Бушковский Г.Г., Иванов С.В., **УДК 330:519.7**

ИГРОВОЙ ПОДХОД К ИНВЕСТИЦИЯМ В ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ

Аннотация. *В статье проведен анализ основных подходов к определению оптимальных объемов инвестиций, необходимых для обеспечения информационной безопасности. Рассмотрены экономическая модель, определяющая оптимальный объем инвестиций в информационную безопасность для защиты заданного информационного ресурса Гордона-Лоеба и модель взаимосвязанных рисков для двух идентичных организаций Вухен Шима, выявлены их основные слабые стороны, которые не позволяют учитывать динамические аспекты а именно эффект инвестиций. Предложена модель оценки эффективности инвестиций в информационную безопасность, основанная на теории игр.*
Ключевые слова. *оптимальный объем инвестиций, информационная безопасность, теория игр, эффективность инвестиций.*

Анотація. *У статті проведено аналіз основних підходів до визначення оптимальних обсягів інвестицій, необхідних для забезпечення інформаційної безпеки. Розглянуто економічна модель, яка визначає оптимальний обсяг інвестицій в інформаційну безпеку для захисту заданого інформаційного ресурсу Гордона - Лоеба і модель взаємозалежних ризиків для двох ідентичних організацій Вухен Шима, виявлено їх основні слабкі сторони, які не дозволяють враховувати динамічні аспекти а саме ефект інвестицій. Запропоновано модель оцінки ефективності інвестицій в інформаційну безпеку, заснована на теорії ігор.*
Ключові слова. *оптимальний обсяг інвестицій, інформаційна безпека, теорія ігор, ефективність інвестицій*

Summary. *Game theory is used to analyze problems in which the payoffs to players depend on the interaction between players' strategies. For example, in the IT security investment problem, the firm and the hackers are players. The firm's payoff from security investment depends on the extent of hacking it is subjected to. The hacker's payoff from hacking depends on the likelihood he or she will be caught.*
Thus, the likelihood of the firm getting hacked depends on the likelihood the hacker will be caught, which, in turn, depends on the level of investment the firm makes in IT security. The first step in using game theory to analyze such strategic interactions among players is to develop a game tree that depicts the strategies of players. Based on Bayes' rule, we expect the strategy of players: firm and hacker.
The solution to the game involves maximization of a polynomial function. This is done by equating the first derivative of the function with respect to each decision variable to zero. At this point, firm knows how much manual monitoring it should implement in order to minimize the total cost of security.
IT security management is a demanding task. Assessing the value of security technologies is essential to manage IT security effectively. However, the lack of a comprehensive model that incorporates the specific features of IT security technologies has prevented firms from applying rigorous quantitative techniques to make security investment decisions. The current set of tools such as risk analysis and cost effectiveness analysis work with very high-level aggregate data, so these tools are of limited value in an IT security setting. We have proposed a comprehensive model to analyze IT security investment problems that overcome some of these limitations. We used this model to derive insights into the value of technologies.
Keywords. *Optimal investment, information security, game theory, investment performance.*

Постановка проблемы. Сегодня в компаниях и предприятиях с повышенными требованиями в области информационной безопасности (государственные, банковские системы, билинговые системы, ответственные производства и т. д.) затраты на обеспечение режима информационной безопасности составляют до 30 % всех затрат на информационную систему, и владельцы информационных ресурсов серьезно рассматривают экономические аспекты обеспечения информационной безопасности. Даже в тех информационных системах, уровень безопасности которых явно недостаточен, у технических специалистов зачастую возникают проблемы обоснования затрат на повышение этого уровня перед руководством предприятий и организаций.

Целью статьи является анализ игрового подхода к оценке эффективности инвестиций в информационную безопасность.

Анализ последних достижений и публикаций. Разработки в области нахождения экономически обоснованного объема денежных средств, необходимого для обеспечения информационной безопасности нашли свое отражение, как в зарубежных, так и в отечественных работах. Однако именно зарубежные работы последнего десятилетия являются передовыми.

