**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**ФАКУЛЬТЕТ**

**« КИБЕРНЕТИКА И**

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»**

**Кафедра**

**«Информационная безопасность банковских систем»**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**ОТЧЕТ**

**о научно-исследовательской работе**

*Применение теории матричных игр для оценки выбора средств защиты информации*

Исполнитель:

студент гр. Б02-44М \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Литюшкин Е.Н.

(подпись, дата)

Научный руководитель:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Будзко В.И.

(подпись, дата)

Консультант:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Грубов Ф.В.

(подпись, дата)

Зам. зав. каф. 44

по учебной работе:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Запечников С.В.

(подпись, дата)

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Москва – 2014**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Содержание**

Термины и определения

Введение

Общие сведения о теории матричных игр

Методы решения матричных игр

Краткое описание объекта защиты

Моделирование угроз информационной безопасности

Оценка рисков информационной безопасности

Разработка мер минимизации выявленных рисков

Применение теории матричных игр для выбора средств защиты информации

Рассмотрение сценария реализации угрозы «Прекращение обработки данных банковских карт»

Выводы

**Термины и определения**

1. Актив (англ. asset) - все, что имеет ценность для организации и находится в ее распоряжении или то, что обладает ценностью или полезностью для организации, ее бизнес-операций и их непрерывности, и поэтому нуждается в защите, которая позволит обеспечить корректное выполнение бизнес-операций и непрерывность бизнеса (1).
2. Антагонистическая игра (игра с нулевой суммой, англ. zero-sum) — термин теории игр. Антагонистической игрой называется некооперативная игра, в которой участвуют два игрока, выигрыши которых противоположны (8).
3. Угроза информационной безопасности — совокупность условий и факторов, создающих опасность нарушения информационной безопасности (2).
4. Риск - сочетание вероятности нанесения ущерба и тяжести этого ущерба. Потенциальная возможность использования уязвимостей активов организации угрозами ИБ для причинения ущерба организации, измеряемая с учетом вероятности реализации угроз ИБ и величины ущерба от реализации угроз ИБ.
5. Анализ рисков ИБ (англ. IS risk analysis): систематическое использование информации (исторических данных, результатов теоретического анализа, информированного мнения) для определения источников и количественной оценки рисков ИБ. Это процесс понимания происхождения риска и определения уровня риска. Анализ рисков ИБ обеспечивает базу для оценивания рисков ИБ, мероприятий по снижению рисков ИБ и принятия рисков ИБ (1).
6. Допустимый риск ИБ: риск ИБ, предполагаемый ущерб от которого организация в данное время и в данной ситуации готова принять (4).
7. Идентификация рисков ИБ (англ. IS risk identification): деятельность, процесс, по нахождению (выявлению), составлению перечня, исследования и описания элементов рисков ИБ (источников или опасности, событий, последствий и вероятности). Она включает идентификацию источников риска, событий, их причин и возможных последствий. Идентификация риска может включать статистические данные, теоретический анализ, обоснованную точку зрения и заключение специалиста, а также потребности заинтересованной стороны (3).
8. Источник угрозы ИБ: субъект (физическое лицо, материальный объект или физическое явление), активизирующий угрозу ИБ и переводящий ее из разряда потенциальной опасности нарушения свойств ИБ (конфиденциальности, доступности, целостности и т. д.) активов организации в реально происходящее нарушение этих свойств.
9. Количественная оценка или установление значения рисков ИБ (англ. IS risk estimation): деятельность, или процесс, по присвоению значений вероятности и последствий рисков ИБ. Количественная оценка рисков ИБ может учитывать стоимость, прибыль, интересы причастных сторон и другие переменные, рассматриваемые при оценивании рисков ИБ (3).
10. Остаточный риск ИБ (англ. IS residual risk): риск ИБ, остающийся после обработки риска ИБ (3).
11. Угроза ИБ (англ. information security threat): совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения свойств ИБ – конфиденциальности, доступности и/или целостности информации/информационных активов организации (2).
12. Уязвимость (англ. vulnerability): любая характеристика или свойство информационной системы, обуславливающее возможность реализации угроз ИБ обрабатываемой в ней информации, или слабое место в инфраструктуре организации, включая СОИБ, которое может быть использовано для реализации или способствовать реализации угрозы ИБ (2)(5).
13. Хост: устройство в сети, имеющее свой уникальный адрес. В данной работе чаше называется сервером.
14. Межсетевой экран (МЭ): локальное (однокомпонентное) или функционально-распределенное средство (комплекс), реализующее контроль за информацией, поступающей в автоматизированную систему (АС) и/или выходящей из АС, и обеспечивает защиту АС посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС.
15. Бизнес-процесс: множество из одной или нескольких упорядоченных во времени, логически связанных и завершенных видов деятельности, в совокупности поддерживающих деятельность организации и реализующих ее политику, направленную на достижение поставленных целей.
16. Доступность: свойство информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие право доступа, могут реализовывать их беспрепятственно (англ. availability).
17. Конфиденциальность: свойство, обеспечивающие недоступность или нераскрываемость информации для неавторизованного субъекта, устройства или процесса (англ. confidentiality).
18. Ба́нковская ка́рта — пластиковая карта, привязанная к одному или нескольким расчетным счетам в банке. Используется для оплаты товаров и услуг, в том числе через Интернет, а также снятия наличных. Карты бывают дебето́вые и кредитные. Дебето́вые карты используются для распоряжения собственными деньгами, находящимися на расчетном счете в банке. Кредитные карты используется для распоряжения деньгами банка, которые при совершении платежа автоматически берутся у банка в кредит (их требуется вернуть банку).
19. Фрод (от англ. fraud) — вид мошенничества в области информационных технологий, в частности, несанкционированные действия и неправомочное пользование ресурсами и услугами. Мошенничество с помощью кредитных карт (кардинг включает в себя кражу данных карты в интернете (фишинг), копирование информации, содержащейся на магнитной полосе карты (скимминг), а также мошенничество при оплате при физическом отсутствии карты (Card not present transaction англ. ).
20. Мошенничество с платежными картами, кардинг (от англ. carding) — вид мошенничества, при котором производится операция с использованием платежной карты или ее реквизитов, не инициированная или не подтвержденная ее держателем. Реквизиты платежных карт, как правило, берут со взломанных серверов интернет-магазинов, платежных и расчётных систем, а также с персональных компьютеров (либо непосредственно, либо через программы удаленного доступа, «трояны», «боты» с функцией формграббера). Кроме того, наиболее распространённым методом похищения номеров платежных карт на сегодня является фишинг (англ. phishing, искаженное «fishing» — «рыбалка») — создание мошенниками сайта, который будет пользоваться доверием у пользователя, например — сайт, похожий на сайт банка пользователя, через который и происходит похищение реквизитов платежных карт .
21. Мошенничество — хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.
22. Linux, Apache, MySQL, PHP – операционная система, web сервер, система управления реляционными базами данных и интерпретируемый язык программирования. Популярны в России, встречаются в реально существующих процессингах.
23. Процессинг – компания или подразделение банка занятое обработкой данных банковских карт.
24. Ssh, telnet, rdp, Https, SOAP – протоколы обмена данными широко применяемые в сети интернет.
25. Мерчант – организация или лицо, клиент процессинга.
26. Теория игр — математический метод изучения оптимальных стратегий в играх. Под игрой понимается процесс, в котором участвуют две и более сторон, ведущих борьбу за реализацию своих интересов. Каждая из сторон имеет свою цель и использует некоторую стратегию, которая может вести к выигрышу или проигрышу — в зависимости от поведения других игроков. Теория игр помогает выбрать лучшие стратегии с учётом представлений о других участниках, их ресурсах и их возможных поступках (8).
27. DDOS – распределённая атака, направленная на отказ в работе сервиса. Обычно путём исчерпания аппаратных ресурсов.
28. Application Firewall – программное или программно-аппаратное средство способное «понимать» протокол передачи данных прикладного уровня и предназначенное для выявления и предотвращения атак через анализируемый протокол.

