УДК 004.056.5 Вестник УрФО № 2(32) / 2019, с. 39–44

Кляус Т. К., Гатчин Ю. А.

DOI: 10.14529/secur190206

ПОДХОД К ОЦЕНКЕ ЭФФЕКТИВНОСТИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ ЭКОНОМИЧЕСКИХ МЕТРИК БЕЗОПАСНОСТИ

Необходимость обеспечения защищенности информации, циркулирующей в информационных системах предприятий и организаций, в совокупности с необходимостью постоянного снижения расходов требует принятия рациональных решений, касающихся затрат на информационную безопасность. В настоящей статье затраты на систему защиты информации рассматриваются в качестве инвестиций капитала, которые не приводят к увеличению прибыли предприятия, но предотвращают ущерб. Рассматриваются экономические метрики информационной безопасности. Предлагается оценка эффективности системы защиты информации на основе оптимизации критерия общего вида, при котором выполняется требование максимизации индекса рентабельности инвестиций в информационную безопасность ROI (Return on Investment) и минимизации индекса прибыли злоумышленника от реализации атаки ROA (Return on Attack).

Ключевые слова: *информационная безопасность, информационная система, система защиты информации, оценка эффективности системы защиты информации, обобщенный критерий эффективности.*

Klyaus T. K., Gatchin Yu. A.

AN APPROACH TO INFORMATION SECURITY SYSTEM EFFECTIVENESS EVALUATION USING ECONOMIC SECURITY METRICS

The necessity of security maintenance of information processed by information systems in enterprises and organizations in conjunction with the necessity of expenditure steady decline requires of security managers reasonable decision-making relating to information security costs. In this article information security costs are considered as capital requirements that do

not lead to increase in profits, but prevent losses. Economic metrics of information security are considered. An approach to information security system effectiveness evaluation based on optimization of general criterion that meets the requirements of maximizing the Return on Investment index (ROI) and minimizing the Return on Attack index (ROA) is proposed.

Keywords: *information security, information system, information security system, information security system effectiveness evaluation, generalized effectiveness criterion.*

Введение

Согласно докладу Всемирного экономического форума о глобальных рисках для предпринимательства («Global risks of highest concern for doing business 2018»), кибератаки, а также хищение и фальсификация данных входят в перечень наиболее опасных рисков для бизнеса, занимая в мировом рейтинге 8 и 17 место соответственно. Растет как распространенность рисков информационной безопасности, так и их потенциал – количество атак на бизнес за последние 5 лет возросло почти вдвое, значительные негативные финансовые последствия инцидентов информационной безопасности обусловлены атаками вирусов-вымогателей, растущей тенденцией является использование кибератак для нарушения функционирования критически важных объектов [1].

Для идентификации уязвимостей, устранения угроз и рисков информационной безопасности применяется управление рисками – процесс, направленный на максимизацию прибыли предприятия путем минимизации вероятности реализации угроз и причиняемого ими ущерба. В различных источниках указывается разное количество этапов процесса управления рисками, но можно выделить два основных, повторяемых циклически: оценка (измерение) рисков и выбор эффективных и экономичных защитных средств (нейтрализация рисков) [2].

Оценка рисков предполагает определение требований к информационной системе (ИС), идентификацию и анализ ее уязвимостей и атак, использующих обнаруженные уязвимости, оценку вероятностей реализации атак и стоимости причиненного атакой ущерба. В настоящее время разработано большое количество методов анализа и оценки рисков (CRAMM, RiskWatch, COBRA, OCTAVE и т.д.), некоторые методы зафиксированы в национальных и международных стандартах (ISO/IEC 31010:2009, NIST SP 800-30).

Этап выбора контрмер направлен на снижение вероятности возникновения инцидента безопасности и снижения потенциального ущерба от его реализации. Он предполагает выбор контрмер, их анализ с точки зрения эффективности, рассмотрение альтернативных решений и выбор наилучшего из них. Уровень расходов на информационную безопасность определяется финансовыми возможностями предприятия. Необходимость обеспечения защищенности обрабатываемой в ИС информации, сохранения деловой репутации и соответствия принятым в стране нормативно-правовым актам в условиях конкурентной борьбы требует принятия рациональных решений, касающихся затрат на информационную безопасность.

