ОЦЕНКА ЭФФЕКТИВНОСТИ МЕРОПРИЯТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ НЕОПРЕДЕЛЕННОСТИ

Е.Н. ЕФИМОВ
доктор экономических наук, профессор кафедры информационных технологий и защиты информации, факультет компьютерных технологий и информационной безопасности, Ростовский государственный экономический университет (РИНХ)
Адрес: 344002, г. Ростов-на-Дону, ул. Большая Садовая, д. 69
E-mail: efimov46@mail.ru

Г.М. ЛАПИЦКАЯ
кандидат экономических наук, профессор кафедры информационных технологий и защиты информации, факультет компьютерных технологий и информационной безопасности, Ростовский государственный экономический университет (РИНХ)
Адрес: 344002, г. Ростов-на-Дону, ул. Большая Садовая, д. 69
E-mail: gmlapickaya@mail.ru

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 эффективность функционирования никогда 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 воздействия 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 ИТ-проектов 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 в методе 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.

Ключевые слова: информационная безопасность, эффективность, моделирование, предотвращенные потери.

Цитирование: Ефимов Е.Н., Лапицкая Г.М. Оценка эффективности мероприятий информационной безопасности в условиях неопределенности // Бизнес-информатика. 2015. № 1 (31). С.51–57.

1. 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. 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 [2, 4, 5].

Сложность оценки эффективности мероприятий по ИБ обусловлена целым рядом обстоятельств. 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 (целевое функционирование), поэтому объективной является оценка по эффективности применения [8, 9].

Кроме этого, создание СЗИ фактически связано с неизвестными событиями в будущем и поэтому всегда содержит элементы неопределенности, прежде всего в результате функционирования. 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 этом критериями оценки служат понятия пригодности и оптимальности. Пригодность означает выполнение всех установленных к СЗИ требований, а оптимальность – достижение одной из характеристик экстремального значения при соблюдении ограничений и условий на другие свойства системы. При выборе конкретного критерия необходимо его согласование с целью СЗИ [2].

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 [3].

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 [2].

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. 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, 6].

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.

2. 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:

$$P_i = P_i' - P_i'',$$

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 [1].

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

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

где Ri – 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. 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. Г.Н. Хубаева) достаточно хорошо зарекомендовал себя в различных сферах деятельности [10].

Используя процессно-статистический подход, предлагается следующая последовательность действий по имитационному моделированию значений предотвращенных потерь [7]:

✦ 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 гистограмму распределения или интегральный процент распределения суммарного значения предотвращенных потерь. Знание закона распределения суммарного значение 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 (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 показателей 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 (M_1, M_2, M_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
M_1	650	P_1	150	260	410
M_2	340	P_2	100	170	300
M_3	210	P_3	50	110	200
Сумма	1200		300	540	910

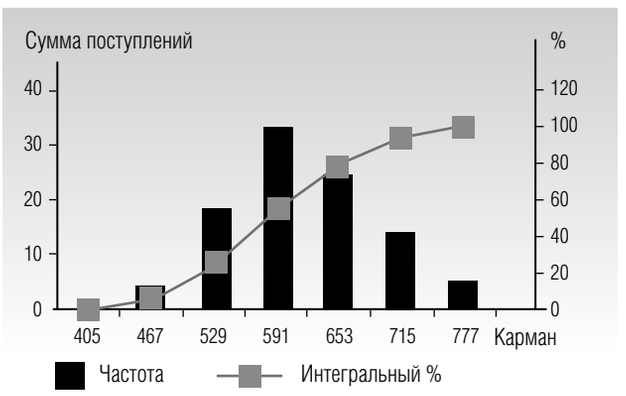

Рис. 1. Суммарное распределение возможного поступления средств от мероприятий $M_1 – M_3$

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.*

Результаты моделирования и описательная статистика итогового распределения использованы для построения сценариев оценки эффективности ИТ-проекта (*табл. 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

Таблица 3.

Сценарии оценки эффективности ИТ-проекта

Сценарии	Обозн.	Объемы поступления платежей за 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.*

Таблица 4.

