УДК 004.94

И.И. Лившиц

КОНЦЕПЦИЯ ОЦЕНКИ УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕРВИС-ПРОВАЙДЕРОВ ИНФОРМАЦИОННЫХ СИСТЕМ ДЛЯ ПРОМЫШЛЕННЫХ ОБЪЕКТОВ

Лившиц И.И. **Концепция оценки уровня информационной безопасности сервис-провайдеров информационных систем для промышленных объектов.**
Аннотация. В настоящее время для информационных систем (ИС) наблюдается значительное количество критичных угроз, что обусловлено появлением новых векторов атак, а также недостатками при управлении рисками. Соответственно, представляет определенный интерес изучение проблемы оценки компетенции ИБ при сопровождении ИС на уровне сервис-провайдеров. В предлагаемой работе предложена формулировка «Парадокса ИБ», которые позволяет учесть наиболее значимые (критичные) угрозы ИБ и предложить подход, основанный на использовании современных риск-ориентированных стандартов, прежде всего международных стандартах ISO. Предложенная концепция оценки уровня ИБ сервис-провайдеров ИС для промышленных объектов состоит из 2-х базовых принципов и нескольких расширений, которые позволяют учесть конкретные требования по ИБ с учетом специфики функционирования ИС и предоставляют возможность оценки (качественно или количественно) в рамках плановых проверок (аудитов).
Ключевые слова: информационная система (ИС), информационная безопасность (ИБ), стандарт, сервис, система менеджмента информационной безопасности (СМИБ), статистика, корреляция.

Livshits I.I., **The concept of assessing the IT service providers information security level for industrial facilities**
Abstract. The information systems (IS) observed a significant amount of critical threats that caused the emergence of new attack vectors, as well as deficiencies in risk management. Respectively, is of particular interest to study the problem of information security competence assessment accompanying the IP level service providers.
In this issue proposes the "IT-Security Paradox" wording, which allows to consider the most important (critical) IT-Security threats and propose an approach based on the modern risk-based standards implementation, especially international standards ISO. The proposed concept of assessing the level of IT service providers information security for industrial facilities consists of 2 basic principles and a few extensions that allow to take into account the specific requirements for the IT-security specific functioning of IS and provide an opportunity to assess (qualitatively or quantitatively) as part of routine inspections (audits).
Keywords: information system (system), IT-security, standard, service, IT-security management system (ISMS), statistics, correlation.

1. Введение. Ряд современных публикаций обращен к вопросу применимости различных систем менеджмента для поддержки принятия решений высшего руководства, и, как логичное следствие – обеспечение роста бизнеса данной организации [8–9]. В частности, достаточное внимание уделено вопросам обеспечения безопасности, надежности и доступности бизнес-процессов, что, очевидно, невозможно обеспечить без реализации комплекса мероприятий в

отношении информационных систем (ИС). Более того, проблема обеспечения комплексной безопасности промышленных объектов непосредственным образом зависит от уровня безопасности, в том числе, информационной безопасности (ИБ), в отношении действующих ИС. Под термином «*информационная система*» предлагается понимать термин «*система (system)*» как комбинация взаимодействующих элементов, организованных для достижения одной или нескольких поставленных целей (п. 4.17 стандарта ГОСТ Р ИСО/МЭК 15288-2005).

В настоящее время, объективно, для ИС достаточно стабильно проявляется значительное количество значимых (критичных) угроз, что обусловлено появлением новых векторов атак («*таргетированные атаки*»), а также недостаточной проработкой и управлением рисками в отношении ранее известных угроз и уязвимостей. Соответственно, представляет определенный интерес изучение проблемы безопасности ИС не только на фазе эксплуатации уже у конечного потребителя (на промышленном объекте), но и обращение внимания к «культуре производства» поставщиков (сервис-провайдеров) ИС, на их компетенции – методическое обеспечение, наличие и уровень внедрения стандартов и методик (применимых для целей создания и обеспечения уровня ИБ при сопровождении ИС).

2. Общая постановка задачи. Как отмечалось выше, процесс оценки ИС, уже применяемых на промышленных объектах, достаточно хорошо специфицирован, кроме того, в дополнение к мерам ИБ, предпринимаемых на объектах, рекомендуется выполнение комплекса специальных мер (сертификация, аттестация и пр.), находящихся в компетенции уполномоченных государственных органов (например, ФСТЭК или ФСБ). Как правило, ряд известных ИС имеют официальные сертификаты, размещенные на публичных сайтах разработчиков и/или системных интеграторов.

Но остается открытым вопрос о существующих мерах контроля ИБ, о достаточности таких мер, об оценке их эффективности и достаточности на всем жизненном цикле ИС – с момента создания, испытания, ввода в действие, эксплуатации, сопровождения и вывода из эксплуатации. Известно, что термин «жизненный цикл системы» («*system life cycle*») определяется как развитие рассматриваемой ИС во времени, начиная от замысла и заканчивая списанием. (п. 4.20 стандарта ГОСТ Р ИСО/МЭК 15288-2005). Соответственно, определенное «формальное соответствия» конкретным требования определенного «регулятора» (ФСТЭК и/или

ФСБ) может быть проверено и результаты его – официально опубликованы. Но вопросы «культуры производства», приверженности определенным методикам, применение набора «лучших практик» и стандартов ИБ – на стороне поставщика ИС (сервис-провайдера) – являются, объективно, не менее важными и оценка их на основании общей методики представляется своевременной и практически востребованной.

