Раздел V. Концептуальные и прикладные вопросы информационной безопасности

УДК 004.051

Е.Н. Ефимов

МОДЕЛИРОВАНИЕ ОЦЕНОК ЭФФЕКТИВНОСТИ МЕРОПРИЯТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПАНИИ ПРИ ВОЗДЕЙСТВИИ СЛУЧАЙНЫХ ФАКТОРОВ ОКРУЖАЮЩЕЙ СРЕДЫ

На всех этапах жизненного цикла системе защиты информации присущи неопределенность ее свойств в условиях реального воздействия случайных факторов из внешней и внутренней среды. По мере реализации проекта системы неопределенность снижается, но никогда эффективность функционирования не может быть адекватно выражена и описана детерминированными показателями. Тогда к оценке эффективности реализации и функционирования систем защиты информации наилучшим образом применимы вероятностные методы. В соответствии с этими методами уровни гарантий безопасности системы трансформируются в доверительные вероятности соответствующих оценок показателей. В этих условиях данные для оценки эффективности мероприятий по повышению информационной безопасности можно получить с помощью имитационного моделирования. Предложенная методика расчета оценки результата от воздействия проведенных мероприятий по информационной безопасности в компании базируется на моделировании оценок предотвращенных потерь. Значение предотвращенных потерь может быть рассчитано, исходя из вероятности возникновения инцидента информационной безопасности и возможных экономических потерь от него до и после реализации мероприятий по обеспечению информационной безопасности на объекте. Получаемое в результате моделирования суммарное значение предотвращенных потерь по всем инцидентам информационной безопасности позволяет задать и осуществить сценарный расчет возможного эффекта от проведенных мероприятий. Итоговый расчет эффективности мероприятий по повышению информационной безопасности компании может быть выполнен любым из известных методов. В мировой практике для оценки эффективности инвестиций широко применяется стандартный метод анализа затрат и выгод (Cost Benefit Analysis – CBA). Реализация предлагаемого варианта расчета эффективности мероприятий по повышению информационной безопасности выполнена на примере по методике CBA. Основным достоинством предлагаемой методики расчета эффективности мероприятий по повышению информационной безопасности является учет неопределенности реальной действительности с помощью имитационного моделирования. Это позволяет, в определенной степени, повысить достоверность расчетов эффекта.

Информационная безопасность; эффективность; моделирование; предотвращенные потери; сценарии расчета.

E.N. Efimov

MODELING ESTIMATES OF THE EFFECTIVENESS OF INFORMATION SECURITY COMPANY AFFECTED BY RANDOM ENVIRONMENTAL FACTORS

At all stages of the life cycle of the information security system inherent uncertainty of its properties in terms of the real impact of random factors of the external and internal environment. As the project system uncertainty is reduced, but never the efficiency cannot be adequately expressed and described by deterministic parameters. Then to evaluate the effectiveness of the im-

plementation and operation of information security systems to best apply probabilistic methods. In accordance with these methods, the levels of the safeguards system are transformed to the probability of the corresponding estimates. Under these conditions, data to assess the effectiveness of measures to improve information security can be obtained using simulation. The methods of calculating the evaluation result from the effects of measures for information security in the company is based on modeling estimates of avoided losses. The value of avoided losses can be calculated on the basis of the likelihood of incident information security and possible economic losses from him before and after the implementation of measures to ensure information security on the object. The resulting simulation of the total value of avoided losses for all information security incidents allows you to specify and implement scenario-based calculation of possible benefits from these measures. The final calculation of efficiency measures to improve information security can be performed by any known methods. In the world practice for evaluating the effectiveness of it projects widely used standard method of analysis of costs and benefits (Cost Benefit Analysis - CBA). Implementation of the proposed calculation of the effectiveness of measures to improve information security is made on the example in the method of CBA. The main advantage of the proposed method of calculating the effectiveness of measures to improve information security is the uncertainty of the real world with simulations. This allows, to a certain extent, to increase the validity of the estimates of effect.

Information security; efficiency; modeling; prevented loss; scenario of the calculation.

Постановка проблемы. Принято считать, что затраты на обеспечение информационной безопасности (ИБ) компании эффективны, если они обеспечивают выполнение требований государственных нормативных документов и стандартов, а также концепции ИБ [1, 2]. Такое понимание связано с тем, что для объективной оценки экономического эффекта ИБ нет универсальных методов. Под экономическим эффектом обычно понимают превышение стоимостных оценок конечных результатов соответствующих мероприятий над совокупными затратами ресурсов на их проведение за расчетный период [3–6].