Гордон и Лоеб предложили экономическую модель, определяющую оптимальный объем инвестиций в информационную безопасность для защиты заданного информационного ресурса [1]. Модель рассматривает то, как уязвимость информации и потенциальные потери вследствие такой уязвимости влияют на оптимальный объем ресурсов, которые должны быть вложены в защиту информации. Показывается, что при определенных предположениях, касающихся связи между уязвимостью и предельной эффективностью инвестиций в информационную безопасность, объем оптимальных инвестиций может либо строго возрастать, либо сначала возрастать, а потом убывать с возрастанием уязвимости. Если информация чрезвычайной важности и ожидаемый ущерб велик, то разумнее выбрать первый вариант модели и защищать высоко уязвимые ресурсы, дабы минимизировать потери. В случае же, когда ожидаемый ущерб не столь велик, прибыль от инвестиций в защищенность высоко уязвимых ресурсов мала, разумнее использовать второй вариант модели и концентрировать финансовые ресурсы на защите информационных ресурсов из диапазона средней уязвимости.

Гордон и Лоеб также показывают, что даже в диапазоне оправданных инвестиций в информационную безопасность максимальный объем, который должна вложить нейтральная к риску организация, составляет лишь часть от ожидаемых потерь в связи с нарушением защищенности. Для двух широких классов функций вероятности нарушения защищенности информационного ресурса, предложенных Гордоном и Лоебом, эта часть никогда не превосходит *37 %* от ожидаемых потерь. Для большинства случаев эта часть значительно меньше *37 %*.

Вухен Шим, базируясь на модели Гордона-Лоеба, разработал модель взаимосвязанных рисков для двух идентичных организаций [2]. Он показал, что оптимальный объем инвестиций в информационную безопасность в случае отрицательных внешних эффектов выше или равен оптимальному объему инвестиций в случае независимых рисков, а область нулевых инвестиций в этом случае оказывается меньше. Если же взаимодействие организаций обуславливает положительные внешние эффекты, то оптимальный объем инвестиций в информационную безопасность ниже или равен оптимальному объему инвестиций в случае независимых рисков, а область нулевых инвестиций оказывается такой же, как в модели с независимыми рисками.

В модели взаимосвязанных рисков с отрицательными внешними эффектами оптимальный объем инвестиций в информационную безопасность не превосходит *73,56 %* от ожидаемых потерь, а в случае положительных внешних эффектов не превосходит $(1 + \delta)^{-1} \cdot 36{,}97\ \%$ от ожидаемых потерь, где δ - параметр, характеризующий степень взаимосвязанности организаций.

У моделей имеются слабые стороны. Ни одна из них не учитывает динамические аспекты, а именно эффект инвестиций. В частности, не рассматривается, как злоумышленник меняет стратегии своих атак в ответ на дополнительные инвестиции в информационную безопасность. Существуют трудности в получении данных для обеих моделей, таких как количественная оценка ущерба, оценка вероятности возникновения угроз и оценка уязвимости. Модель взаимосвязанных рисков разработана лишь для идентичных организаций, что не всегда имеет место. Обе модели базируются на двух специфических классах: функций вероятности нарушения защищенности информационного ресурса. И остается неясным, дадут ли другие классы функций похожие результаты.

Изложение основного материала. Теория игр используется для анализа задач, в которых выплаты игрокам зависят от взаимодействия стратегий. Например, в проблеме инвестиций в IT-безопасность игроки - это фирмы и хакеры. Выигрыш фирмы от инвестиций в обеспечение безопасности зависит от степени урона от взлома. Выигрыш хакеров от взлома зависит от вероятности того, что он будет пойман. Таким образом, вероятность того, что фирма будет взломана, зависит от вероятности того, что хакер будет пойман, которая, в свою очередь, зависит от уровня инвестиций, который фирма вкладывает в область информационной безопасности. Первый шаг в использовании теории игр для анализа стратегических взаимодействий между игроками является разработка дерева игры, которое изображает стратегии игроков. На рисунке 1 представлено дерево игры для проблемы IT-безопасности.