Показатели эффективности ИТ-проекта по сценариям

Показатели эффективности	Обозначения	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

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}.

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).

Выводы

Выполнен анализ предметной области, с точки зрения оценки эффективности СЗИ. При этом показано, что объективной характеристикой качества СЗИ – степенью ее приспособленности к достижению требуемого уровня безопасности в условиях реального воздействия случайных факторов, может служить только вероятность достижения цели операции, выполнения задачи системой или иное.

Обоснована возможность получения необходимых данных для оценки эффективности мероприятий по повышению ИБ компании с помощью имитационного моделирования. Предложена методика расчета для оценки результата от воздействия проведенных мероприятий по ИБ, представленная 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 в принципе 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. ■

Литература

1. Андреев К. Метод оценки экономической эффективности подразделения по защите информации // Информационная безопасность. 2010. № 5. [Электронный ресурс]: http://www.itsec.ru/articles2/Oborandteh/metod-ocenki-ekonomicheskoi-effektivnosti-podrazdeleniya-po-zashite-informacii (дата обращения 27.12.2014).
2. Баутов А. Эффективность защиты информации // Открытые системы. 2003.№ 07-08. [Электронный ресурс]: http://www.osp.ru/os/2003/07-08/183282/ (дата обращения 27.12.2014).

3. Горбунов А., Чуменко В. Выбор рациональной структуры средств защиты информации в АСУ. [Электронный ресурс]: http://kiev-security.org.ua/box/2/26.shtml (дата обращения 27.12.2014).
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. /Рост. гос. эконом. ун-т (РИНХ). Ростов н/Д: 2011. Вып. 14. С. 68–75.
6. Ефимов Е.Н., Лапицкая Г.М. Информационная безопасность и бизнес-процессы компании // Известия ЮФУ. Технические науки. Информационная безопасность. 2013. № 12. С 253–260.
7. Крепков И.М., Ефимов Е.Н., Фоменко Н.М. Анализ и учет рисков продвижения Интернет-проектов предприятия // Вестник МЭИ. 2010. № 2. С. 101–107.
8. Петухов Г. Основы теории эффективности целенаправленных процессов. Часть 1. Методология, методы, модели. М.: МО СССР, 1989.
9. Петухов Г.Б., Якунин В.И. Методологические основы внешнего проектирования целенаправленных процессов и целеустремленных систем. М.: АСТ, 2006.
10. 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.

EVALUATION OF INFORMATION SECURITY EFFECTIVENESS MEASURES UNDER UNCERTAINTY

Evgeny EFIMOV
Professor, Department of Information Technologies and Information Protection,
Faculty of Computer Technologies and Information Security,
Rostov State Economic University (RINE)
Address: 69, Bolshaya Sadovaya Street, Rostov-on-Don, 344002, Russian Federation
E-mail: efimov46@mail.ru

Galina LAPITSKAYA
Professor, Department of Information Technologies and Information Protection,
Faculty of Computer Technologies and Information Security,
Rostov State Economic University (RINE)
Address: 69, Bolshaya Sadovaya Street, Rostov-on-Don, 344002, Russian Federation
E-mail: gmlapickaya@mail.ru

Uncertainty of information security system properties is inherent at all stages of its life cycle due to real exposure to random factors of external and internal environment. As a project is implemented, the system uncertainty tends to reduce, but its operation efficiency can never be adequately expressed and described by deterministic parameters. In this case probabilistic methods are most applicable to evaluate efficiency of implementation and operation of information security systems. In accordance with these methods, levels of system safeguards are transformed into confidence levels of corresponding estimates. Under these conditions, data to evaluate effectiveness of information security enhancement measures can be obtained by using simulation modeling.

A suggested methodology for information security impact assessment at a company implies modeling of estimates of losses avoided. The value of losses avoided can be calculated on the basis of the likelihood of an information

security incident and resulting possible economic losses before and after implementation of information security measures at an object.