Сложность оценки эффективности мероприятий по ИБ обусловлена целым рядом обстоятельств [7–9]. В соответствии с теорией оценки эффективности систем, качество любого объекта, в том числе и системы защиты информации (СЗИ), проявляется лишь в процессе его использования по назначению, поэтому объективной является оценка по эффективности применения [10–13].

Кроме этого, создание СЗИ фактически связано с неизвестными событиями в будущем и поэтому всегда содержит элементы неопределенности. Причем этапу проектирования СЗИ вначале сопутствует значительная неопределенность. По мере реализации проекта ее уровень снижается, но никогда эффективность СЗИ не может быть адекватно выражена и описана детерминированными показателями. Процедуры испытаний, сертификации или лицензирования не устраняют полностью неопределенность свойств СЗИ или ее отдельных элементов и не учитывают случайный характер атак. Поэтому объективной характеристикой качества СЗИ (степенью ее приспособленности к достижению требуемого уровня безопасности в условиях реального воздействия случайных факторов) может служить только вероятность, например, характеризующая степень возможностей конкретной СЗИ при заданном комплексе условий, достижение цели операции или выполнение задачи системой. Данная вероятность должна быть положена и в основу комплекса показателей, и критериев оценки эффективности СЗИ. При выборе конкретного критерия необходимо его согласование с целью СЗИ [3].

Обычно при синтезе системы возникает многокритериальная задача сравнения различных структур СЗИ. В число рассматриваемых в задаче показателей входят и показатели эффективности, имеющие вероятностно-временной характер функций распределения. В частности, к ним относятся вероятность преодоления системы защиты информации за некоторое время [14–16].

Таким образом, к оценке эффективности функционирования СЗИ наилучшим образом применимы вероятностные методы, в соответствии с которыми уровни гарантий безопасности СЗИ трансформируются в доверительные вероятности соответствующих оценок показателей. Оценка оптимального уровня гарантий безопасности в компании в значительной степени зависит от предотвращенного ущерба. Для получения численных оценок риска необходимо знать распределения случайных величин ущерба. Во многих случаях такие оценки можно получить, например, с помощью имитационного моделирования или по результатам активного аудита СЗИ [3].

Когнитивные модели могут быть использованы для оценки эффективности процессов. Они позволяют объединить элементы внутренней и внешней экономической среды компании в единую систему, а также проанализировать систему в целом и отдельные ее компоненты, не теряя взаимосвязей между ними. Исследователь в модели может осуществить выбор комплекса мероприятий (факторов), определить их возможную или желаемую силу и направленность воздействия на ситуацию, а также выбор наблюдаемых индикаторов, характеризующих развитие ситуации [17]. Основное достоинство когнитивного моделирования заключается в том, что появляется возможность учесть как количественные, так и качественные показатели деятельности исследуемых процессов. А недостаток в том, что оно позволяет выполнить лишь сценарный прогноз развития ситуации [4, 5].

Резюмируем вышеизложенное. Во-первых, эффективность мероприятий по ИБ в СЗИ вряд ли может быть определена в детерминированных оценках. Во-вторых, эффективность мероприятий по ИБ в СЗИ наилучшим образом может быть представлена вероятностными характеристиками – функциями распределения показателей, прежде всего предотвращенного ущерба. Таким образом, при оценке эффективности мероприятий ИБ необходим учет неопределенности воздействия реальной действительности на СЗИ компании.

Вариант решения проблемы. В расчетах эффективности, как правило, фигурируют две основные компоненты: получаемый результат от внедрения мероприятия и затраты, необходимые на его реализацию.

Конечным результатом проведения мероприятий по обеспечению ИБ обычно считают значение предотвращенных потерь. Значение предотвращенных потерь P_i может быть рассчитано исходя из вероятности возникновения i-го инцидента ИБ (i = 1, 2, …n) и возможных экономических потерь от него до и после реализации мероприятий по обеспечению ИБ на объекте:

$$\boldsymbol{P_i = P_i' - P_i''},$$

где P_i' и P_i'' – потери от реализации угроз до и после внедрения мероприятий, повышающих уровень ИБ соответственно.

По сути, значение предотвращенных потерь отражает ту часть прибыли, которая могла быть потеряна, если бы не применялись мероприятия, повышающие уровень ИБ [18].