**Введение.**

В соответствии со стандартами Банка России в основе исходной концептуальной схемы ИБ лежит противоборство собственника и злоумышленника с целью получения контроля над информационными активами. Таким образом, уже на уровне концептуальной схемы ИБ мы имеем дело с «игрой» в том смысле, в котором данный термин применяется в математической теории игр. Теория игр представляет собой весьма обширный раздел прикладной математики, поэтому имеет смысл рассмотреть некоторую её часть. Целью данной работы является рассмотрения возможности применения теории матричных игр к вопросу выбора средств защиты информации. Для придания рассуждениям конкретики будет использованы результаты, полученные в защищённой ранее работе «Оценка и минимизация рисков ИБ для процессинга банковских карт». В рамках указанной работы была произведена инвентаризация активов, моделирование угроз и нарушителей и выбор организационных и технических мер минимизации рисков информационной безопасности для компании занятой обработкой данных банковских карт. Также была произведена оценка стоимости активов, стоимости рисков и рассчитан период возврата вложений в выбранные защитные меры. В настоящей работе предполагается обобщить методику выбора мер минимизации рисков при помощи теории матричных игр и рассмотреть границы применимости подобного похода.

**Общие сведения о матричных играх**

Рассмотрим игру, в которой участвуют два игрока, причем каждый из них имеет конечное число стратегий. Обозначим для удобства одного из игроков через А, а другого через В.

Предположим, что игрок А имеет m стратегий: , , …, а игрок В – n стратегий: , , …,

Пусть игрок А выбрал стратегию , а игрок В – стратегию Будем считать, что выбор игроками стратегий и однозначно определяет исход игры – выигрыш игрока А и выигрыш игрока В, причем эти выигрыши связаны равенством =.

Последнее условие показывает, что в рассматриваемых обстоятельствах выигрыш одного из игроков равен выигрышу другого, взятому с противоположным знаком. Поэтому при анализе такой игры можно рассматривать выигрыши только одного из игроков. Пусть это будет, например, выигрыши игрока А.

Если нам известны значения выигрыша при каждой паре стратегий , i = 1,2,…,m, j = 1,2,…,n, то их удобно записывать или в виде матрицы, строки которой соответствуют стратегиям игрока А, а столбцы – стратегиям игрока В (рис. 1.),

Рис. 1. Общий вид платёжной матрицы матричной игры

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  | **…** |  |
|  |  |  | *...* |  |
|  |  |  | *...* |  |
| **…** | *...* | *...* | *...* | *...* |
|  |  |  | *...* |  |

Полученная матрица имеет размер m n и называется матрицей игры или платежной матрицей.

Матричной игрой (при двух участниках) называется игра, в которой выигрыши первого игрока (проигрыши второго игрока) задаются матрицей. Матричные игры относятся к разряду так называемых антагонистических игр, т. е. игр, в которых интересы игроков прямо противоположны.

Суммируя сказанное: под матричными играми понимается игра двух лиц с нулевой суммой, имеющих конечное число стратегий. Выигрыш определяется матрицей игры (матрицей платежей), она же является Нормальной формой игры.

Равновесная ситуация

Каждый из игроков стремится максимизировать свой выигрыш с учётом поведения противодействующего ему игрока. Поэтому для игрока A необходимо определить минимальные значения выигрышей в каждой из стратегий, а затем найти максимум из этих значений, то есть определить величину Vн, или найти минимальные значения по каждой из строк платёжной матрицы, а затем определить максимальное из этих значений. Величина Vн называется максимином матрицы или нижней ценой игры.

Величина выигрыша игрока A равна, по определению матричной игры, величине проигрыша игрока B. Поэтому для игрока B необходимо определить значение Vв=.

Или найти максимальные значения по каждому из столбцов платёжной матрицы, а затем определить минимальное из этих значений. Величина Vв называется минимаксом матрицы или верхней ценой игры.

В случае, если значения Vн и Vв не совпадают, при сохранении правил игры (коэффициентов ) в длительной перспективе, выбор стратегий каждым из игроков оказывается неустойчивым. Устойчивость он приобретает лишь при равенстве Vн = Vв = V. В этом случае говорят, что игра имеет решение в чистых стратегиях, а стратегии, в которых достигается V - оптимальными чистыми стратегиями. Величина V называется чистой ценой игры.

Цена игры совпадает с элементом матрицы игры A, расположенным на пересечении -й строки (стратегия игрока A) и -го столбца (стратегия игрока B), - минимальным в своей строке и максимальным в своем столбце.

Этот элемент называют седловой точкой матрицы A или точкой равновесия, а про игру говорят, что она имеет седловую точку.

Стратегии и , соответствующие седловой точке, называют оптимальными, а совокупность оптимальных ситуаций и цена игры – решением матричной игры с седловой точкой.

Седловых точек в матричной игре может быть несколько, но все они имеют одно и то же значение.

Матричные игры с седловой точкой важны и интересны, однако более типичным является случай, когда применение описанного алгоритма приводит к неравенству Vн < Vв.

Смешанные стратегии

      В играх без седловых точек любые стратегии игроков, в том числе максиминная и минимаксная, в известном смысле, являются ненадежными. В этих играх среди имеющихся у игроков стратегий нет таких, которые гарантировали бы получение возможно большего выигрыша: как бы ни рассуждал игрок при выборе своей стратегии, его противник может восстановить ход его мыслей и наказать его. Оказывается, наилучшим способом сохранения тайны является случайный выбор стратегии. В этом случае противник не может догадаться о том, какая стратегия будет выбрана, поскольку даже сам игрок не знает, каков будет результат случайного выбора. Больше того, и это главное, оказалось, что разумно построенный случайный выбор стратегии гарантирует игрокам определенный исход игры, как это имело место в играх с седловой точкой. Такой способ выбора, предложенный французским математиком Э.Борелем, получил название смешанной стратегии. Суть смешанной стратегии заключается в одновременном задействовании или "смешивании" нескольких стратегий, каждой из которых предписывается определенный вес.

Приведем простой пример смешивания стратегий.