Инвестиции в информационную безопасность

Затраты на информационную безопасность могут рассматриваться в качестве инвестиций капитала, однако, как правило, они рассматриваются как операционные расходы в течение периода [3]. В статье [4] проведен анализ более 200 научных работ, на основании которого выявлено, что принятие инвестиционных решений может быть обосновано с помощью:

- микроэкономических подходов (подходов, основанных на теории игр);
- финансового анализа (расчета рентабельности инвестиций, чистой приведенной стоимости, внутренней нормы рентабельности);
- управленческого анализа (подходов, основанных на теориях принятия решений, управления рисками, теории организаций).

В настоящей статье подход к оценке эффективности инвестиций в информационную безопасность будет рассматриваться с помощью методов финансового анализа.

Особенность инвестиций в обеспечение информационной безопасности заключается в том, что они не приводят к увеличению прибыли предприятия, но оказывают положительное влияние на его эффективность, так как предотвращают ущерб [4]. Для оценки затрат и выгод от обеспечения информационной безопасности используются экономические метрики безопасности.

Экономические метрики информационной безопасности

Известны две общие категории рассчитываемых экономических метрик информационной безопасности [5]:

• показатели, оценивающие выгоды (прибыль) от внедрения мер защиты информации;

• показатели, представляющие собой инвестиционные метрики.

Рассмотрим подробнее каждую категорию.

1. Оценка выгод (прибыли) от внедрения мер защиты информации.

Выгоды от внедрения защитных мер обеспечиваются за счет уменьшения величины ущерба от инцидентов информационной безопасности.

1.1. ALE (Annual Loss Exposure) – годовые ожидаемые потери.

Годовые ожидаемые потери представляют собой финансовые потери предприятия и рассчитываются по формуле:

$$ALE = SLE * ARO, \quad (1)$$

где: *SLE* (Single Loss Exposure) – потенциальный ущерб от реализации единичной угрозы; *ARO* (Annual Rate of Occurrence) – ожидаемое ежегодное количество атак.

Потенциальный ущерб от реализации единичной угрозы рассчитывается по формуле

$$SLE = AV * EF, \quad (2)$$

где: *AV* – стоимость активов предприятия, относящихся к информационной безопасности; *EF* – коэффициент риска потерь от реализации угроз, выраженный в долях от стоимости активов предприятия, относящихся к системе информационной безопасности.

1.2. EBIS (Expected Benefit of Information Security) – ожидаемые выгоды от инвестиций в обеспечение информационной безопасности.

Ожидаемые выгоды от инвестиций в обеспечение информационной безопасности представляют собой разность между годовыми ожидаемыми потерями при отсутствии мер безопасности (ALE_0) и годовыми ожидаемыми потерями при использовании защитных мер (ALE_s):

$$EBIS_S = ALE_0 - ALE_S. \quad (3)$$

1.3. ENBIS (Expected Net Benefit of Information Security) – ожидаемые чистые выгоды от инвестиций в обеспечение информационной безопасности.

Ожидаемые чистые выгоды от инвестиций в обеспечение информационной безопасности представляют собой разность между ожидаемой прибылью от инвестиций в обеспечение информационной безопасности и затратами предприятия на реализацию контрмер:

$$ENBIS_S = EBIS_S - CSI = ALE_0 - ALE_S - CSI, \quad (4)$$

где: *CSI* – затраты предприятия на реализацию контрмер.

2. Инвестиционные метрики

2.1. ROI (ROSI) (Return on Investment / Return on Security Investment) – рентабельность инвестиций в информационную безопасность.

Рентабельность инвестиций в информационную безопасность – это концепция, связывающая расходы на меры и средства защиты информации с управлением рисками для демонстрации финансовых выгоды для организации [6]. Рентабельность инвестиций представляет собой соотношение ожидаемой чистой прибыли от инвестиций в обеспечение информационной безопасности к затратам на реализацию контрмер:

$$ROI = \frac{ENBIS_S}{CSI} = \frac{ALE_0 - ALE_S - CSI}{CSI}. \quad (5)$$

В работе [7] индекс ROI предлагается рассчитывать на основании следующей формулы:

$$ROI = \frac{[ALE * RM - CSI]}{CSI}; \quad (6)$$

где *RM* – показатель эффективности контрмеры.

Годовые ожидаемые потери *ALE* рассчитывается по формуле:

$$ALE = AV * ARO * EF. \quad (7)$$

ROI (ROSI) является популярной метрикой в силу многих факторов: простоты для понимания и вычисления, доступности данных бухгалтерского учета и официальной финансовой документации и т.д. Показатель позволяет проводить сравнительный анализ различных проектов и фокусируется на одной из основных корпоративных метрик – прибыльности [6].