Тогда суммарное значение предотвращенных потерь P по всем инцидентам ИБ определяется как

$$\boldsymbol{P = \sum_{i=1}^{n} (P_i + R_i)}$$

где R_i – непосредственно возвращаемые средства компании, например, возмещение третьей стороной, которая виновна в инциденте ИБ, средства, полученные в результате применения штрафных санкций к сотрудникам, виновным в инцидентах ИБ, страховое возмещение и другое.

Сложность точного определения значения предотвращенных потерь очевидна [13]. Источником данных для расчета потерь может быть либо статистика, либо экспертные методы оценки инцидентов ИБ. В первом случае статистика может

отсутствовать, или она недостаточна и даже недоступна для принятия решений. Во втором случае обычно превалирует субъективизм оценок, что не повышает достоверности расчетов. Выходом из создавшегося положения может быть совместное применение обоих методов в рамках имитационного моделирования значений предотвращенных потерь. Данный метод ("процессно-статистический подход" в трактовке автора – проф. Хубаева Г.Н.) достаточно хорошо зарекомендовал себя в различных сферах деятельности [19].

Используя процессно-статистический подход, предлагается следующая последовательность действий по имитационному моделированию значений предотвращенных потерь [6, 20]:

- разбиение возможных потерь на группы, например, по инцидентам ИБ;
- оценка экспертным путем или на основании статистики значения величины потерь (тяжести последствий) по каждому инциденту: минимальное (*min*), наиболее вероятное (*mid*) и максимальное (*max*) значения (до и после проведения мероприятий по ИБ);
- моделирование значений величины потерь (до и после проведения мероприятий по повышению ИБ), на основе определенных выше характеристик (по треугольному закону распределения);
- расчет суммарного значения предотвращенных потерь на основании моделируемых значений;
- расчет статистических характеристик моделированных суммарных значений предотвращенных потерь;
- расчет показателей эффективности проведенных мероприятий и формулировка выводов.

В результате расчета получаем распределение суммарного значения предотвращенных потерь. Знание закона распределения предотвращенных потерь позволяет легко оценить вероятность конкретного значения в любой выбранной точке или вероятность нахождения значений предотвращенных потерь в заданном интервале. Данную вероятность, с конкретным значением суммы предотвращенных потерь, можно считать в обосновании эффективности мероприятий по повышению ИБ гарантийной вероятностью.

Вторая компонента, используемая при оценке эффективности мероприятий ИБ компании, – это затраты на их обеспечение. Такого рода затраты для совокупности мероприятий по ИБ могут включать:

- затраты на содержание подразделения ИБ (обычно как доля затрат);
- затраты на закупку и содержание аппаратно-программных средств защиты информации (непосредственно для реализации мероприятий);
- затраты на закупку и содержание иных средств защиты информации, непосредственно для реализации мероприятий.

Полученные таким образом компоненты (результат и затраты) могут быть использованы для расчета эффективности мероприятий по повышению ИБ компании с гарантийной вероятностью в любом из известных методов. Так, в мировой практике для оценки эффективности ИТ-проектов довольно широко применяется стандартный метод анализа затрат и выгод *Cost Benefit Analysis* (*CBA*). В данном методе выполняется оценка и сравнение выгод (*benefit*), полученных в результате осуществления проекта, с затратами (*cost*) на его реализацию. При этом рассчитываются такие показатели, как чистый приведенный доход (*Net Present Value, NPV*), индекс рентабельности *(Profitability index, PI),* внутренняя норма доходности *(Internal rate of return, IRR)* и другие.

Рассмотрим реализацию предлагаемого варианта расчета эффективности на примере. ИТ-проект представляет собой внедрение трех мероприятий по ИБ (E_1, E_2, E_3), суммарные затраты по которым составляют 1200 тыс. руб. и процентная ставка r = 10 %. Инвестиции осуществляются в течение первого периода проекта.

Затраты по мероприятиям ИБ и оценки объемов возможных поступлений средств от предотвращенных потерь по ним приведены в табл. 1.