 Арбитр футбольного матча, чтобы определить первую атакующую команду, бросает монету, т.е. вместо того, чтобы принять определенное решение, выбирает пару чисел (1/2, 1/2), где первое число – есть вероятность того, что атакующей будет первая команда, второе - вероятность для второй команды.   
        Четыре студентки, проживающие в одной комнате, тянут четыре спички, одна из которых короче остальных. Та "неудачница", которой достанется короткая спичка, должна вымыть пол. Поступая так, студентки добавляют к своим четырем стратегиям: "моет пол Галя", "поет пол Вера", "моет пол Наташа", "моет пол Лена" еще одну, а именно, вектор х=(1/4, 1/4, 1/4, 1/4). Дополнительная стратегия х состоит в смешивании четырех стратегий, каждой с вероятностью 1/4.

     Чтобы отличить от стратегий вида х первоначальные стратегии игроков будем называть их чистыми стратегиями. Мы переходим теперь к формальному определению смешанных стратегий.

Пусть дана игра A= ,

в которой у игрока A - m, а у игрока B - n чистых стратегий.   
        Смешанной стратегией игрока называется вероятностное распределение на множестве его чистых стратегий.

Смешанная стратегия игрока A в игре есть вектор , где (i=1,...,m) - вероятность выбора i-й чистой стратегии. Так как - вероятность, то 0 и, поскольку одна из m чистых стратегий обязательно будет выбрана, то представляет собой вероятность полной группы событий. Значит,=1.

Аналогично, смешанная стратегия игрока B есть вероятностный вектор Y, где (j=1,...,n) выбора j-й чистой стратегии, 0 и =1.

В этих условиях каждая обычная ситуация по определению является случайным событием и ввиду независимости X и Y реализуется с вероятностью . Поскольку в этой ситуации игрок A получает выигрыш , то математическое ожидание выигрыша в условиях ситуации в смешанных стратегиях равно = .

Это число принимается за средний выигрыш игрока A в ситуации в смешанных стратегиях .

Стратегии и называются оптимальными смешанными стратегиями игроков A и B соответственно, если выполнено следующее соотношение: .

Последнее равносильно тому, что

.

Величина V=, определяемая последней формулой называется ценой игры.

Набор , состоящий из оптимальных смешанных стратегий игроков A и B и цены игры, называется решением матричной игры.

Не всякая матричная игра имеет решение в чистых стратегиях. Благодаря введению смешанных стратегий становится возможным следующее важнейшее в теории игр утверждение.

Теорема 1 (о минимаксе). Любая матричная игра имеет решение в смешанных стратегиях.

Теорема о минимаксе, или основная теорема для матричных игр, впервые была доказана Дж. фон Нейманом.

существуют и равны между собой:

.

Более того, существует хотя бы одна ситуация в смешанных стратегиях , для которой выполняется соотношение

**Методы решения матричных игр**

Сравнительно просто решаются игры, в которых хотя бы один игрок имеет всего две чистых стратегии: игры 22, 2n, mn. Когда m, n>2 теория игр не имеет собственного точного метода. Такие игры сводятся к задачам линейного программирования и решаются методом симплекс-таблиц. Нужно заметить, что применение симплекс метода приводит к громоздким вычислениям уже для игры 3x3. Для игр больших размеров применяются приближенные методы.

Решение 22-игры

В общем случае игра 22 определяется матрицей

.

Прежде всего, необходимо проверить, есть ли у данной игры седловая точка. Если да, то игра имеет решение в чистых стратегиях, причём оптимальными стратегиями игроков A и B соответственно будут чистая максиминная и чистая минимаксная стратегии. Если же игра с матрицей выигрышей А не имеет решения в чистых стратегиях, то оба игрока имеют только такие оптимальные стратегии, которые используют все свои чистые стратегии с положительными вероятностями.

Пусть U = (ξ, 1 − ξ) оптимальная стратегия игрока A. Тогда

; .

Аналогично, если W = (η, 1 – η) – оптимальная стратегия игрока B, то

.

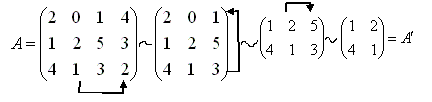
m n – игры

В некоторых случаях игры больших размеров можно упростить и привести к малым размерам. В основе такого преобразования лежит понятие доминирования стратегий.

Пусть дана m n - игра А. Говорят, что i-я стратегия игрока A доминирует его k-ю стратегия, если для всех j = 1,2,…,n. Говорят, что j-я стратегия игрока B доминирует его l-и стратегию, если для всех i = 1,2,…,m. .   
        Из определения видно, что доминирующая стратегия дает игроку выигрыш не хуже, чем доминируемая. Отсюда следует, что игрок всегда может обойтись без доминируемых стратегий, в частности, если есть одинаковые стратегии, то он может применять только одну из них. Поэтому в матрице А доминируемые стратегии (строки или столбцы) могут быть отброшены, а это приводит к матрице малых размеров. В результате выполнения доминирования получается игра, эквивалентная первоначальной, в смысле следующего утверждения.

Теорема 2. Пусть (x,y) - седловая точка m n - игры А, а () - седловая точка - игры A' (), полученной из А в результате исключения доминируемых стратегий. Тогда , для всех недоминируемых i, j: =0, для всех доминируемых i:

Пример 1. Рассмотрим игру



Стрелками показаны доминируемые стратегии. Получили 2х2-игру, в которой все стратегии недоминируемы. Игра эквивалентна первоначальной игре А, т.е. оптимальные стратегии в игре А имеют вид x=(0,),

        В результате вместо игры А мы можем решить более простую 2х2-игру .

Теперь мы можем указать общий порядок решения матричной игры:

проверить, существует ли решение в чистых стратегиях; если есть, то игра решена;

если нет решения в чистых стратегиях, то выполнить доминирование;

найти решение в смешанных стратегиях.

Решение игр 2

Для построения решений 2 - игр существует эффективный метод, основанный на простых геометрических соображениях. Этот метод называют графическим.

Рассмотрим игру 2n: .



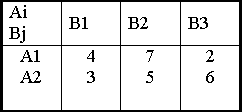
Задача игрока A состоит в максимизации функции .Так как , мы имеем .



Таким образом, v является минимумом n линейных функций одной переменной ; можно вычертить графики этих функций и затем максимизировать их минимум g() графическими методами. Покажем на примере игры 23.

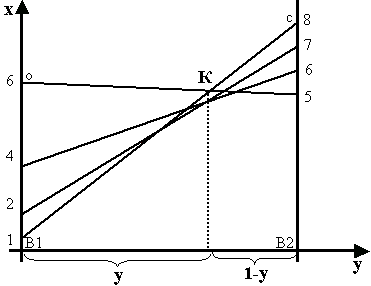
Поясним на примере 1.

Рис. 2. Платёжной матрицы матричной игры



На плоскости хОу введём систему координат и на оси Ох отложим отрезок единичной длины А1, А2, каждой точке которого поставим в соответствие некоторую смешанную стратегию игрока 1 (х, 1-х). В частности, точке А1 (0;0) отвечает стратегия А1, точке А2 (1;0) - стратегии А2 и т. д.

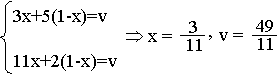
Рис. 3. Выбор стратегии матричной игры



На перпендикуляре А1 будем откладывать выигрыш игрока 1 при стратегии 1, на втором - при стратегии А2.