Total losses avoided resulting from the simulation covering all information security incidents enable to specify and to carry out scenario-based calculations of potential effects of such measures. The final evaluation of information security enhancement measures can be performed by any known method. Globally a standard method of cost-benefit analysis (CBA) is widely used to evaluate effectiveness of IT projects. Implementation of the suggested information security enhancements evaluation methodology has been based on the CBA method.

The main advantage of the proposed information security enhancements evaluation methodology is its ability to pay due regard to the real world uncertainty thanks to simulation modeling. This enables to some extent to increase the validity of evaluation estimates.

Key words: information security, effectiveness, modeling, losses prevented.

Citation: Efimov E.N., Lapitskaya G.M. (2015) Ocenka jeffektivnosti meroprijatij informacionnoj bezopasnosti v uslovijah neopredelennosti [Evaluation of the effectiveness of information security in conditions of uncertainty]. *Business Informatics*, no. 1 (31), pp. 51–57 (in Russian).

References

1. Andreev K. (2010) Metod ocenki jekonomicheskoj jeffektivnosti podrazdelenija po zashhite informacii [A method of evaluation of economic performance of an information security division]. *Information Security* (electronic journal). Available at: http://www.itsec.ru/articles2/Oborandteh/metod-ocenki-ekonomicheskoi-effektivnosti-podrazdeleniya-po-zashite-informacii (accessed 27 December 2014). (in Russian)
2. Bautov A. (2003) Jeffektivnost' zashhity informacii [The effectiveness of information security]. *Open Systems* (electronic journal), no. 07-08. Available at: http://www.osp.ru/os/2003/07-08/183282/ (accessed 27 December 2014). (in Russian)
3. Gorbunov A., Chumenko V. *Vybor racional'noj struktury sredstv zashhity informacii v ASU* [Selection of the rational structure of information protection instruments in information systems]. Available at: http://kiev-security.org.ua/box/2/26.shtml (accessed 27 December 2014). (in Russian)
4. Denisov M., Dolzhenko A., Efimov E. (2012) Kognitivnoe modelirovanie ocenki jeffektivnosti jelektronnyh biznes–otnoshenij predprijatija [Cognitive modeling evaluation of the effectiveness of electronic business relations company]. *Bulletin of the Rostov State Economic University*, no. 1 (37), pp. 83–90. (in Russian)
5. Efimov E. (2011) Ocenka jeffektivnosti jelektronnyh biznes-otnoshenij predprijatija [Assessment of the effectiveness of electronic business relations company]. *Problems of Federal and Regional Economy: Scientific Notes of Rostov State Economic University*, no. 14, pp. 68–75. (in Russian)
6. Efimov E., Lapickaja G. (2013) Informacionnaja bezopasnost' i biznes-processy kompanii [Information security and business processes of the company]. *Proceedings of South Federal University. Technical Science. Information Security*, no. 12, pp. 253–260. (in Russian)
7. Krepkov I., Efimov E., Fomenko N. (2010) Analiz i uchet riskov prodvizhenija Internet-proektov predprijatija (2010) [Analysis and risk-based promotion of Internet projects]. *Bulletin of Moscow Power Engineering Institute*, no. 2, pp. 101–107. (in Russian)
8. Petuhov G. (1989) *Osnovy teorii jeffektivnosti celenapravlennyh processov. Chast' 1. Metodologija, metody, modeli.* [Fundamentals of the theory of the effectiveness of targeted processes. Part 1. Methodology, methods, models]. Moscow: The USSR Ministry of Defence. (in Russian)
9. Petuhov G. (2006) *Metodologicheskie osnovy vneshnego proektirovanija celenapravlennyh processov i celeustremlennyh sistem* [Methodological basis of the external design of targeted processes and dedicated systems]. Moscow: AST. (in Russian)
10. Hubaev G. (2008) Processno-statisticheskij podhod k uchetu zatrat resursov pri ocenke (kal'kuljacii) sebestoimosti produkcii i uslug: osobennosti realizacii, preimushhestva. [Process-statistical approach to cost accounting resources assessment (costing) cost of products and services: implementation peculiarities, advantages]. *Problems of Economics*, no. 2, pp. 158–166. (in Russian)