2.2. ROA (Return on Attack) – выгоды (прибыль) злоумышленника от реализации атаки.

Применение индекса ROA впервые предложено в работе [8]. Индекс предназначен для измерения того, как изменяется сложность реализации атаки злоумышленником с принятием меры безопасности. ROA – это превышение доходов атакующей стороны над затратами, которые он несет из-за принятия подразделением по защите информации мер безопасности.

$$ROA = \frac{[GI*(1-RM)-(Cost_a+Cost_{ac})]}{(Cost_a+Cost_{ac})}, \quad (8)$$

где: *GI* – ожидаемая выгода от атаки (принимается равной показателю ALE); $Cost_a$ – постоянные расходы атакующей стороны; $Cost_{ac}$ – дополнительные расходы атакующей стороны.

Обоснование критерия для оценки эффективности системы защиты информации

Задачей специалистов по информационной безопасности является выбор технических мер защиты информации, которые дают возможность максимизации рентабельности инвестиций в информационную безопасность ROI и минимизации прибыли атакующей стороны ROA. Гарантированный выбор эффективных контрмер может сводится к решению следующих задач [7]:

1. Максимизации индекса ROI и минимизации индекса ROA. Как следует из формул (6) и (8), решение данной задачи может быть сведено к повышению показателя эффективности контрмеры RM за счет выбора программно-аппаратных средств, обеспечивающих оптимальную конфигурацию системы защиты информации.

2. Обеспечения условий оптимальности по Парето, т.е. такого состояния системы защиты, при котором значение каждого частного критерия, описывающего ее состояние, не может быть улучшено без ухудшения положения других элементов.

3. Оптимизации критерия общего вида, при котором одновременно выполняется требование максимизации индекса ROI и минимизации индекса ROA.

В настоящей статье предлагается реализация решения задачи в соответствии с указанным выше пунктом 3 на основе подхода, изложенного в работе [7].

Преобразуем выражения (6) и (8) к следующему виду:

$$ROI = \frac{[ALE*RM]}{CSI} - CSI, \quad (9)$$

$$ROA = \frac{[GI*(1-RM)]}{} - 1, \quad (10)$$

$$CA = Cost_a^{CA} + Cost_{ac}, \quad (11)$$

где: *CA* – суммарные постоянные и дополнительные расходы атакующей стороны.

Оценка эффективности системы защиты информации на основе оптимизации критерия общего вида

На основании изложенного выше, для оценки эффективности системы защиты информации ИС предложим специально выбранный критерий общего вида, при котором одновременно выполняется требование максимизации рентабельности инвестиций в систему безопасности ROI и минимизации прибыли от нападения атакующей стороны ROA.

Одним из вариантов, удовлетворяющих данному требованию, является следующее условие:

$$\sqrt{\sum_{i=1}^{n} w_i * \left(\frac{ROA_i}{ROI_i}\right)^2} \to min, \quad (12)$$

при одновременном росте индекса ROI_i и снижении индекса ROA_i для каждой *i*-ой угрозы (атаки).

Одно из преимуществ данного критерия – возможность учета всех атак на ИС с соответствующей вероятностью их реализации, определяемой весовым коэффициентом w_i.

Значение весового коэффициента w_i может быть присвоено посредством экспертных оценок, полученных на основе статистических данных и (или) значений, рассчитанных с помощью теории вероятностей. Значение вероятностей реализации атак может быть найдено с помощью графических способов анализа атак, позволяющих провести количественный анализ их сценариев. В частности, для прогнозирования вероятностей реализации атак может быть использован метод анализа дерева событий [9].

При анализе зависимостей (6), (7) и (8) становится очевидно, что при заданных значениях параметров *ALE*, *CSI*, *GI* и *CA*, определяющих затраты защищающей стороны на систему безопасности и затраты атакующей стороны на реализацию атак, поведение индексов ROI_i и ROA_i для *i*-ой угрозы зависит от показателя эффективности контрмеры RM_i.

На основании данного вывода, показатель эффективности контрмеры RM_i определяется в качестве исходной переменной. Оптимизация критерия даст числовые значения параметрам RM_i для каждой отдельной *i*-ой угрозы. Такая количественная оценка позволяет специалистам по защите информации принимать решения относительно приобретения средств защиты информации.

Задача поиска экстремума предложенного критерия для оценки эффективности сводится к задаче нелинейного программирования, решаемой численными методами оптимизации.