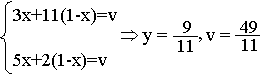
Таким образом, ординаты точек, принадлежащих ломаной оMNс определяют минимальный выигрыш игрока 1 при применении им любой смешанной стратегии. Эта минимальная величина является максимальной в точке N; следовательно, этой точке соответствует оптимальная стратегия Х\* = (х, 1-х), а её ордината равна цене игры. Координаты точки N находим как пересечение прямых.

Соответствующие два уравнения имеют вид



следовательно, х = (3/11,9/11), при цене игры v = 49/11. таким образом мы можем найти оптимальную стратегию при помощи матрицы

Оптимальные стратегии для игрока 2 можно найти из системы



Укажем основные этапы нахождения решения игры 2n (m2):

* Строим прямые, соответствующие стратегиям второго (первого) игрока.
* Определяем нижнюю (верхнюю) огибающую графиков, соответствующих столбцам (строкам).
* Находим две стратегии второго (первого) игрока, которым соответствует две прямые, пересекающиеся в точке с максимальной (минимальной) ординатой.
* Определяем цену игры и оптимальные стратегии игроков.

Симплекс-метод является самым распространенным и наиболее универсальным методом решения задач линейного программирования (ЗЛП). Любую матричную игру можно свести к ЗЛП, точнее, задачам нахождения оптимальных стратегий первого и второго игроков в каждой матричной игре соответствует пара двойственных ЗЛП. Благодаря этому становится возможным применение симплекс-метода для решения матричной игры.   
        Пусть игрок A играет оптимально, а игрок B вместо выбирает чистую стратегию j. По определению седловой точки, каждому такому отклонению соответствует неравенство:

При j=1

При j=2

При j=n

    Предположим, что V>0. Разделим обе части каждого неравенства на V и введем новую переменную . Тогда мы имеем:

Рассмотрим сумму

Z==1/V.

 Целью игрока A является получение максимального выигрыша. Легко видеть, что это равносильно уменьшению функции Z. Пользуясь новыми переменными, задачу вычисления оптимальной стратегии игрока A можем теперь сформулировать так:

Найти такие что Z= при ограничениях , i = 1,2,…,m, j = 1,2,…,n, . Здесь , Z=1/V.

Рассуждая аналогично, задачу нахождения оптимальной стратегии игрока B можно написать следующим образом:

Найти такие что W= при ограничениях , i = 1,2,…,m, j = 1,2,…,n, . Здесь , W=1/V.

 Задачи представляют собой пару двойственных задач линейного программирования. Суть применения симплекс-метода такова: решая задачу, находим ее оптимальный план и значение , V, .

**Краткое описание объекта защиты**

Для придания большей определённости дальнейшим рассуждениям необходимо кратко описать информационную систему компании занятой обработкой данных банковских карт. Данное описание не будет содержать сведений об «офисной» составляющей. Кроме того предполагается, что уже применены все необходимые в соответствии с PCI DSS меры безопасности. Рассматриваемая информационная система отделена от сети интернет межсетевым экраном. Межсетевой экран надёжен и корректно настроен. Также предполагается применение корректных процедур архивирования данных банковских карт, защиты от вредоносного программного обеспечения, ведения системных журналов, синхронизации времени и строгой политики паролей.

В качестве стандартной среды на всех серверах установлен Linux, применяется web сервер apache, интерпретатор php и система управления базами данных MySQL. Единственным средством удалённого управления является протокол ssh. Данные банковских карт поступают на платёжный шлюз непосредственно от клиентов мерчантов перенаправляемых со страница интернет-магазинов. Весь информационный обмен с клиентами мерчантов защищён при помощи протокола https. Информационный обмен с банками и иными платёжными системами осуществляется путём передачи SOAP сообщений через HTTPS или обменом CVS файлами через sftp. Все сервера размещены в удалённом центре обработки данных, сертифицированном в соответствии со стандартом PCI-DSS.

Также для упрощения дальнейших рассуждений введём краткий список серверов входящих в процессинг:

* Сервер приложений. Выполняет роль шлюза для приёма соединений от клиентов мерчантов, и банков. Извне доступен как web сервер. На нём исполняется основная часть программного обеспечения процессинга, написанная на php.
* Сервер баз данных. Поддерживает систему управления базами данных MySQL. Из вне недоступен. Доступен с сервера приложений через MySQL.
* Терминальный сервер. Выполняет роль сервера разработки. Извне доступен как ssh и web сервер. На нём происходит программного обеспечения процессинга, для этого установлен php, apache и MySQL. С данного сервера через протокол ssh доступны все остальные узлы и сетевое оборудование.

**Оценка информационных активов компании занятой обработкой информации банковских карт**

Обработку данных банковских карт, возможно, рассмотреть как совокупность нескольких связанных бизнес-процессов.

Вся деятельности процессинга начинается с подключения нового клиента - мерчанта. Мерчантом называют компанию продающую товары или услуги в сети интернет и принимающей банковские карты к оплате. Бизнес процессы, технологические процессы, и особенности архитектуры информационной системы мерчанта обычно несовместимы напрямую с аналогичными сущностями банка. Это приводит с одной стороны к невозможности непосредственного взаимодействия с автоматизированной банковской системой, с другой к необходимости в существовании информационного посредника – процессинга. Задачей посредника является предоставление возможности взаимодействия информационной системы мерчанта с автоматизированными системами банков таким, образом, чтобы у мерчанта появилась возможность принимать к оплате банковские карты. На входе данного процесса находится поток заявок от клиентов. На выходе – набор заявок к техническому персоналу по разработке или доработке программного обеспечения процессинга.

Вторым бизнес-процессом процессинга является разработка или доработка программного обеспечения процессинга. Обычно для этого создаётся группа технических специалистов занятая разработкой программного обеспечения и эксплуатаций информационной системы процессинга. Результатом данного процесса является программный код и настройки компонентов информационной системы предназначенной для обработки банковских карт.

Третьим бизнес-процессом является собственно процесс обработки данных банковских карт. Данный бизнес-процесс во многом совпадает с технологическим процессом обработки информации о банковских картах поступающей от мерчантов и их клиентов. Кратко его возможно описать как получение нужной информации через сеть интернет и набор платёжных шлюзов. Проверку волосности полученной информации. Архивирование нужных сведений. Аккумуляция полученной информации со справочными данными, например курсами валют и формирование в результате сообщений данных и электронных платёжных поручений в формате принятом в участвующих во взаимодействии банках и платёжных системах.

После рассмотрения бизнес-процессов нетрудно выделить основные информационные активы компании занятой обработкой данных банковских карт:

* Данные банковских карт;
* Персональные данные держателей карт;
* Денежный поток, проценты от которого формируют доход процессинга;
* Программное обеспечение, применяемое для обработки данных банковских карт.
* Проведём приблизительную оценку активов. Данные необходимые для данной оценки получены в ходе неформального общения с представителями ряда российских банков.
* Средний остаток на карточном счёте физического лица – порядка 100 тысяч рублей;
* Среднее количество транзакций, совершаемое за сутки – 20 тысяч;
* Средняя величина транзакции – 1 тысяча рублей;
* В среднем 1 из 10 тысяч транзакций имеет мошеннический характер;
* Приблизительная численность уникальных физических лиц, чьи данные находятся в оперативной обработке – 10 тысяч человек;
* Стоимость персональных данных одного пользователя из России – 10 тысяч рублей;
* Стоимость работы квалифицированного программиста – 100 тысяч рублей в месяц;
* Трудозатраты на разработку и доработку программного обеспечения процессинга составляют около 30 человеко-лет.

