XRec, решение второго игрока будет в массиве YRec2.

Рекурсивный алгоритм зондирования решения (массива X размерности m) по правилу «0 доминирует 1»:

1. Задаем начальное решение $\vec{Y}$, состоящее из всех нулей $\vec{Y} = ||0, 0, \dots, 0||^T$, (в про- грамме массив Y размерности n) полагаем UMax=0.

2. Выполнение рекурсивного алгоритма зондирования $\vec{Y}$ решения по правилу «0 до- минирует 1».

3. Если UMax<UMinMax, то полагаем UMinMax = UMax и сохраняем решение YRec в массиве YRec2 (рекордное решение по критерию минимакс), сохраняем значение массива X в массиве XRec (рекордное решение по критерию минимакс).

4. По правилу 1 в цикле получаем решение следующего уровня решетки – новый вектор $\vec{X}_{next}$ (массив X размерности m). Если решение $\vec{X}_{next}$ допустимое по ограничению (2), то для него запускаем рекурсивный алгоритм зондирования

решения $\vec{X}$ по правилу «0 до- минирует 1». Если таких решений не существует, алгоритм прекращает свою работу.

Рекурсивный алгоритм зондирования решения $\vec{Y}$ (массива Y размерности n) по правилу «0 доминирует 1»:

1. Вычисляем значение показателя (1): U = $U(\vec{X}, \vec{Y})$.
2. Если U > UMax, то полагаем UMax = U и сохраняем решение Y в массиве YRec (ре- кордное значение по критерию максимум).
3. По правилу 1 в цикле получаем решение следующего уровня решетки – новый вектор $\vec{Y}_{next}$ (массив Y размерности n). Если решение $\vec{Y}_{next}$ допустимо по ограничению (3), то для него запускаем рекурсивный алгоритм зондирования решения $\vec{Y}$ по правилу «0 доминирует 1». Если таких решений не существует, алгоритм прекращает свою работу.

Алгоритм неявного перебора на решетке, построенной по правилу «1 доминирует 0»

Стартовый алгоритм метода неявного перебора на решетке, построенной по правилу «1 доминирует 0», имеет следующие шаги:

1. Задаем начальное решение, состоящее из всех единиц $\vec{X} = \|1, 1, \dots, 1\|^T$ (в программе массив X размерности m), полагаем UMinMax= ∞.
2. Выполнение рекурсивного алгоритма зондирования решения $\vec{X}$ по правилу «1 до- минирует 0».
3. После работы алгоритма зондирования значение показателя для первого игрока, осуществляющего выбор средств защиты, найденное по критерию минимакс (6), будет равно UMinMax, полученное решение будет записано в массиве XRec, решение второго игрока будет в массиве YRec2.

Рекурсивный алгоритм зондирования решения $\vec{X}$ (массива X размерности m) по правилу «1 доминирует 0»:

1. Если решение $\vec{X}$ допустимо в соответствии с ограничением (2), то задаем начальное решение $\vec{Y}$, состоящее из всех единиц $\vec{Y} = \|1, 1, \dots, 1\|^T$, (в программе массив Y размерности n) полагаем UMax=0, переходим к следующему шагу, в противном случае переходим к шагу 5.
2. Выполнение рекурсивного алгоритма зондирования $\vec{Y}$ решения по правилу «1 до- минирует 0».
3. Если UMax<UMinMax, то полагаем UMinMax = UMax и сохраняем решение YRec в массиве YRec2 (рекордное решение по критерию минимакс), сохраняем значение массива X в массиве XRec (рекордное решение по критерию минимакс).
4. Алгоритм завершает работу.
5. По правилу 2 в цикле получаем решение следующего уровня решетки новый вектор $\vec{X}_{next}$ (массив X размерности m), для каждого $\vec{X}_{next}$ запускаем

рекурсивный алгоритм зондирования $\vec{X}$ по правилу «1 доминирует 0». Если таких решений не существует, алгоритм завершает свою работу.

Рекурсивный алгоритм зондирования решения (массива Y размерности n) по правилу «1 доминирует 0»:

1. Если решение $\vec{Y}$ допустимо в соответствии с ограничением (3), то вычисляем значение показателя (1): U = $U(\vec{X},\vec{Y})$ и переходим к следующему шагу, в противном случае переходим к шагу 3.

2. Если U > UMax, то полагаем UMax = U и сохраняем решение Y в массиве YRec (рекордное значение по критерию максимум), алгоритм завершает работу.

3. По правилу 2 в цикле получаем решение следующего уровня решетки – новый вектор $\vec{Y}_{next}$ (массив Y размерности n), для каждого $\vec{Y}_{next}$ запускаем рекурсивный алгоритм зондирования $\vec{Y}$ по правилу «1 доминирует 0». Если таких решений не существует, алгоритм завершает свою работу.