Таблица 1

Затраты и возможное поступление средств по мероприятиям ИБ

Мероприятия ИБ	Затраты, тыс. руб.	Поступления, тыс. руб.			
		Обозн.	*min*	*mid*	*max*
E_1	650	P_1	150	260	410
E_2	340	P_2	100	170	300
E_3	210	P_3	50	110	200
Сумма	1200		300	540	910

Рассчитаем чистый приведенный доход (*NPV*), индекс рентабельности (*PI*), внутреннюю норму доходности (*IRR*), модифицированную внутреннюю норму доходности (*MIRR*), дисконтированный срок окупаемости проекта (*DPB*). При этом выполним сценарный расчет и сделаем выводы о целесообразности инвестиций.

Вначале осуществляется моделирование объемов возможных поступлений средств по приведенным мероприятиям (предотвращенный ущерб). Данные по поступлению средств, полученные в процессе их моделирования, обобщаются как сумма поступлений в итоговое распределение (рис. 1). Описательная статистика итогового распределения суммы предотвращенного ущерба приведена в табл. 2.

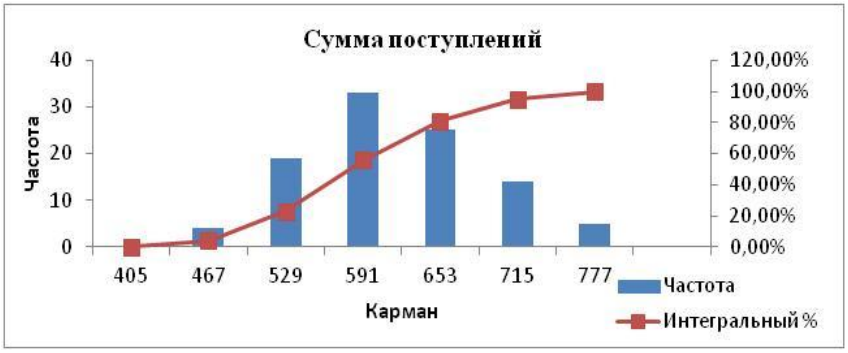

Рис. 1. Суммарное распределение возможного поступления средств от мероприятий E_1—E_3

Таблица 2

Описательная статистика распределения суммы поступлений средств

Показатель	Значение
Среднее	587,82
Стандартная ошибка	7,43
Стандартное отклонение	74,30
Дисперсия выборки	5521,24
Минимум	408
Максимум	768

Результаты моделирования и описательная статистика итогового распределения использованы для построения сценариев оценки эффективности ИТ–проекта (табл. 3).

Таблица 3

Сценарии	Обозн.	Объемы поступления платежей в период, тыс. руб.
Пессимистический	S_p	408
Наиболее вероятный	S_v	591
Оптимистический	S_o	768

Для каждого из сценариев были выполнены расчеты показателей эффективности ИТ–проекта, приведенные в табл. 4.

Для сценариев выполняются почти все условия одобрения ИТ–проекта: $NPV>0$; $PI>1$ (кроме сценария S_p); $MIRR>r$.

Окончательный выбор предлагается выполнить путем определения близости каждого из сценариев к идеальному проекту, например, с помощью Евклидова расстояния. Для этого показатель *NPV* по сценариям нормируется по отношению к максимальному значению, а также устанавливаются экспертным путем весовые коэффициенты. Идеальный проект может быть выбран, например, как {*NPV*=2; *PI*=2; *MIRR*=1}, соответственно весовые коэффициенты {0,4; 0,3; 0,3}.

Таблица 4

Показатели эффективности ИТ-проекта по сценариям

Показатели эффективности	Обозн.	Сценарии		
		S_p	S_v	S_o
Индекс рентабельности	*PI*	0,84	1,22	1,11
Дисконтированный срок окупаемости проекта	*DPB*	3,66	2,39	1,79
Чистый приведенный доход	*NPV*	93,3	269,7	132,9
Поступления, приведенные к моменту окончания проекта	*FVI*	1893,5	1956,2	1612,8
Затраты, приведенные к моменту времени 0	*PVO*	1200	1200	1200
Модифицированная внутренняя норма доходности	*MIIR*	0,12	0,18	0,16
Внутренняя норма доходности	*IIR*	0,135	0,224	0,181

По результатам расчета расстояния до идеального проекта равны для сценариев S_p, S_v и S_o соответственно 0,865; 0,392; 0,679. Таким образом, можно считать, что оптимальным вариантом является сценарий S_v (наиболее вероятный).