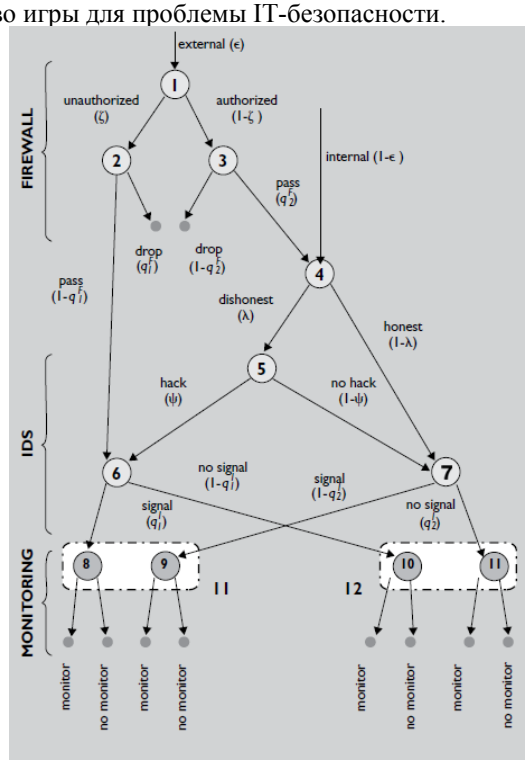

Рис.1. Дерево игры

Игра начинается с выбора природы типа трафика системы, который может быть внешним (узел 1) с вероятностью ε или внутренним (узел 4) с вероятностью (1 - ε). Узел 2 представляет внешнего хакера, в то время как узел 3 легального внешнего пользователя. 5-й узел характеризует несанкционированный доступ к внутренней сети. Нечестный пользователь может совершить два действия: взламывать или не взламывать.

Если хакер решает взломать, игра перемещается к узлу 6, в противном случае - к узлу 7. Система обнаружения вторжений (IDS) захватывается узлом 6. Фирма принимает решение о необходимости контролирования в зависимости от состояния (наличие сигнала или его отсутствие) в котором она находится. Фирма должна принимать решения, не зная точно на каком узле игра находится. Тем не менее, можно определить вероятность проникновения с сигналом или его отсутствием, используя правило Байеса:

$$\eta_1 = P(intrusion|signal) = \frac{P(signal|intrusion)P(intrusion)}{P(signal|intrusion)P(intrusion) + P(signal|no-intrusion)P(no-intrusion)}$$

$$\eta_2 = P(intrusion|no-signal) = \frac{P(no-signal|intrusion)P(intrusion)}{P(no-signal|intrusion)P(intrusion) + P(no-signal|no-intrusion)P(no-intrusion)}$$

Искомыми переменными для фирмы являются вероятность наблюдения сигнала, который нам идет с IDS, $\rho 1$, и вероятность отсутствия сигнала от IDS, $\rho 2$. Фирма максимизирует свой ожидаемый выигрыш, в связи с этим нахождение искомых переменных показано ниже.

$$F = [P(signal)F_S + P(nosignal)F_N + P(drop)\sigma](1)$$

где $F_S = \{-\rho_1 c - \eta_1(1-\rho_1)d - \eta_1\rho_1[(1-\alpha)d + \alpha(1-\varphi)d]\}$

и $F_N = \{-\rho_2 c - \eta_2(1-\rho_2)d - \eta_2\rho_2[(1-\alpha)d + \alpha(1-\varphi)d]\}$

являются выплаты для состояний наличия сигнала и его отсутствия соответственно, каждый из которых состоит из потерь незамеченных вторжений, потерь при обнаружении вторжений (таких, как неустранимая часть потерь, даже если вторжение обнаружено), а также стоимость мониторинга.