Следует уточнить, что после завершения оперативной обработки данные банковской карты должны быть переданы в архив в зашифрованном виде. Мы будем считать хранение в архиве надёжным.

Под стоимостью персональных данных понимается сумма иска, который может быть предъявлен за их утечку или ненадлежащую обработку. К сожалению судебная статистика по данному вопросу пока отсутствует, поэтому данная переменная получена полностью эвристическим путём.

Применяя полученные цифры можно легко рассчитать:

* Стоимость данных банковских карт находящихся в оперативной обработке – 10 тысяч карт X 100 тысяч рублей = 1 миллиард рублей;
* Стоимость данных банковских карт проходящих через процессинг в течении суток - 20 тысяч карт X 100 тысяч рублей = 2 миллиард рублей;
* Стоимость персональных данных пользователей, чьи банковские карты находятся в оперативной обработке – 10 тысяч карт X 10 тысяч рублей = 100 миллионов рублей;
* Стоимость программного обеспечения – 100 тысяч рублей за один человеко-месяц X 360 человеко-месяцев = 36 миллионов рублей;
* Стоимость денежного потока - 20 тысяч транзакций в сутки X 1 тысячу рублей = 20 миллионов рублей в сутки или 700 миллионов в год. При условии что процессинг берёт 5% с каждой транзакции – 35 миллионов рублей в год выручки;

Суммирую сказанное, таблица с перечнем активов и их стоимостью приведена ниже.

Таблица 1.

|  |  |
| --- | --- |
| **Активы** | **Стоимость** |
| Сервис обработки данных банковских карт | 3,5 миллиарда рублей |
| Данные банковских карт | 1 миллиард рублей |
| Персональные данные держателей карт | 100 миллионов рублей |
| Денежный поток, проценты от которого формируют доход процессинга | 35 миллионов рублей |
| Программное обеспечение, применяемое для обработки данных банковских карт | 36 миллионов рублей |

**Моделирование угроз информационной безопасности**

Выделив активы, возможно, найти направленные на них угрозы. Следует только сопоставить возможные источники угроз с активами и исключить невозможные физически сочетания.

В качестве источников угроз мы будем рассматривать:

* Отказы аппаратуры;
* Ошибки персонала;
* Внутренние нарушители, т.е. персонал занявшейся противозаконной деятельностью;
* Внешние нарушители.

Стихийные бедствия не вошли в данный список, по той причине, что центры обработки данных прошедшие проверку на соответствие требованиям PCI DSS имеют высокую степень защиты от всех природных и техногенных катастроф, которые могут произойти в их окружении. Также мы считаем надёжным и не несущим угрозы персонал центра обработки данных.

Отказ аппаратуры включённой в технологический процесс обработки данных банковских карт ведёт к его временному прекращению. Период на которые данный процесс прекратится зависит, от того насколько быстро персонал отвечающий за эксплуатацию информационной системы узнает о произошедшем, и насколько быстро сможет устранить неисправность.

Ущерб в свою очередь зависит от количества утерянных за это время транзакций, их средней стоимости, а в некоторых случаях от «медийного» эффекта аварии.

Средняя стоимость простоя в течении одного часа равна 20 тысяч транзакций в сутки/ 24 часаX среднюю стоимость транзакции. Приблизительно 800 тысяч рублей. Разумно ожидать как минимум одного аппаратного сбоя в течении года.

Ошибки персонала также могут приводить к прекращению обработки карточных данных. Подключение почти любого мерчанта требует внесения изменений в программный код или настройки программного обеспечения процессинга. Стоимость простоя аналогична. Вероятность подобного события также как минимум один раз в год.

Внутренние и внешние нарушители могут быть также источниками угрозы прекращения обработки карточных данных. Также они могут нарушать конфиденциальность данных банковских карт, персональных данных клиентов мерчантов или пытаться скопировать исходный код программного обеспечения процессинга.

Возможно, предположить, что внешние нарушители могут пытаться прекратить процесс обработки данных банковских карт при помощи атаки на отказ в обслуживании. Скорее всего, это будет распределённая атака на отказ в обслуживании. Стандарт PCI DSS требует применения межсетевых экранов с целью исключения доступа извне в сеть, где обрабатываются карточные данные, кроме как к необходимым сервисам. Исходя из этого мы можем свести угрозу прекращения обработки карточных данных исходящую от внешних нарушителей к возможности DDOS атаки платёжные шлюзы. Или к получению на них возможности исполнять произвольный код.

Внутренние нарушители могут получить доступ к данным банковских карт, персональным данным или коду программного обеспечения процессинга при помощи стандартных средств удалённого управления – ssh, telnet, rdp. Применение иных протоколов, возможно, ограничить при помощи межсетевых экранов.

Угрозой направленной на возможность получения оплаты за предоставленные услуги процессинга (Денежный поток, проценты от которого формируют доход процессинга) являются фродовые т.е. мошеннические транзакции инициированные внешними нарушителями. При помощи кражи персональных данных и данных банковских карт внешние нарушители могут пытаться купить товары или услуги предоставляемые клиентами процессинга. Владельцы украденных карт, обнаружив кражу денежных средств, откажутся оплачивать покупки совершённые злоумышленниками. Результатом этого будет отказ банка эмитента и расчётного центра принять транзакцию к обработке и недополученные процессингом прибыли.

Взаимосвязь угроз и источников приведена ниже, в таблице 2:

Таблица 2.

|  |  |
| --- | --- |
| Угроза | Источники |
| Прекращение обработки данных банковских карт | • Отказы аппаратуры; • Ошибки персонала; • Внутренние нарушители, т.е. персонал занявшейся противозаконной деятельностью; • Внешние нарушители; |
| Кража данных банковских карт | • Внутренние нарушители, т.е. персонал занявшейся противозаконной деятельностью; • Внешние нарушители; |
| Кража персональных данных клиентов | • Внутренние нарушители, т.е. персонал занявшейся противозаконной деятельностью; • Внешние нарушители; |
| Кража исходного кода программного обеспечения процессинга | • Внутренние нарушители, т.е. персонал занявшейся противозаконной деятельностью; • Внешние нарушители; |
| Потеря части денежного потока вследствие отказа банков оплачивать мошеннические транзакции | • Внешние нарушители; |

**Оценка рисков информационной безопасности**

Определив активы, угрозы и источники угроз информационной безопасности, возможно, перейти к количественной оценке рисков. Как уже было сказано риск - сочетание вероятности нанесения ущерба и тяжести этого ущерба. Потенциальная возможность использования уязвимостей активов организации угрозами ИБ для причинения ущерба организации, измеряемая с учетом вероятности реализации угроз ИБ и величины ущерба от реализации угроз ИБ. В данной работе, как в классической теории управления рисками информационной безопасности вообще рассматриваются чистые риски. Это обозначает, что риски приводят к убыткам или недополученной прибыли и не могут приводить к увеличению прибыли.

В качестве источника информации для численной оценки рисков будут использованы ряд криминологических исследований, а также экспертное мнение научного консультанта.