Заключение. На всех этапах существования СЗИ оценку ее эффективности реализации и функционирования предопределяет значительная степень неопределенности. Во-первых, этот ряд параметров производственных систем (цены, объемы, расходные коэффициенты) является по своей сути случайным, что позволяет задать его в виде интервалов значений. Во-вторых, это характеристики СЗИ, имеющих вид случайностей практически на всех этапах жизненного цикла. В соответствие с этими уровни гарантий безопасности защищаемой системы трансформируются в распределения вероятностей соответствующих оценок показателей.

Предлагаемая методика оценки результата от воздействия проведенных мероприятий по ИБ представлена на конкретном примере. В данной методике моделируются оценка предотвращенного ущерба, являющаяся базовым показателем при обосновании экономического эффекта СЗИ.

С помощью имитационного моделирования учитывается относительная неопределенность реальной действительности, что позволяет повысить достоверность обоснования эффективности проектов ИБ. В методике возможен учет воздействия как прямых, так и косвенных факторов эффективности проектов ИБ. Знание законов распределения суммарного значение предотвращенных потерь позволяет задать и осуществить сценарный расчет оценки эффекта от внедрения ИТ–проекта с заданной гарантийной вероятностью.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. BS 7799-3:2006 Information security management systems – Part 3: Guidelines for information security risk management, 2006.
2. *Lyon Gordon F.* Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley; 2 edition. April 14, 2008.
3. *Баутов А.* Эффективность защиты информации // Открытые системы. – 2003. – № 07-08. – Режим доступа: http://www.osp.ru/os/2003/07-08/183282/.
4. *Денисов М.Ю., Долженко А.И., Ефимов Е.Н.* Когнитивное моделирование оценки эффективности электронных бизнес–отношений предприятия // Вестник Ростовского государственного экономического университета «РИНХ». – 2012. – № 1 (37). – С. 83-90.
5. *Ефимов Е.Н.* Оценка эффективности электронных бизнес–отношений предприятия // Проблемы федеральной и региональной экономики: ученые записки. – Ростов-на-Дону: Рост. гос. эконом. ун-т (РИНХ), 2011. – Вып. 14. – С. 68-75.
6. *Ефимов Е.Н.* Инвестиционный анализ проекта информационных технологий в условиях неопределенности // Известия ЮФУ. Технические науки. – 2014. – № 8 (157). – С. 66-74.
7. *Ефимов Е.Н.* Эффективность ИТ-проектов в системе сбалансированных показателей // Аспирант. – 2015. – № 2. – С. 8-10.
8. *Ефимов Е.Н., Ефимова Е.В.* Модели и технологии сетевых электронных бизнес–отношений: монография. – Ростов-на-Дону: Изд-во РГЭУ (РИНХ), 2014. – 198 с.
9. *Ефимов Е.Н., Лапицкая Г.М.* Оценка эффективности ИТ-проектов в рамках Balanced Scorecard // Информационные системы, экономика, управление трудом и производством: Уч. записки. Вып. 15. – Ростов-на-Дону: РГЭУ (РИНХ), 2013. – С. 59-65.
10. *Ефимов Е.Н., Лапицкая Г.М.* Информационная безопасность и бизнес-процессы компании // Известия ЮФУ. Технические науки. – 2013. – № 12 (149). – С. 253-260.
11. *Петухов Г.Б., Якунин В.И.* Методологические основы внешнего проектирования целенаправленных процессов и целеустремленных систем. – М.: АСТ, 2006. – 504 с.
12. *Brotby Krag, Hinson Gary* PRAGMATIC Security Metrics: Applying Metametrics to Information Security. CRC Press. January 8, 2013.
13. Shostack Adam Threat Modeling: Designing for Security. WILEY. February 17, 2014.
14. *Горбунов А., Чуменко В.* Выбор рациональной структуры средств защиты информации в АСУ. – Режим доступа: http://kiev-security.org.ua/box/2/26.shtml.
15. *Javaid Muhammad A.* Information Security: How to Ensure Privacy in a Computing Environment. September 6, 2013.
16. *Collins Michael S.* Network Security Through Data Analysis: Building Situational Awareness. O'REILLY. February 23, 2014.
17. *Jacobs Jay, Rudis Bob.* Data-Driven Security: Analysis, Visualization and Dashboards. WILEY. February 24, 2014.
18. *Андреев Кирилл.* Метод оценки экономической эффективности подразделения по защите информации // Information Security/Информационная безопасность". – 2010. – № 5. – Режим доступа: http://www.itsec.ru/articles2/Oborandteh/metod-ocenki-ekonomicheskoi-effektivnosti-podrazdeleniya-po-zashite-informacii.
19. *Хубаев Г.Н.* Процессно-статистический подход к учету затрат ресурсов при оценке (калькуляции) себестоимости продукции и услуг: особенности реализации, преимущества // Вопросы экономических наук. – 2008. – № 2. – С. 158-166.
20. *Крепков И.М., Ефимов Е.Н., Фоменко Н.М.* Анализ и учет рисков продвижения Internet–проектов предприятия // Вестник МЭИ. – 2010. – № 2. – С. 101-107.