Рассмотрим алгоритм приближенного метода решения задачи, некоторые аналоги которого рассмотрены в [14], алгоритм является эвристическим и не гарантирует получение приближенного решения с заданной априорно точностью, т.е. погрешность алгоритма может быть достаточно велика. Применение определенных критериев остановки предохраняет алгоритм от зацикливания. Алгоритм метода включает следующие шаги:

1. Задаем начальное решение, состоящее из всех нулей $\vec{X} = ||0, 0, \dots, 0||^T$ (в программе массив X размерности m), полагаем UMinMax= ∞.

2. Некоторым методом булевого программирования, возможно приближенным, решаем задачу максимизации (2.8) при фиксированном векторе $\vec{X}$ (массиве X), получаем решение $\vec{Y}$ (массив Y) и значение показателя для этого решения UMax.

3. Если UMax<UMinMax, то полагаем UMinMax = UMax и сохраняем решение Y в массиве YRec (рекордное решение по критерию минимакс), сохраняем значение массива X в массиве XRec (рекордное решение по критерию минимакс).

4. Проверяем критерий остановки, если он выполняется, алгоритм завершает свою работу, в противном случае переходим к следующему шагу.

5. Некоторым методом булевого программирования, возможно приближенным, решаем задачу минимизации (2.7) при фиксированном векторе (массиве YRec), получаем решение X, переходим к шагу 2.

Учитывая то, что множество решений конечно, то при работе алгоритма решения будут повторяться через некоторое число итераций. В качестве критериев остановки можно использовать следующие критерии в порядке очередности их проверки:

- получение повторного решения на шаге 3 со значением показателем качества UMax, равным значению сохраненном в переменной UMinMax, что не всегда происходит. Иногда решение с минимальным значением показателя получается

на одной из первых итераций алгоритма и далее не повторяется, происходит повторение последовательности решений, среди которых нет решения с минимальным значением показателя, тогда используется следующий критерий;

- получение повторного решения на шаге 3, искомым решением будет одно из решений, полученных на предыдущих шагах с минимальным значением показателя, сохраненным в UMinMax.

Приближенный алгоритм может быть использован для быстрого поиска допустимого решения в случае задач большой размерности, параметры этого алгоритма, полученные в ходе экспериментов, представлены ниже.

В работе [14] представлено описание экспериментов для исследования параметров алгоритма и приведен пример решения задачи.

Контрольные вопросы:

1. *Что представляет из себя задача выбора оптимальной стратегии выбора стратегий защиты информационных систем?*
2. *Что позволяет реализовать анализ выбранного оборудования?*
3. *Раскройте понятие «максмина».*
4. *Каковы варианты построения СЗИ от сетевых атак?*
5. *В чем состоят особенности динамического формирования множества наблюдаемых параметров?*
6. *Что рассматривается в качестве нарушителя информационной безопасности?*
7. *Что представляет собой решение бескоалиционной игры?*
8. *Какие стратегии используют игроки в бескоалиционной игре?*
9. *Какие модели используются, когда в игре участвуют противоборствующие стороны?*
10. *Какие задачи решают стороны в антагонистической игре?*

3. Антагонистические игры в задачах защиты информации.

3.1. Выбор стратегии ложной информационной системы.

Одной из задач, решаемых специалистами по информационной безопасности, является сбор сведений, позволяющих обнаружить атаки, и анализ действий злоумышленника. Обнаружение атак на основе ложных информационных систем, иначе технология Honeypot («ловушка»), позволяет на более ранней стадии обнаружить факт подготовки атаки, изучить поведение ее инициатора при попытке проникновения и управления уже захваченным ресурсом, получить информацию о ранее неизвестных методах атак, дезинформировать злоумышленника, а также обнаружить «дыры» в безопасности и своевременно применить меры по их устранению. Honeypot является ложным ресурсом информационной системы (ИС), не используемым санкционированными пользователями сети и находящимся под полным контролем специалистов по информационной безопасности. Это позволяет сократить число ложных тревог и объем обрабатываемых событий безопасности, поскольку в системе регистрируется только реальные попытки зондирования или атаки. Однако следует отметить, что необходимы обоснованные подходы и рекомендации к процессу проектирования таких «ловушек», так как в случае обнаружения злоумышленником ЛИС она может быть использована для организации атак на другие системы [11]. Таким образом, исследование и разработка научно обоснованных решений для проектирования ЛИС в реальных автоматизированных системах (АС) представляет собой актуальную проблему в сфере информационной безопасности.