Рассмотрим угрозу прекращения процесса обработки данных кредитных карт. Данная угроза имеет четыре источника:

* Отказы аппаратного обеспечения;
* Ошибки персонала;
* Внешние злоумышленники;
* Внутренние злоумышленники.

Отказ аппаратного обеспечения характеризуется величиной называемой «наработка на отказ». Большинство производителей серверного оборудования указывают наработку на отказ около года непрерывной работы. Существуют производители, указывающие и большие значения данной величины. Учитывая, что информационная система рассматриваемой компании состоит из нескольких серверов, и выход из строя одного из них равносилен неработоспособности всей системы - будем считать значением данной величины – год непрерывной работы.

В случае выхода из строй сервера, потребуется, диагностика неисправности, замена вышедшего из строя блока, и перенастройка или переустановка аппаратного обеспечения. Будем считать, что на все указанные действия суммарно потребуются сутки. Для выполнения подобных действий в удалённом центре обработки данных это реалистичное предположение.

Под ошибками персонала будем понимать неправильно введённые настройки активного оборудования или ошибки в разрабатываемом программном обеспечении процессинга, которые приводят к его неработоспособности. Процесс обнаружения, выявления причины и устранения ошибок также может занимать длительное время. Разумно предположить, что подобные ситуации случаются как минимум раз в год и могут продолжаться до одних суток.

Внешние злоумышленники могут пытаться осуществить DDOS атаки. Как показывает практика априорная вероятность стать целью такой атаки составляет 0,1 в год. Средняя продолжительность атаки может достигать пары недель. Примем вероятность 0,1 и продолжительность атаки – 10 суток. В течение всего этого времени сервис обработки данных банковских карт предполагается недоступным.

Внешние злоумышленники могут использовать неизвестные поставщикам системного программного обеспечения уязвимости с целью остановки работы важных системных процессов и вызывания отказа в работе сервиса. Средний период между обнаружением уязвимости и выпуском исправлений, различается у разных поставщиков между несколькими днями и неделями и даже месяцами. Для стека Linux+Apache+Php он составляет около двух недель.

Для нас эта величина и характеризует период времени, на который злоумышленник сможет остановить работу процессинга. Примем вероятность подобной атаки 0,01 в течении года, срок выпуска исправления безопасности – 10 дней.

Суммируя произведения вероятностей на величину простоя получаем суммарное время простоя – 4 суток в год.

Рассмотрим вероятность утечки данных банковских карт. Существует два источника данной угрозы:

* Внешние нарушители;
* Внутренние нарушители.

Предположим, что внешние нарушители используют неизвестные поставщикам системного программного обеспечения уязвимости с целью получения доступа к обрабатываемой на серверах информации. Как уже рассматривали средний период между обнаружением уязвимости и выпуском исправлений, для стека Linux+Apache+Php он составляет около двух недель. Вероятность подобной атаки 0,01. В результате можем сказать что злоумышленник «в среднем» сможет украсть данные банковских карт в объеме «дневного» траффика процессинга – 20 тысяч штук.

Вероятность того, что персонал процессинга станет учувствовать в махинациях с банковскими картами составляет около 0,01. Это крайне приблизительная экспертная оценка. Более точные данные можно получить только путём обследования конкретного коллектива. Учитывая тот факт, что данные после оперативной обработки отправляются в архив, где хранятся в защищённой криптографическими методами форме, внутренний нарушитель может получить доступ к ограниченному количеству информации – до 20 тысяч записей о банковских картах.

Аналогично возможно рассчитать вероятность и последствия кражи персональных данных физических лиц. Отличием будет гораздо более низкая мотивация злоумышленника. Тем более получив доступ к внутренним компонентам процессинга иррационально ограничить свою деятельность только персональными данными, не затронув информацию о платёжных картах.

Источником угрозы кражи исходного кода программного обеспечения процессинга является внутренний нарушитель. Программное обеспечение разрабатывается на отдельном сервере недоступном из сети интернет. Поэтому внешние нарушители могут быть исключены. По аналогии с предыдущим пунктом вероятность того, что персонал процессинга станет учувствовать в подобной махинации, составляет около 0,01.

Ещё одним активом, крайне важным для компании занимающейся обработкой данных банковских карт является поток денежных средств, состоящий из платежей клиентов мерчантов. Обработка информации об этих платежах составляет одну из основных задач процессинга, а отчисления мерчантов в виде определённого процента с выручки, полученной при помощи оплаты банковскими картами – выручку рассматриваемой компании. В среднем как минимум один платёж из ста является мошенническим. Источником данной угрозы являются внешние нарушители.

Взаимосвязь между активами, свойствами безопасности и вероятностью их потери показана в таблице 3.

Таблица 3.

|  |  |  |  |
| --- | --- | --- | --- |
| **Активы** | **Стоимость** | **Вероятность потери свойства безопасности** | **Средние потери от реализации рисков** |
| Сервис обработки данных банковских карт | 3,5 миллиарда рублей | 4 сутки простоя в год.  Вероятность – 1 | 40 миллионов рублей |
| Данные банковских карт | 1 миллиард рублей | Вероятность 0,1  20 тысяч карт | 10 миллионов рублей |
| Персональные данные держателей карт | 100 миллионов рублей | Вероятность 0,001  Потеря информации о 20 тысячах субъектах | 20 тысяч рублей |
| Денежный поток, проценты от которого формируют доход процессинга | 35 миллионов рублей | 0,01 процента транзакций фродовые | 350 тысяч рублей |
| Программное обеспечение, применяемое для обработки данных банковских карт | 36 миллионов рублей | Вероятность несанкционированного копирования 0,01 | 3,6 миллиона рублей |

**Разработка мер минимизации выявленных рисков**

В целях минимизации угрозы «прекращение обработки данных банковских карт» предлагается:

* Внедрить отказоустойчивый кластер серверов. Каждый сервер, задействованный в контуре обработке карточных данных дублируется.
* Внедрить стандартизированную процедуру внесения изменений в настройки оборудования и запуска новой версии программного обеспечения в «промышленной среде». Процедура должна определять как порядок согласования и документирования изменений так и автоматизированные средства распространения настроек и программного обеспечения. Данные средства должны позволять «откатить» изменения в случае отсутствия подтверждений корректности работы от системных администраторов.
* В целях противодействия внешним злоумышленникам внедрить специализированные средства AntiDDOS и Application Firewall позволяющей нейтрализовать уязвимости в программном обеспечении до выхода исправлений от производителя.
* В целях предотвращения деятельности внутренних злоумышленников предлагается внедрение систему записи сессий удалённого управления серверами.

Ранее уже упоминалось, что средства создания резервных копий обрабатываемой информации уже внедрены и функционируют. Следует распространить практику создания резервных копий на настройки компонентов информационной системы, системное и прикладное программное обеспечение.

Кража данных банковских карт возможна как со стороны внешних, так и со стороны внутренних нарушителей. В целях предотвращения реализации данной угрозы предполагается внедрить:

* Систему записи сессий удалённого управления серверами;
* Application Firewall позволяющей нейтрализовать уязвимости в программном обеспечении до выхода исправлений от производителя.