Заключение

Необходимость обеспечения защищенности обрабатываемой в ИС информации и рационального расходования средств предприятий и организаций обязывает применять меры по защите информации, которые соответствовали бы как техническим, так и экономическим

критериям эффективности. Методы математического программирования предназначены для нахождения наилучшего решения среди многих потенциально возможных, вследствие чего они широко применяются для решения задачи минимизации рисков информационной, экономической и промышленной безопасности. Наиболее распространенными методами математического программирования, используемыми для решения задач управления рисками, являются методы линейного [10, 11] и динамического программирования [12, 13].

В настоящей статье задача оценки эффективности системы защиты информации сводится к задаче нелинейного программирования. Её решение предполагает оптимизацию критерия общего вида, при котором выполняется требование максимизации индекса рентабельности инвестиций в информационную безопасность ROI и минимизации индекса прибыли злоумышленника от реализации атаки ROA. Сформулированная задача может быть решена с помощью градиентных методов нелинейного программирования – численных методов решения, сводящихся к нахождению экстремумов функции.

Литература

1. Global risks of highest concern for doing business [Электронный ресурс] // The World Economic Forum. Режим доступа: http://reports.weforum.org/global-risks-2018/global-risks-of-highest-concern-for-doing-business-2018/, (дата обращения: 10.02.2019).

2. Управление рисками [Электронный ресурс] // НОУ «Интуит». Режим доступа: http://www.intuit.ru/studies/professional_retraining/941/courses/10/lecture/308, (дата обращения: 10.02.2019).

3. Böhme R., Nowey T. Economic Security Metrics // Dependability Metrics. Springer, Berlin, Heidelberg. – 2008. – Vol. 4909 in LNCS. – P. 176-187.

4. Weishäupl E., Yasasin E., Schryen G. IT Security Investments Through the Lens of the Resource-Based View: A new Theoretical Model and Literature Review // European Conference of Information Systems. – 2015.

5. Böhme R. Security Metrics and Security Investment Models // IWSEC 2010: Advances in Information and Computer Security. – 2010. – Vol. 6434 of LNCS. – P. 10-24.

6. Economics of security: facing the challenges. A multidisciplinary assessment. [Электронный ресурс] // ENISA – European Network and Information Security Agency. Режим доступа: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/files/EoS%20Final%20report/, (дата обращения: 10.02.2019).

7. Bistarelli S., Fioravanti F., Peretti P. Defense trees for economic evaluation of security investments // Proceedings of International Conference on Availability, Reliability and Security (ARES'06). – 2006. – P. 423-430.

8. Cremonini M., Martini P. Evaluating information security investments from attackers perspective: the Return-On-Attack (ROA) // Workshop on Economics of Information Security. – 2005.

9. Кляус Т.К., Гатчин Ю.А. Определение вероятности реализации атак на информационную систему с помощью деревьев событий. // Вестник УрФО. Безопасность в информационной сфере. – 2018. – № 4 (30). – С. 31-37.

10. Иванченко П.Ю., Кацуро Д.А., Медведев А.В., Трусов А.Н. Математическое моделирование информационной и экономической безопасности на предприятиях малого и среднего бизнеса // Фундаментальные исследования. – 2013. – № 10-13. – С. 2860-2863.

11. Зикратов И.А., Одегов С.В., Смирных А.В. Оценка рисков информационной безопасности в облачных сервисах на основе линейного программирования // Научно-технический вестник информационных технологий, механики и оптики. – 2013. – №1 (83). – С.141-144.

12. Ендовский А.С. Разработка методики управления рисками информационной безопасности на основе метода динамического программирования // Сборник тезисов докладов II Всероссийского конгресса молодых ученых. Выпуск 1. – 2013. – С. 135-136.

13. Ростова Е.П. Постановка задачи динамического программирования для распределения средств по управлению рисками на предприятии // Известия Самарского научного центра РАН. – 2013. – № 6-4. – С. 1078-1081.

References

1. Global risks of highest concern for doing business. The World Economic Forum. Available at: http://reports.weforum.org/global-risks-2018/global-risks-of-highest-concern-for-doing-business-2018/ (accessed 10.02.2019).

2. Upravlenie riskami. NOU «Intuit». [Risk management. National Open University Intuit]. Available at: http://www.intuit.ru/studies/professional_retraining/941/courses/10/lecture/308 (accessed 10.02.2019).

3. Böhme R., Nowey T. Economic Security Metrics. Dependability Metrics. Springer, Berlin, Heidelberg, 2008, vol. 4909 in LNCS, pp. 176-187.