ЛИС может представлять собой как отдельный хост сети, так и сеть, наполненную разного рода объектами: маршрутизаторами, серверами, рабочими станциями, реальными или виртуальными. Следует отметить, что развитию практики применения ЛИС способствует активное внедрение технологии виртуализации, появление программных средств виртуализации, позволяющих создать виртуальную инфраструктуру и управлять ею [1]. Однако с увеличением степени использования рассматриваемой технологии злоумышленники принимают во внимание возможность существования ЛИС в атакуемой сети и пытаются обойти «ловушки». Следовательно, такие ИР должны быть достаточно замаскированы и не очевидны, ЛИС не должна представлять из себя наиболее уязвимую цель для злоумышленника (при этом должна быть обеспечена высокая вероятность выбора злоумышленником в качестве цели ложной ИС, а не реальной системы) [2]. Это приводит к рассмотрению некоторой состязательности между злоумышленником и ЛИС, анализу стратегий взаимодействующих сторон. С этой задачей может справиться математический аппарат теории игр.

Ложные информационные системы и теория игр

В настоящее время предложено немало решений, в том числе открытых реализаций, для проектирования ЛИС, однако меньше известно о том, как разработать стратегию «ловушки» в защищаемой сети [15].

При решении задач, связанных с обеспечением информационной безопасности, широкое применение находит математический аппарат теории игр. Теория игр является формальным подходом, предназначенным для анализа взаимодействий между несколькими участниками игры, принимающими решения. В области защиты информации присутствуют две стороны: сторона нападения и сторона защиты, в качестве которой выступают системы защиты информации.

Рассмотрим примеры использования теории игр. В работе [4] предложена математическая модель антагонистической игры и алгоритмы, позволяющие решить задачу выбора средств защиты информации в АС. Методы теории игр используют и для выбора средств защиты от конкретных сетевых атак. Например, в [13] разработана матричная игра двух игроков с нулевой суммой для выбора эффективного средства защиты от DoS/DDoS-атак. В работе [11] рассмотрено взаимодействие узловой системы обнаружения вторжений и нарушителя информационной безопасности с помощью некооперативной игры с ненулевой суммой, где оптимальные стратегии игроков выбираются согласно равновесию Нэша. Математический аппарат теории игр находит свое применение и в технологии ЛИС.

Имеющиеся на данный момент работы, исследующие взаимодействие злоумышленника и ЛИС (сторона защиты) с помощью теории игр, можно разделить на две категории: моделирование взаимодействия сторон для конкретной атаки и моделирование взаимодействия до проведения атаки, когда злоумышленник, анализируя сеть, выбирает цель нападения [15]. Во втором случае рассматривается проблема повышения вероятности выбора злоумышленником ложной ИС для проведения атаки. В работе [15] представлены две теоретико-игровые модели с нулевой суммой, позволяющие понять, какой должна быть «ловушка», чтобы максимизировать вероятность проведения атаки на ЛИС, а не на реальную систему. Первая модель позволяет определить число приманок, размещаемых в ЛИС, и их конфигурацию. Вторая модель включает в рассмотрение стратегию зондирования, целью которой является обнаружение ЛИС в реальной сети. В [15] посредством некооперативной игры с ненулевой суммой рассмотрено взаимодействие между ЛИС и бот-сетью (от англ. botnet; от слов robot и network). При моделировании большое внимание уделяется проблеме обнаружения ЛИС ботами. Следует отметить, что в поиске уязвимых мест ложной ИС заинтересованы как злоумышленники, так специалисты по информационной безопасности.

Таким образом, можно сделать вывод, что теория игр – это математическая теория, которая способна вырабатывать и находить оптимальные стратегии и

инструкции по организации систем информационной безопасности. Ниже будет предложена постановка задачи выбора ресурсов сети, моделируемых в ЛИС, на основе теоретикоигрового подхода.

Рассмотрим постановку задачи выбора ресурсов сети для их моделирования в ЛИС. Подобная постановка была представлена в [9].

Исходные данные

$S = \{s_1, s_2, \dots, s_n\}$ – множество защищаемых ИР,

$N = \{1,2, \dots, n\}$ – множество индексов ресурсов.

$w_i > 0, \forall\, i \in N$ – стоимость защищаемых ресурсов (возможный ущерб при нарушении требований безопасности).

$c_{зi} > 0, \forall\, i \in N$ – стоимость защиты ИР посредством технологии ЛИС.

$c_{нi} > 0, \forall\, i \in N$ – стоимость проведения атаки на ИР.

$p_{лi} > 0, \forall\, i \in N$ – вероятность выбора i-го ложного ИР злоумышленником для проведения атаки.

Показатели игроков

Для стороны защиты введем переменную $p_i \in [0,1], \forall\, i \in N$, имеющую содержательный смысл вероятности конфигурации i-го реального ИР в системе ЛИС, переменные образуют вектор $\vec{P}$. Для стороны нападения введем переменную $q_i \in [0,1], \forall\, i \in N$, имеющую содержательный смысл вероятности атаки на i-ый ИР переменные образуют вектор $\vec{Q}$. Векторы $\vec{P}$ и $\vec{Q}$ определяют стратегии игроков.

В отношении каждого объекта для сторон защиты и нападения возможны две стратегии: сторона защиты моделирует ИР в ЛИС или не моделирует, сторона нападения проводит атаку на ресурс сети или нет. Матрицы игры для отдельного ИР в рамках взаимодействующих сторон могут быть построены аналогично тем, что приведены в [9].