Первое средство позволит выявить нарушителей среди персонала процессинга, если такие появятся, и послужит хорошим сдерживающим фактором. Application Firewall позволит предотвращать атаки использующие неисправленные уязвимости в стеке приложений Linux+Apache+Php+MySQL.

Противодействие угрозе кражи персональных данных клиентов аналогично предотвращению кражи данных банковских карт.

* Систему записи сессий удалённого управления серверами;
* Application Firewall позволяющей нейтрализовать уязвимости в программном обеспечении до выхода исправлений от производителя.

Аналогична ситуация и с противодействием краже программного обеспечения процессинга. За исключением того, что источником данной угрозы является только внутренние нарушители и единственной защитной мерой является внедрение системы записи сеансов работы с серверами процессинга.

Более сложной является задача противодействия мошенническим транзакциям. Для её решения потребуется внедрение специализированной системы противодействия мошенничеству. Подобное программное средство анализирует параметры транзакции, особенности рабочей станции клиента, строит профили типичного поведения для каждого пользователя и сравнивает с ними текущее обращение клиента.

Ожидается, что внедрение:

* кластера серверов – приведёт к отсутствию простоя процессинга вследствие аппаратных отказов;
* стандартизированной процедуры внесения изменений в настройки оборудования и запуска новой версии программного обеспечения в «промышленной среде» - уменьшит время простоя процессинга вследствие ошибок персонала до одного часа в год;
* средств противодействия DDOS атакам - уменьшит время простоя до одного часа в год;
* Application Firewall - уменьшит время простоя до одного часа в год;
* средств записи сеансов удалённого управления серверами сведёт к нулю прости процессинга вследствие деятельности внутренних нарушителей.

Также ожидается, что внедрение:

* Application Firewall уменьшит на порядок вероятность кражи данных банковских карт и персональных данных со стороны внешних злоумышленников;
* средств записи сеансов – приведёт к нулевой вероятности кражи данных, банковских карт, персональных данных и исходного кода программного обеспечения процессинга;
* средства выявления мошеннических транзакций - уменьшит на порядок величину фрода.

Экономическая эффективность мер направленных на снижение угроз:

Таблица 4.

|  |  |  |  |
| --- | --- | --- | --- |
| **Угроза** | **Средние потери от реализации рисков** |  | **Меры противодействия и средние потери после их применения** |
| Прекращение обработки данных банковских карт | 40 миллионов рублей |  | * отказоустойчивый кластер серверов * стандартизированной процедуры внесения изменений в настройки оборудования и запуска новой версии программного обеспечения * средство противодействия DDOS атакам * Application Firewall * средств записи сеансов удалённого управления серверами   Результат – уменьшение потерь до 3 миллионов в год. |
| Кража данных банковских карт | 10 миллионов рублей |  | * Application Firewall * средств записи сеансов удалённого управления |
| Кража персональных данных клиентов | 20 тысяч рублей |  | * Application Firewall * средств записи сеансов удалённого управления |
| Кража исходного кода программного обеспечения процессинга | 350 тысяч рублей |  | * средств записи сеансов удалённого управления |
| Потеря части денежного потока вследствие отказа банков оплачивать мошеннические транзакции | 3,6 миллиона рублей |  | * средства выявления мошеннических транзакций |

Возврат инвестиций в меры по снижению угроз информационной безопасности:

Таблица 5.

|  |  |  |  |
| --- | --- | --- | --- |
| **Меры противодействия и эффект от их применения** | **Стоимость мер** |  | **Период возврата инвестиций** |
| Отказоустойчивый кластер серверов.  Устранение 10000000 рублей потерь в год. | 1000000 рублей; |  | 1 месяц. |
| Cстандартизированные процедуры внесения изменений в настройки оборудования и запуска новой версии программного обеспечения.  Устранение 9000000 рублей потерь в год. | 0 рублей |  | «мгновенно» |
| Средство противодействия DDOS атакам (Arbor Prevail). Устранение 9000000 рублей потерь в год. | 1000000 рублей. |  | Около 1-го месяца. |
| Application Firewall (Imperva WAF).  Устранение 9000000 рублей потерь в год. | 1000000 рублей. |  | Около 1-го месяца. |
| Application Firewall (Imperva WAF) как средство защиты от внешних злоумышленников. Против кражи данных банковских карт.  Устранение 10000000 рублей потерь в год. | 1000000 рублей. | | 1 месяц. |
| Средство записи сеансов удалённого управления.  Против кражи данных банковских карт.  Устранение 10000000 рублей потерь в год. | 1000000 рублей. | | 1 месяц. |
| Application Firewall (Imperva WAF) как средство защиты от внешних злоумышленников. Против кражи персональных данных.  Устранение 20 тысяч рублей потерь в год. | 1000000 рублей. | | 50 месяцев. |
| Средство записи сеансов удалённого управления.  Против кражи персональных данных.  Устранение 20 тысяч рублей потерь в год. | 1000000 рублей. | | 50 месяцев. |
| Средство записи сеансов удалённого управления.  Против кражи исходного кода.  Устранение 350 тысяч рублей потерь в год. | 1000000 рублей. | | 3 года. |
| Средство выявления мошеннических транзакций.  Предотвращают потерю 3,6 миллиона рублей в год. | 36 миллионов рублей. | | 10 лет. |

**Применение теории матричных игр для выбора средств защиты информации**

Как уже было сказано в основе исходной концептуальной схемы ИБ лежит противоборство собственника и злоумышленника с целью получения контроля над информационными активами. В том случае если результатом противоборства является выигрыш одной из сторон и симметричный проигрыш противоположной стороны – возможно, говорить об антагонистической игре или игре с нулевой суммой. Величину выигрыша или проигрыша, возможно, оценивать по-разному. Разумной кажется оценка в денежных единицах. Такая оценка позволит сравнивать возможные выигрыши или потери с затратами на реализацию тех или иных стратегий. Современные информационные системы строятся на основе машин фон Неймана, которые как известно имеют счётное и конечное число состояний. Интуитивно кажется разумным предположение о том что существует счётное множество возможных стратегий злоумышленника и собственника. Также возможно что экономические, физические и иные ограничения приводят к тому что множества стратегий будут не только счётны но и конечны.

Суммируя сказанное:

* В основе концепции ИБ лежит противоборство собственника и злоумышленника с целью получения контроля над информационными активами;
* Стоимость активов, возможно, оценить в финансовом смысле;
* Также в финансовом смысле, возможно, оценить стоимость реализации тех или иных стратегий и их результативность, как для собственника активов, так и для нарушителя;
* По крайней мере, выигрыш злоумышленника финансово эквивалентен потерям собственника;
* Учитывая дискретный характер современных информационных систем, существует конечное множество стратегий злоумышленника и стратегий собственника активов.
* В ряде случаев указанные ранее счётные множества стратегий конечны.

Вывод: в некотором подмножестве случаев противостояние собственника и злоумышленника является антагонистической игрой со счётным и конечным количеством стратегий и как следствие сводимо к матричной игре.