REFERENCES

1. BS 7799-3:2006 Information security management systems – Part 3: Guidelines for information security risk management, 2006.
2. *Lyon Gordon F.* Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley; 2 edition. April 14, 2008.
3. *Bautov A.* Effektivnost' zashchity informatsii [The effectiveness of information protection], Otkrytye sistemy [Open Systems], 2003, No. 07-08. Available at: http://www.osp.ru/os/2003/07-08/183282/.
4. *Denisov M.Yu., Dolzhenko A.I., Efimov E.N.* Kognitivnoe modelirovanie otsenki ef-fektivnosti elektronnykh biznes–otnosheniy predpriyatiya [Cognitive modeling evaluation of the effectiveness of e–business relations of the company], *Vestnik Rostovskogo gosudarstvennogo ekonomicheskogo universiteta «RINKh*» [Bulletin of the Rostov state economic University "RINH"], 2012, No. 1 (37), pp. 83-90.
5. *Efimov E.N.* Otsenka effektivnosti elektronnykh biznes–otnosheniy predpriyatiya [Assessment of the effectiveness of e-business relations between enterprises], *Problemy federal'noy i regional'noy ekonomiki: uchenye zapiski* [The problems of the Federal and regional Economics: proceedings of the]. Rostov-on-Don: Rost. gos. ekonom. un-t (RINKh), 201I, Issue 14, pp. 68-75.
6. *Efimov E.N.* Investitsionnyy analiz proekta informatsionnykh tekhnologiy v usloviyakh neopredelennosti [Investment analysis of the project of information technology in conditions of uncertainty], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2014, No. 8 (157), pp. 66-74.
7. *Efimov E.N.* Effektivnost' IT-proektov v sisteme sbalansirovannykh pokazateley [The effectiveness of it projects in the balanced scorecard], *Aspirant* [Postgraduate Student], 2015, No. 2, pp. 8-10.
8. *Efimov E.N., Efimova E.V.* Modeli i tekhnologii setevykh elektronnykh biznes–otnosheniy: monografiya [Models and technologies of a network of e–business relations: monograph]. Rostov-on-Don: Izd-vo RGEU (RINKh), 2014, 198 p.
9. *Efimov E.N., Lapitskaya G.M.* Otsenka effektivnosti IT-proektov v ramkakh Balanced Scorecard [Evaluation of the effectiveness of it projects within the framework of the Balanced Scorecard], *Informatsionnye sistemy, ekonomika, upravlenie trudom i proizvodstvom: Uch. zapiski* [Information systems, Economics, management of work and production: proceedings of the], Issue. 15. Rostov-on-Don: RGEU (RINKh), 2013, pp. 59-65.
10. *Efimov E.N., Lapitskaya G.M.* Informatsionnaya bezopasnost' i biznes-protsessy kompanii [Information security and business processes of the company], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2013, No. 12 (149), pp. 253-260.
11. *Petukhov G.B., Yakunin V.I.* Metodologicheskie osnovy vneshnego proektirovaniya tselenapravlennykh protsessov i tseleustremlennykh system [Methodological basis of the external design of targeted processes and dedicated systems]. Moscow: AST, 2006, 504 p.
12. *Brotby Krag, Hinson Gary* PRAGMATIC Security Metrics: Applying Metametrics to Information Security. CRC Press. January 8, 2013.
13. Shostack Adam Threat Modeling: Designing for Security. WILEY. February 17, 2014.
14. *Gorbunov A., Chumenko V.* Vybor ratsional'noy struktury sredstv zashchity informatsii v ASU [The choice of rational structure of information protection in automated control system]. Available at: http://kiev-security.org.ua/box/2/26.shtml.
15. *Javaid Muhammad A.* Information Security: How to Ensure Privacy in a Computing Environment. September 6, 2013.
16. *Collins Michael S.* Network Security Through Data Analysis: Building Situational Awareness. O'REILLY. February 23, 2014.
17. *Jacobs Jay, Rudis Bob.* Data-Driven Security: Analysis, Visualization and Dashboards. WILEY. February 24, 2014.
18. *Andreev Kirill.* Metod otsenki ekonomicheskoy effektivnosti podrazdeleniya po zashchite informatsii [Method of economic evaluation division information security], *Informatsionnaya bezopasnost* [Information Security], 2010, No. 5. Available at: http://www.itsec.ru/ articles2/Oborandteh/metod-ocenki-ekonomicheskoi-effektivnosti-podrazdeleniya-po-zashite-informacii.