После исключения компонент показателей, определяющих затраты игроков, и их переноса в ограничения, как это было сделано в [10], была получена модель игры с нулевой суммой. Таким образом, выигрыш стороны нападения, который можно рассматривать как результат игры «атакующих» отдельные ИР, определяется максимальным ущербом, который может быть нанесен стороной нападения при атаке на реальные ИР, минус предотвращенный ущерб стороной защиты:

$$F_{\text{н}}(\vec{P}, \vec{Q}) = -F_{\text{н}}(\vec{P}, \vec{Q}) = \sum\nolimits_{i \in N} [p_i q_i p_{лi} w_i - q_i w_i].$$

Ограничения

Для стороны защиты ограничения на ресурсы, выделяемые на защиту:

$$\sum_{i \in N} c_{зi} p_i \leq C_з^{max},$$

где $C_з^{max}$ – максимальный размер ресурсов, выделенных на ЛИС. Аналогично для стороны нападения:

$$\sum_{i \in N} c_{нi} q_i \leq C_н^{max},$$

где $C_н^{max}$ – максимальный размер ресурсов, выделенных на проведение атак.

Каждая из сторон стремится выбрать такую стратегию, чтобы максимизировать свой показатель (выигрыш). Решением подобной игры может стать поиск седловой точкой, т.е. пары $(\overrightarrow{P_0}, \overrightarrow{Q_0}) \in M_p \times M_q$, где M_p, M_q– множество допустимых векторов $\vec{P}, \vec{Q}$ соответственно, при которой игрокам не выгодно отклоняться от выбранных стратегий. Компоненты вектора-стратегии $\overrightarrow{P_0}$, имеющие содержательный смысл вероятности моделирования i-го реального ресурса в ЛИС, определяют ИР, которые будут играть роль «ловушек». Для решения данной задачи можно предложить алгоритм, основанный на игровой модели и принципе равномерной защищенности объектов, предложенный в [14].

3.2 Использование методов теории игр для устранения уязвимостей в программном обеспечении.

В связи с быстрыми темпами развития информационных технологий усложняется задачи обеспечения информационной безопасности в каждой организации. Существуют разные методы и подходы для решения задач обеспечения информационной безопасности. Все они по-разному, но вполне успешно решают поставленную задачу в рамках, которые предусмотрел их разработчик. Для обеспечения сохранности и целостности информации и защищенности поддерживающей ее инфраструктуры от любых случайных или злонамеренных воздействий, организация использует различные способы преград для угроз информационной безопасности. Но что делать, если уязвимость появляется в программном продукте? Проблема обнаружения уязвимостей в программном продукте исследуется довольно давно, и существуют базы данных, содержащие перечни известных уязвимостей и их характеристики. Существование отрытых баз данных, имеющих описание уязвимостей, позволяет специалистам по информационной безопасности использовать их в прогнозировании и, возможно, помогает устранить их в программном продукте.

В разделе на основе информации о программном обеспечении, установленном в организации, и использовании открытой БД NVD (National Vulnerability Database) об уязвимостях предложена методика оценки рисков, связанных с конкретными уязвимостями в программном обеспечении. Результатом применения этой методики является отыскание множества наиболее опасных уязвимостей, которые необходимо устранять в первую очередь. Для оценки рисков были использованы методы теории игр. Выборка интересующих партнеров игры (атаки и защиты) уязвимостей из БД по определенным направлениям (ожидаемый результат, программное обеспечение и т.д.) дает возможность практической реализации вычислительного алгоритма.

Обоснованность применения теории игр для решения задачи противоборства сторон за информационный ресурс, следует из предложения об использовании игровых методов. *Матрица игры приведена в Таблице 3.1.*

Элемент платежной матрицы должен содержать сведения о выборе решения, как атакой, так и защитой. При совпадении решений i, j элемент матрицы a_{ij} равен нулю. В любом случае:

$$a_{ij} = I_i \varphi_{ij} R_i, \tag{3.1}$$

где R_i – степень распространенности атаки в программных системах организации. Чем больше этот показатель, тем больше вероятность того, что организация подвергнется атаке, использующей определенную уязвимость. Этот показатель соответствует значению *TD (target distribution)* в системе оценки уязвимостей *CVSS*, который в свою очередь равен отношению количества программных систем, которым угрожает данная уязвимость, к общему числу программных систем в организации. I_i – характеризует влияние уязвимости на

целостность, доступность и конфиденциальность системы. Это значение берется из БД *NVD*. φ_{ij} – функция затрат на i −ую атаку и на j −ую защиту. Выбор функции $\varphi({}^{c_j}/_{c_i})$ производится, при следующих логически очевидных ограничениях:

$$\varphi_{ij} = 0 \text{ только при } {}^{c_j}/_{c_i} = 0,$$

$$c_i \leq c_j, \tag{3.2}$$

$\varphi_{ij} = 1$ только при $c_i = 0$.