4. Weishäupl E., Yasasin E., Schryen G. IT Security Investments Through the Lens of the Resource-Based View: A new Theoretical Model and Literature Review. European Conference of Information Systems, 2015.

5. Böhme R. Security Metrics and Security Investment Models. IWSEC 2010: Advances in Information and Computer Security, 2010, vol. 6434 of LNCS, pp. 10-24.

6. Economics of security: facing the challenges. A multidisciplinary assessment. ENISA – European Network and Information Security Agency. Available at: https://www.enisa.europa.eu/topics/threat-risk-management/riskmanagement/files/

7. EoS%20Final%20report/ (accessed 10.02.2019).

8. Bistarelli S., Fioravanti F., Peretti P. Defense trees for economic evaluation of security investments. Proceedings of International Conference on Availability, Reliability and Security (ARES'06), 2006, pp. 423-430.

9. Cremonini M., Martini P. Evaluating information security investments from attackers perspective: the Return-On-Attack (ROA). Workshop on Economics of Information Security, 2005.

10. Klyaus T.K., Gatchin Ju.A. Probability Evaluation of Attacks on Information System Using Event Tree Analysis [Opredelenie verojatnosti realizacii atak na informacionnuju sistemu s pomoshh'ju derev'ev sobytij]. Vestnik UrFO. Bezopasnost' v Informacionnoj Sfere [UrFR Newsletter. Information Security], 2018, no. 4(30), pp. 31-37.

11. Ivanchenko P.Y., Katsuro D.A., Medvedev A.V., Trusov A.N. Mathematical Modeling of Information and Economic Security of Small and Medium Business [Matematicheskoe modelirovanie informacionnoj i jekonomicheskoj bezopasnosti na predprijatijah malogo i srednego biznesa]. Fundamental'nye Issledovanija [Fundamental Research], 2013, no. 10-13, pp. 2860-2863.

12. Zikratov I. A., Odegov S. V., Smirnykh A. V. Information Security Risks Optimization in Cloudy Services on the Basis of Linear Programming [Ocenka riskov informacionnoj bezopasnosti v oblachnyh servisah na osnove linejnogo programmirovanija]. Nauchno-tehnicheskij Vestnik Informacionnyh Tehnologij, Mehaniki i Optiki [Scientific and Technical Journal of Information Technologies, Mechanics and Optics], 2013, no. 1(83), pp. 141-144.

13. Endovskij A.S. A Development of information Security Risk Management Methodology Based on Dynamic Programming Method [Razrabotka metodiki upravlenija riskami informacionnoj bezopasnosti na osnove metoda dinamicheskogo programmirovanija]. Sbornik tezisov dokladov II Vserossijskogo kongressa molodyh uchenyh [Proceedings of II All-Russian Congress of Young Scientists], 2013, vol. 1, pp. 135-136.

14. Rostova E.P. Formulation of the Problem of Dynamic Programming for the Allocation of Risk Management at the Enterprise [Postanovka zadachi dinamicheskogo programmirovanija dlja raspredelenija sredstv po upravleniju riskami na predprijatii]. Izvestija Samarskogo nauchnogo centra RAN [Proceedings of the Samara Scientific Center of the Russian Academy of Sciences], 2013, no. 6-4, pp. 1078-1081.

КЛЯУС Татьяна Константиновна, аспирант факультета Безопасности информационных технологий Федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики». Россия, 197101, г. Санкт-Петербург, Кронверкский пр., д. 49. E-mail: t_klyaus@corp.ifmo.ru

ГАТЧИН Юрий Арменакович, доктор технических наук, профессор факультета Безопасности информационных технологий Федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики». Россия, 197101, г. Санкт-Петербург, Кронверкский пр., д. 49. E-mail: gatchin@mail.ifmo.ru

KLYAUS Tatiana, Postgraduate Student, Department of Information Technology Security, Federal State Autonomous Educational Institution of Higher Education "St. Petersburg National Research University of Information Technologies, Mechanics and Optics". Russia, 197101, Saint Petersburg, Kronverkskii avenue, 49. E-mail: t_klyaus@corp.ifmo.ru

GATCHIN Yurii, doctor of technical sciences, professor of the Faculty of Secure Information Technologies Federal State Autonomous Educational Institution of Higher Education "St. Petersburg National Research University of Information Technologies, Mechanics and Optics". Russia, 197101, Saint Petersburg, Kronverkskii avenue, 49. E-mail: E-mail: gatchin@mail.ifmo.ru