Рассмотрим несколько примеров показывающих возможность применения теории матричных игр к выбору средств управления рисками информационной безопасности. Существует организация X. Данная организация владеет и эксплуатирует информационную систему персональных данных. В соответствии с требованиями законодательства владелец информационной системы произвёл выделение информационной системы персональных данных, её обследование и классификацию. Далее возник вопрос о применении организационных и технических мер, каждая из которых имеет некую финансовую стоимость. Количество возможных мер – конечно, соответственно конечно и множество их конечных сочетаний – это возможные стратегии организации. Злоумышленников в данном случае выступает регулирующий орган. В зависимости от того насколько выполняются требования действующего законодательства он может применить те или иные штрафные санкции. Количество требований нормативных актов – конечно, соответственно конечно и множество их конечных сочетаний – это возможные стратегии нарушителя. В таких условиях составление платёжной матрицы уже вполне возможно.

**Рассмотрение сценария реализации угрозы «Прекращение обработки данных банковских карт»**

Механизмы реализации данной угрозы рассмотрены и описаны ранее. В целях применения теории матричных игр будем считать все источники угрозы одним игроком Механизмы реализации угрозы – стратегиями данного игрока. Защитные меры – стратегиями собственника активов. Вычитая из стоимости рисков, полученные для различных механизмов реализации данной угрозы, стоимость защитных мер приведённых к одному временному периоду составим платёжную матрицу игры. Далее определим цену игры и её возможность розыгрыша в чистых стратегиях. Также попробуем найти оптимальную смешанную стратегию собственника активов.

Источниками угрозы «Прекращение обработки данных банковских карт» являются:

* Отказы аппаратуры;
* Ошибки персонала;
* Внутренние нарушители, т.е. персонал занявшейся противозаконной деятельностью;
* Внешние нарушители.

Защитные меры, реализуемые собственником активов:

* Применение отказоустойчивого кластера серверов;
* Введение стандартизированной процедуры внесения изменений в настройки оборудования и запуска новой версии программного обеспечения в «промышленной среде»;
* Внедрение АнтиDDOS;
* Внедрение средства регистрации действий системных администраторов.

Платёжная матрица игры представлена ниже:

Таблица 6.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Отказоустойчивый кластер серверов | Стандартизированная процедура внесения изменений в настройки оборудования. | АнтиDDOS | Средства записи действий системных администраторов | Внедрение всех перечисленных защитных мер |
| Отказ аппаратуры | -1000000 | -10000000 | -11000000 | -11000000 | -3000000 |
| Ошибка персонала | -11000000 | 0 | -11000000 | -11000000 | -3000000 |
| Внутренние нарушители | -11000000 | -10000000 | -11000000 | -1000000 | -3000000 |
| Внешние нарушители | -11000000 | -10000000 | -1000000 | -11000000 | -3000000 |
| Реализация всех сценариев сразу | -34000000 | -30000000 | -34000000 | -34000000 | -3000000 |

Решение минимаксным методом.

Проверяем, имеет ли платежная матрица седловую точку. Если да, то выписываем решение игры в чистых стратегиях. Считаем, что игрок I выбирает свою стратегию так, чтобы получить максимальный свой выигрыш, а игрок II выбирает свою стратегию так, чтобы минимизировать выигрыш игрока I.

Таблица 7.

|  |  |  |  |
| --- | --- | --- | --- |
| Игроки | B1 | B2 | **a = min(Ai)** |
| A1 | 0 | 0 | **0** |
| A2 | -10000000 | 800000 | **-10000000** |
| **b = max(Bi)** | **0** | **800000** |  |

Находим гарантированный выигрыш, определяемый нижней ценой игры a = max(ai) = 0, которая указывает на максимальную чистую стратегию A1.  
Верхняя цена игры b = min(bj) = 0.  
Седловая точка (1, 1) указывает решение на пару альтернатив (A1,B1). Цена игры равна 0.  
Решим задачу геометрическим методом, который включает в себя следующие этапы:  
1. В декартовой системе координат по оси абсцисс откладывается отрезок, длина которого равна 1. Левый конец отрезка (точка х = 0) соответствует стратегии A1, правый - стратегии A2 (x = 1). Промежуточные точки х соответствуют вероятностям некоторых смешанных стратегий S1 = (p1,p2).  
2. На левой оси ординат откладываются выигрыши стратегии A1. На линии, параллельной оси ординат, из точки 1 откладываются выигрыши стратегии A2.  
Решение игры (*2 x n*) проводим с позиции игрока A, придерживающегося максиминной стратегии. Доминирующихся и дублирующих стратегий ни у одного из игроков нет.  
Максиминной оптимальной стратегии игрока A соответствует точка N, для которой можно записать следующую систему уравнений:  
y = 0 + (-10000000 - 0)p2  
p2 = 0  
Откуда  
p1 = 1  
p2 = 0  
Цена игры, y = 0  
Теперь можно найти минимаксную стратегию игрока B, записав соответствующую систему уравнений  
= y  
-10000000q1+800000q2 = y  
q1+q2 = 1  
или  
= 0  
-10000000q1+800000q2 = 0  
q1+q2 = 1  
Решая эту систему методом обратной матрицы, находим:  
q1 = 1  
q2 = 0

Таким образом наиболее оптимальной стратегией

**Выводы**

Как показывает практика применение теории матричных игр к выбору средств управления рисками информационной безопасностью или к выбору средств защиты информации вполне возможно. Однако практическое использование данной идеи наталкивается на ряд сложностей.

Во-первых – практическое использование требует наличие хорошо структурированной базы данных описывающей средства защиты информации, организационные и технические меры, их особенности, характеристики и стоимость.

Во-вторых, для сколько-либо сложной информационной системы, возникает проблема сложности вычислений.

В-третьих необходимо проанализировать допустимость применения теории матричных игр для различных бизнес-задач. Далеко не всегда интересы собственника активов и злоумышленника настолько антагонистичны чтобы была возможность говорить об игре с нулевой суммой.

Интересным представляется практическое решения задачи выбора оптимального сочетания различных организационных и технических мер для сложной информационной системы с привязкой к бизнес задачам. Или расширения решаемой в данной работе задачи на случаи, в которых затруднена численная оценка активов, неизвестна эффективность применяемых мер или существует неопределённость в наличии дальнейшей поддержки внедряемых технических решений со стороны производителя.

**Использованные источники**

1. ГОСТ Р ИСО/МЭК 27001–2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».
2. Стандарт Банка России СТО БР ИББС-1.0 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».
3. ГОСТ Р ИСО/МЭК 27005–2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности». М.: Стандартинформ, 2011
4. ГОСТ Р ИСО/МЭК 17799–2005 «Информационная технология. Методы и средства обеспечения безопасности. Практические правила управления информационной безопасностью».
5. ГОСТ Р 50922–2006 «Защита информации. Основные термины и определения».
6. «Управления инцидентами информационной безопасности» Н.Г. Милославская,

М.Ю. Сенаторов, А.И. Толстой

1. «Управление рисками информационной безопасности» Н.Г. Милославская,

М.Ю. Сенаторов, А.И. Толстой

1. <http://wikipedia.ru>
2. Карлин С. Математические методы в теории игр, программировании и экономике М., «Мир», 1964
3. Оуэн Г. Теория игр. М. «Мир», М., 1971

Приложение 1.

Структура информационной системы до применения технических мер по снижению рисков информационной безопасности



Приложение 2.

Структура информационной системы после применения технических мер по снижению рисков информационной безопасности