19. *Khubaev G.N.* Protsessno-statisticheskiy podkhod k uchetu zatrat resursov pri otsenke (kal'kulyatsii) sebestoimosti produktsii i uslug: osobennosti realizatsii, preimushchestva [Process-statistical approach to cost accounting resources when estimating (costing) cost of products and services: implementation and benefits], *Voprosy ekonomicheskikh nauk* [Questions of Economic Sciences], 2008, No. 2, pp. 158-166.
20. *Krepkov I.M., Efimov E.N., Fomenko N.M.* Analiz i uchet riskov prodvizheniya Internet–proektov predpriyatiya [Analysis and risk-based promotion of Internet–projects of the enterprise], Vestnik MEI [MPEI Vestnik], 2010, No. 2, pp. 101-107.

Статью рекомендовал к опубликованию к.т.н. А.П. Лапсарь.

Ефимов Евгений Николаевич – Ростовский государственный экономический университет (РИНХ); e-mail: efimov46@mail.ru; 344002, г. Ростов-на-Дону, Большая Садовая, 69, комн. 306 а; тел.: 89525721917; кафедра информационных технологий и защиты информации; д.э.н.; профессор.

Efimov Evgeny Nikolaevich – Rostov state economic University; e-mail: efimov46@mail.ru; Rostov-on-don, 344002, Large Garden, 69, room 306 a; phone: +79525721917; the Department of information technologies and information protection; dr. of ec. sc.; professor.

УДК 631.8

И.А. Калмыков, Т.А. Гиш, М.И. Калмыков, Д.О. Науменко, А.В. Дунин

ТЕХНОЛОГИЯ ЗАЩИТЫ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ НЕПОЗИЦИОННЫХ КОДОВ ДЛЯ СИСТЕМ УПРАВЛЕНИЯ УДАЛЕННЫМИ ОБЪЕКТАМИ

Для обеспечения эффективной работы системы мониторинга, контроля и управления удаленными экологически опасными объектами в настоящее время широко используются системы спутниковой связи. Введение в состав абонентского терминала управления удаленным объектом запросно-ответной системы опознавания спутника позволит программно-аппаратному комплексу перед организацией информационного обмена произвести определение статуса космического аппарата, который находится в зоне видимости. В этом случае использование системы определения «свой-чужой» позволит снизить вероятность отказов и сбоев в процессе функционирования оборудования экологически опасных технологий из-за навязывания ложных управляющих команд, поступающих от чужих космических аппаратов. Для повышения эффективности работы запросно-ответной системы в работе предлагается использовать протокол с нулевым разглашением. Однако в процессе обмена данными между спутником и объектом управления может возникнуть ситуация перехвата, модификации и навязывания ложной информации. Для обеспечения высокой степени защиты информации от несанкционированного доступа в работе предлагается использовать алгоритм шифрования, реализованный в полиномиальной системе классов вычетов. Целью работы является повышение криптозащищенности запросно-ответной системы, применение которой позволит снизить вероятность навязывания ложной информации.

Система опознавания «свой-чужой»; криптографический протокол аутентификации; псевдослучайная функция; модулярные алгебраические структуры; алгоритм шифрования; полиномиальная система классов вычетов.

I.A. Kalmykov, T.A. Gish, M.I. Kalmykov, D.O. Naumenko, A.V. Dunin

THE INFORMATION PROTECTION TECHNOLOGY USING NON-POSITIONAL CODES FOR CONTROL SYSTEMS REMOTE OBJECTS

To ensure the effective operation of the system monitoring framework, monitoring and control of remote ecologically dangerous objects at the present time widely used satellite communication systems. The introduction of the subscriber terminal control of a remote object challenge-