Таблица 3.1. Матрица игры

	1	**2**	**…**	**n**	$\sum_3^i = \sum_{j=1}^{n} q_j a_{ij}$
1	a_{11}	a_{12}	…	a_{1n}	$\sum_3^1$
2	a_{21}	a_{22}	…	a_{2n}	$\sum_3^2$
…	…	…	…	…	
m	a_{m1}	a_{m2}	…	a_{mn}	$\sum_3^m$
$\sum_a^j = \sum_{i=1}^{m} p_i a_{ij}$	$\sum_a^1$	$\sum_a^2$	…	$\sum_a^n$	

При построении φ_{ij} используется экспоненциальная функция затрат, достаточно гибкая и легко согласуемая с ограничением (3.2):

$$\varphi_{ij} = 1 - e^{-a\frac{c_j}{c_i}}, \tag{3.3}$$

где c_j – затраты на j −ю защиту, c_i – затраты на i −ю атаку, a – управляющий множитель ($a>0$). Затраты на j −ю защиту (c_j) назначается ЛПР, а затраты на i −ю атаку (c_i) равны значению параметра *Exploitability* в БД *NVD*.

Атака соответствует одному выбранному варианту из множества P_m допустимых распределений $P_m = \{(p)_s\}_{s=1}^{s=M}$ $(p)_s = \{p_1, \dots, p_m\}$. Можно, согласно подходу из теории игр, исходить из гипотезы о том, что выбор осуществляется сознательно с целью максимизировать наименьший ожидаемый средний выигрыш:

$$max_{p_m}\{\min(\sum_{i=1}^{m} a_{i1}p_i, \dots, \sum_{i=1}^{m} a_{in}p_i)\} \quad (3.4)$$

Защита может сознательно выбирать стратегию из множества Q_n допустимых распределений $Q_n = \{(q)_r\}_{r=1}^{r=N}$ $(q)_r = \{q_1, \dots, q_n\}$, чтобы минимизировать наибольший ожидаемый средний проигрыш:

$$min_{Q_n}\{\max(\sum_{j=1}^{n} a_{1j}q_j, \dots, \sum_{j=1}^{n} a_{mj}q_j)\} \quad (3.5)$$

Минимаксный ожидаемый проигрыш защиты больше или равен максиминного ожидаемого выигрыша атаки. В случае их равенства стратегия именуется оптимальной. В качестве критерия останова избрано такое состояние процесса, когда наибольшее возможное уменьшение средних эффективностей $\sum_a^j = \sum_{i=1}^{m} p_i a_{ij}$ $\sum_3^i = \sum_{j=1}^{n} q_j a_{ij}$ становится меньше задаваемых ограничений:

$$\left|\sum_{j=1}^{n} q_j a_{ij} - \sum_{j=1}^{n} q_j a_{rj}\right| \le \varepsilon_1 \text{ при всех } i = \overline{1,m} \text{ и } r = \overline{1,m}, \quad (3.6)$$

$$\left|\sum_{i=1}^{m} p_i a_{ij} - \sum_{i=1}^{m} p_i a_{ir}\right| \le \varepsilon_2 \text{ при всех } j = \overline{1,n} \text{ и } r = \overline{1,n}. \quad (3.7)$$

Оставшиеся варианты считаются искомым решением игры. На основании вышеуказанной методики создан программный продукт, алгоритм которого содержит следующие этапы:

1. построение матрицы игры при равновероятном выборе атак/защит;
2. присвоение вероятностей выбора атаки/защиты;
3. расчет средних эффективностей;
4. проверка выполнения условия удаления наименее эффективных из атак/защит и принятие решения о продолжении процедуры;
5. удаление наименее эффективных из атак или (и) защит.

Пункты 2 – 5 выполняются до тех пор, пока не выполнится условие останова процедуры минимизации платежной матрицы.

3.3. Игровой метод оценки ущерба от реализации злоумышленником внутренних угроз.

Проблема защиты конфиденциальной информации в общей теории защиты информации весьма актуальна. Это связано с очевидными и вполне объективными закономерностями, которые проявляются в современных непростых условиях информационных взаимоотношений. Исследования показывают достаточно устойчивую тенденцию утечки конфиденциальной информации, связанную с реализацией злоумышленником внутренних угроз. Анализ имеющейся статистической информации свидетельствует о том, что 65% до 85% утечки конфиденциальной информации является следствием воздействия внутренних угроз на автоматизированную информационную систему, ее относительно самостоятельные структурные элементы. С точки зрения эффективности защиты конфиденциальной информации, представляется возможным воспользоваться таким понятием, как величина ущерба от реализации злоумышленником внутренней угрозы.