Ожидаемый выигрыш хакера включает ожидаемую полезность от вторжения и ожидаемую стоимость, если вторжение обнаружено. Хакер, в то же время, максимизирует свою функцию выигрыша, которая показана здесь искомой переменной ψ.

$$H = P(hacking)(Benefit - Cost) = \psi\mu - \psi\alpha(\beta + \gamma d)[\rho_1 q_1^I + \rho_2(1-q_1^I)](2)$$

Для данного набора параметров решение в игре дает уникальные для фирмы и также для хакера искомые значения переменных. Следует отметить, что решение игры включает в себя максимизацию полиномиальной функции. Это делается путем приравнивания первой производной функции по отношению к каждой искомой переменной к нулю. В этот момент фирма знает, какой контроль следует осуществлять для того, чтобы свести к минимуму общую стоимость безопасности. Проиллюстрируем этот подход с использованием числового примера с параметрами:

$$\mu = 600, \alpha = 0.2, \beta = 5000, d = 1000000, \gamma = 0.01, q_1^I = 0.9, q_2^I = 0.9, q_1^F = 0.9, q_2^F = 0.9, \lambda = 0.5, \varphi = 0.8, \varepsilon = 0.001, \sigma = 20, c = 5.$$

Эти числовые значения для гипотетического сценария и используются только для иллюстрации. Фирма, которая использует нашу модель, должна оценить эти параметры, используя любой из методов оценки риска. Модель предсказывает оптимальный ответ $\rho_1 = 0{,}56$ и $\rho_2 = 0$, а это означает, что фирма будет контролировать 56% случаев, для которых она получает сигнал от IDS, и не будет контролировать при отсутствии сигнала вообще.

Выводы: Управление IT-безопасностью является сложной задачей. Оценка стоимости технологий безопасности имеет большое значение для эффективного управления IT-безопасностью. Тем не менее, отсутствие всеобъемлющей модели, которая включает в себя особенности технологий IT-безопасности, помешало применять строгие количественные методы для принятия решений эффективности инвестиций в безопасность. Текущий набор инструментов, таких как анализ рисков и анализ эффективности затрат характеризуется очень высоким уровнем совокупных данных, так что эти инструменты имеют ограниченную ценность в обеспечении IT-безопасности. Мы предложили модель для анализа инвестиционных проблем IT-безопасности на основе теории игр, которая позволяет преодолеть некоторые из этих ограничений. Мы использовали эту модель, чтобы понять значение технологий.

Перспективным направлением для дальнейших исследований является совершенствование модели на основе проведения эмпирических исследований, при этом необходимо обращать внимание на то, как организации инвестируют информационную безопасность, как они оценивают потенциальные потери, вероятности возникновения и реализации угроз не практике.

Источники и литература:

1. Lawrence A. Gordon. The Economics of Information Security Investment / Lawrence A. Gordon, Martin P. Loeb // ACM Transactions on Information and System Security. - 2002. - Vol. 5. - № 4.
2. Woohyun Shim. Vulnerability and Information Security Investment under Interdependent Risks: a Theoretical Approach / Woohyun Shim // Asia Pacific Journal of Information Systems. - 2011. - Vol. 21. - No. 4.
3. Cavusoglu H. A model for evaluating IT security investments / Cavusoglu H., Mishra B., Raghunathan S. // Communications of the ACM. - 2004. - Т. 47. - №. 7. - С. 87-92.
4. Петренко С. А. Оценка затрат на кибербезопасность / С. А. Петренко // Труды Института системного анализа Российской академии наук. - 2006. - Т. 27. - С. 234-265.
5. Собакин И. Б. Анализ подходов к определению оптимального объема инвестиций в информационную безопасность / И. Б. Собакин // Труды ИСА РАН. - 2012. - Том 62.- С. 63-68