Так как величина ущерба носит случайный характер, то в качестве критерия может быть принята вероятность события нарушения конфиденциальности информации, следствием которого является нанесение ущерба собственнику конфиденциальной информации. Пусть на автоматизированную информационную систему воздействует конечное множество внутренних угроз. Каждая *i-я* внутренняя угроза характеризуется вероятностью возникновения – $P_{вуi}$, вероятностью парирования – $P_{\text{вуi}}^{\text{пар}}$ и величиной ущерба от воздействия *i-й* угрозы на конфиденциальную информацию – $\Delta W_{\text{вуi}}$ Тогда, предотвращенный ущерб от воздействия на конфиденциальную информацию n внутренних угроз, при условии их независимости и аддитивности последствий, имеет вид [5,6]:

$$W = \sum_{i=1}^{n} P_{\text{вуi}} P_{\text{вуi}}^{\text{пар}} \Delta W_{\text{вуi}}. \qquad (3.8)$$

Не трудно заметить, что произведение

$$P_{\text{вуi}} \Delta W_{\text{вуi}} = Q_i\,, \qquad (3.9)$$

где Q_i - степень риска от реализации злоумышленником i-й внутренней угрозы.

Вероятности $P_{\text{вуi}}$ и $P_{\text{вуi}}^{\text{пар}}$ характеризуют, соответственно, возможности (временные, экономические) злоумышленника по реализации i-й угрозы и возможности собственника конфиденциальной информации по применению защитных механизмов. Несмотря на кажущуюся простоту выражения (3.8), следует отметить, что такому подходу присущи недостатки, связанные с отсутствием достаточно компетентной априорной статистической информации по частоте реализации внутренних угроз. Поэтому в процессе оценки и анализа величины ущерба с использованием выражения (3.8) исходные данные, как правило, принимаются эмпирически. Проблема, связанная с защитой

конфиденциальной информацией, относится к трудно формализуемым процедурам. Это связано с тем, что при решении такой задачи в большинстве случаев необходимо принимать решение в условиях отсутствия или неполной информации. О фактических силах и средствах, применяемых как собственником информации, так и злоумышленником. При этом неполнота и неопределенность информации сказывается на действиях двух сторон с противоположными интересами.

Собственник информации должен определить и реализовать защитные механизмы в соответствии с ценностью защищаемой информации, а злоумышленник - определить и реализовать силы и средства в интересах несанкционированного получения конфиденциальной информации. Степень информированности игроков может характеризоваться некоторым пороговым уровнем информации, переводящим систему из исходного i - го в последующее j - е состояние. Таким образом, при анализе степени информированности игроков необходимо учитывать, что накопление информации о поведении противоположных сторон и принятие решения зависит от применяемых методов и средств несанкционированного доступа к информации, а также от степени защищенности (ценности) информации. Указанную ситуацию можно представить следующим образом (рис.3.2).

Как показано на рис. 3.1, поведение игроков в условиях неполной (ограниченной) информированности предполагает.

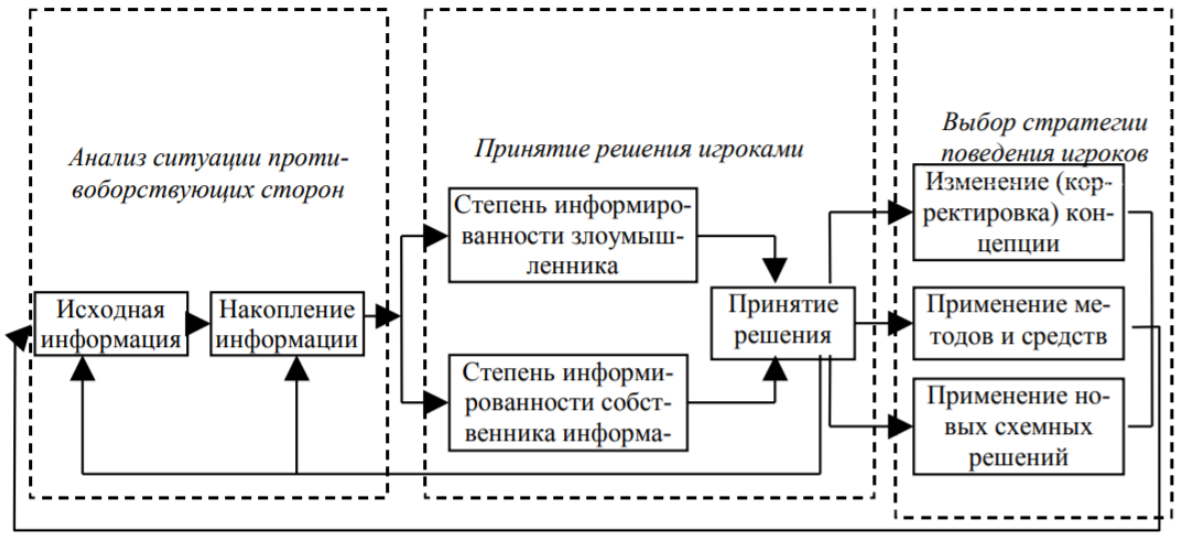

Рис. 3.1. Поведение игроков в зависимости от их информированности

1. Анализ ситуации противоборствующими сторонами, включающий априорный анализ исходной информации, а также информации, которая накапливается, систематизируется в течение длительного времени. Информация о неопределенных факторах противоборствующих сторон может быть получена на основе:

- прогнозирования условий применения (или изменения) игроками методов и средств защиты конфиденциальной информации и несанкционированного доступа к ней;

- анализа поведения сторон в процессе развития имевших место конфликтных ситуаций, возможных вариантов наиболее благоприятных (неблагоприятных) для сторон исходов;

- применения методов экспертных оценок, в случае необходимости, для получения недостающей информации.

2. Принятие решения игроками на основе степени их информированности о возможных силах и средствах несанкционированного доступа к конфиденциальной информации, применяемых защитных механизмов собственником информации.

3. Реализация принятого решения на основе выбора стратегии поведения игроков. Как видно из рис.3.1, в результате изменения информированности игроков принимаются решения, связанные с:

- изменением концепции поведения сторон, соответствующей перспективным направлениям теории и практики защиты информации;

- применением новых методов и средств противодействия сторон в интересах достижения поставленной задачи;

- применением новых схемных решений, позволяющих достичь более высоких характеристик эффективности противодействия.

Формализация содержательного описания конфликта – $x_i(t)$ представляет собой математическую модель, которую называют игрой, а участников конфликта – игроками, вида:

$$x_i(t) = \{x_i y_i, I_i J_i\}, \tag{3.10}$$

где x_i – множество возможных действий злоумышленника по несанкционированному доступу к *i-му* информационному ресурсу;

y_i – множество возможных действий собственника конфиденциальной информации по защите *i-го* информационного ресурса;

I_i – функция полезности действий злоумышленника по несанкционированному доступу к *i-му* информационному ресурсу;

J_i – функция полезности действий собственника конфиденциальной информации по реализации защитных механизмов *i-го* информационного ресурса.

Нетрудно заметить, что целью организации игровой модели в соответствии с выражением (3) является разработка рекомендаций по повышению эффективности поведения игроков в конфликтных ситуациях, то есть определение оптимальной стратегии каждого из игроков. Оптимальной считается такая стратегия, которая при многократном повторении игры обеспечивает игроку максимально возможный выигрыш или минимально возможный средний проигрыш. Пусть имеется игрок, обозначим его через A_j –

злоумышленник, покушающийся на конфиденциальную информацию. Предположим, что игрок А имеет две стратегии: A_1 - имеющимися силами и средствами реализовать внутреннюю угрозу; A_2 - не предпринимать мер по реализации внутренней угрозы. Пусть также имеется игрок В – собственник конфиденциальной информации. Игрок В имеет тоже две стратегии: B_1 – имеющимися силами и средствами обеспечить сохранность КИ; B_2 – не предпринимать никаких действий в отношении защиты КИ. Рассмотрим модель действий злоумышленника с целью несанкционированного доступа к конфиденциальной информации. Пусть в момент времени $t>0$ злоумышленник воздействует несанкционированным образом на конфиденциальную информацию, реализуя *i - ую* внутреннюю угрозу. По результатам воздействия возможны следующие исходы.

1. Угроза не реализовалась. Такой исход соответствует случаю, когда применяемые злоумышленником силы и средства несанкционированного доступа к конфиденциальной информации недостаточны, а применяемые защитные механизмы собственника информации достаточно эффективны и обеспечивают защиту конфиденциальной информации. Эта ситуация соответствует проигрышу злоумышленника, обозначим его через (- a), на величину затраченных им сил и средств.

2. Угроза реализовалась. В этом случае силы и средства злоумышленника по несанкционированному доступу к конфиденциальной информации Известия ЮФУ. Технические науки Тематический выпуск 46 более эффективны, чем защитные механизмы, применяемые собственником информации для ее защиты, либо когда собственник информации не применяет защитные механизмы. Указанная ситуация соответствует выигрышу злоумышленника, обозначим его через (b) , и проигрышу собственника конфиденциальной информации на величину, соответствующую ценности конфиденциальной информации.

3. Угроза злоумышленника, связанная с несанкционированным доступом к конфиденциальной информации, не применяется. Такая ситуация может иметь место, когда, во-первых, конфиденциальная информация злоумышленника не интересует, либо, когда, во-вторых, защитные механизмы собственника конфиденциальной информации значительно эффективнее, чем силы и средства, применяемые злоумышленником. В этом случае злоумышленник получает выигрыш, обозначим его через (c), так как он не расходует силы и средства несанкционированного доступа к конфиденциальной информации.

4. Защитные механизмы собственником информации не применяются, что соответствует ситуации, когда отсутствуют возможности по защите конфиденциальной информации, либо, когда отсутствует информация о потенциальных возможностях злоумышленника. В свою очередь, злоумышленник не воспользовался благоприятной для него ситуацией и не применяет угрозы безопасности конфиденциальной информации. Такая ситуация соответствует проигрышу злоумышленника, обозначим его через (- d),

на величину ценности той информации, которую он мог бы получить в результате применения угрозы безопасности конфиденциальной информации с целью несанкционированного доступа к такой информации. Все перечисленные исходы от взаимодействия двух сторон с противоположными интересами можно представить в виде матрицы;

$$M_{ij} = \begin{vmatrix} -a & b \\ c & -d \end{vmatrix} \quad (3.11)$$

Матрица (3.11) является математической моделью игрового метода принятия решения злоумышленником и собственником конфиденциальной информации в условиях неполной (ограниченной) информации. Такая игровая модель применяется для оценки и прогнозирования достигнутого уровня защиты информации с учетом выбора наиболее целесообразной стратегии поведения игроков. При многократном повторении игры реализация оптимальных стратегий обеспечит игроку максимально возможный средний выигрыш.

Контрольные вопросы

1. Раскройте содержание технологии "Honeypot".

2. На какие параметры влияет ложная информационная система?

3. Для каких локальных вычислительных сетей используется технология ловушек?

4. Как оценивается предотвращенный ущерб?

5. Поясните формирование ограничений при решении задачи.

6. Чему равен элемент платежной матрицы при совпадении решений?

7. Какой показатель характеризует влияние уязвимости на целостность, доступность и конфиденциальность информации?

8. Поясните алгоритм решения задачи.

9. Как оценивается предотвращенный ущерб от внутренних угроз?

10. Как накопленная информация влияет на поведение противоположных сторон?

Заключение

В настоящее время существует большое количество игровых методов решения задач в области защиты информации. Причем необходимо отметить вырисовывающиеся направления:

- выбор оптимальной структуры программно-аппаратных средств защиты информации;
- оценка уязвимостей риска и ущерба от возможных злоумышленных и незлоумышленных атак на информационные системы.

Обучающийся должен отдавать себе отчет в том, что для успешного и квалифицированного решения рассматриваемых задач студент должен хорошо знать методы исследования операций, функционального анализа и вариационного исчисления.

Полученные знания в процессе изучения рассматриваемых задач позволят более квалифицированно и компетентно решать вопросы построения политики информационной безопасности наряду с адаптивной программно-аппаратной системы защиты информации.

Литература

1. Домарёв В. В. Безопасность информационных технологий. Системный подход. –К.: ООО «ТИД ДС», 2004.

2. Шаньшин В. Ф. Защита компьютерной информации. Эффективные методы и средства. –М.: ДМК Пресс, 2010.

3. Бендот Д. С. Измерение и анализ случайных процессов. –М.: Мир, 1971.

4. Гентмахер Ф. Р. Теория матриц. –М.: Наука, 1988.

5. Майстренко В. А. Безопасность информационных систем и технологий. Омск, изд. – во ОГТУ, 2006.

6. Губанов Г. А. Новиков Д. А. Чхартишвили А. Г. Социальные сети: модели информационного влияния, управления и противоборства. –М.: Физматгиз, 2010.

7. BS ISO/IEC 17799:2005. Information technology – Security technics – code of practice for information security management.

8. ISO/IEC 27005:2008. Information technology – Security technics – Information security risk management.

9. Рассел С., Норвит П. Искусственный интеллект: современный подход. –Н.: Изд-й дом «Вильямс», 2005.

10. Корниченко А. А., Слюсаренко Н. М. Системы и методы обнаружения вторжений: современное состояние и направление совершенствования [электронный ресурс]. Режим доступа URL: hhtp://citforum.ru/security/internet/ids overview.

11. Лаврентьев А. В., Зязин В. П. О применении методов теории игр для решения задач компьютерной безопасности. Безопасность информационных технологий. 2013, №3, с. 19-24.

12. Руднев Д. О., Сычугов А. А. Задача автоматической генерации сигнатур для системы противодействия вторжениям в распределенных информационных системах. || Известия Тульского государственного университета. –Тула: изд-во ТулГУ, 2015. Вып. 7. С. 174-181.

13. Петросян Л. А., Зинкевич Н. А., Самина Е. А. Теория игр. –М.: Высшая школа. Книжный дом «Университет», 1998.

14. Быков А. Ю., Алтухов Н. О., Сосенко А. С. Задача выбора средств защиты информации в автоматизированных системах на основе модели антагонистической игры. Инженерный вестник МГТУ им. Н. Э. Баумана №4, 2014.

15. Pibil R., Lisy V., Kiekintveld C., Pechoucek M. Game thecretic model of strategic honeypot selection in computer networks, GameSec, 2012. LNCS Vol. 7638. 2012, pp. 201-220. DOI: 10.1007/978-3-642-342-66-0_12.

Оглавление