В качестве примера, подтверждающего важность качества работы «сервисной» компоненты при сопровождении важной (критичной) ИС со стороны сервис-провайдера, рассмотрим пример одного опроса Cnews «*Что вызывает ваше раздражение при контакте с сервисной службой*?». Опрос касался только конечных пользователей, при этом из общего перечня выделены только вопросы, касающиеся темы данной публикации и наиболее ярко отражающие поставленную проблему (допускалось отвечать на несколько вариантов сразу):

– длительное время ожидания – 74 %;

– много переключений между сотрудниками для решения – 42 %;

– недостаточная компетенция оператора при ответе – 38 %;

– низкий уровень ответственности оператора для решения – 27 %;

– отключения оператора для консультаций – 13 %.

Другим достаточно ярким примером является инцидент прерывания обслуживания международных платежных систем (МПС) в марте 2014 г. – Visa и MasterCard прекратили обслуживание ряда российских банков. Логичной реакцией на этот инцидент стала законодательная инициатива в форме ФЗ-112 о создании Национальной системы платежных карт и обеспечении бесперебойности работы МПС с целью поддержания бесперебойности денежных переводов и гарантии их безопасности [6]. Для целей данной публикации важно, что в [6] определены ключевые требования, в том числе и по «триаде ИБ» – (конфиденциальности, целостности и доступности). Дополнительно должен быть принят во внимание комплекс угроз касательно возможности приостановления технической поддержки со стороны крупнейших зарубежных ИТ-поставщиков (Oracle, HP и IBM). На уровне Банка России эта угроза получила подтверждение (например, возможность отзыва лицензий на ПО), как отметил заместитель начальника главного управления

безопасности и защиты информации ЦБ Артем Сычев [7]. По данным ряда экспертов, доля зарубежного ПО в российских банках высока – в Сбербанке она составляет примерно 50%, в ВТБ – до 40%, в Промсвязьбанке около 30% [7]. Таким образом, реальные примеры текущей деятельности ряда крупнейших организаций только подчеркивают особое внимание, которое требуется уделять «качеству работы» и компетенциям сервис-провайдеров.

Предпринятое исследование ставит следующую задачу – рассмотреть на основе опубликованных рейтингов крупнейших сервис-провайдеров и известных стандартов ИБ, возможные оценки качества предоставляемых услуг, оценить уровень приверженности международных стандартов и «лучших практик» ИБ и сформировать концепцию оценки уровня ИБ сервис-провайдеров ИС для промышленных объектов.

3. Анализ исходных данных. В качестве исходных данных рассмотрены обзоры CNews Analytics [1–5], в которых приведены общие данные о рейтингах и результатах деятельности ИТ-компаний в России, а также публичные данные о применяемых в процессе основной деятельности стандартах, методиках и «лучших практиках». Из общего массива данных (рейтинг «Крупнейшие ИТ-компании России 2013» включал данные 100 ИТ-компаний [1]), были отобраны только ключевые сервис-провайдеры, т.е. те компании, в поле «Сфера деятельности» которых указано точно «ИТ-услуги» – таких компаний 51 (таким образом, выбыли из анализа те компании, которые имели специализацию по дистрибуции, разработке ПО и интеграции).

Как показало исследование CNews [4], опрошенные провайдеры опираются в своей деятельности на методики ITIL/ITSM, COBIT, MOF, активно используются стандарты ISO 20000, 27001, 9000 и также различные ГОСТ – серии 34, серии 19 и пр. Дополнительно был изучен рейтинг («Подходы к стандартизации ИТ-сервиса в России 2014» [5]), которые включал данные всего по 9 крупнейшим сервис-провайдерам в России («Ай-теко», «АйТи», «Астерос», «Аутсорсинг 24», «Гелиос ИТ», Maykor, «Оптима», «Техносерв» и «ЮНИТ-Оргтехника»). Примечание – ряд организаций, традиционно предоставлявших данные для рейтинга CNews100, отказались участвовать в анализе 2013 г., что, вероятно, подразумевает отрицательные результаты деятельности. Это предположение подтверждается фактами участия в более ранних рейтингах (например, для компании «Аутосорсинг 24» и «Optima»).

Соответственно, итоги сопоставления сервис-провайдеров, включенных в рейтинги [1 – 4] за 2013 г., представлены в таблице 1.

Таблица 1. Рейтинги сервис-провайдеров 2013 г., обработка

Место 2013	Место 2012	Компания	Город	Выручка 2013	Выручка 2012	Рост
3	4	Техносерв	Москва	40.161.571	43.117.193	-6.9 %
10	12	Ай-Теко	Москва	22.662.179	21.495.000	5 %
15	13	Астерос	Москва	19.731.474	19.156.771	3 %
26	25	Maykor	Москва	9.275.729	8.014.110	15.7%
28	28	АйТи	Москва	7.700.000	7.050.000	9.2 %
67	-	Юнит	Екатеринбург	1.534.306	1.461.244	5 %

Соответственно, итоги сопоставления сервис-провайдеров, включенных в рейтинги [2 – 4] за 2012 г., представлены в таблице 2.

Таблица 2. Рейтинги сервис-провайдеров 2012 г., обработка

Место 2012	Место 2011	Компания	Город	Выручка 2012	Выручка 2011	Рост
4	5	Техносерв	Москва	43.117.192	40.334.137	6,9 %
12	15	Ай-Теко	Москва	21.495.000	16.900.000	27,2 %
13	14	Астерос	Москва	19.156.770	17.258.352	11%
25	-	Maykor	Москва	8.014.113	4.273.571	87,5 %
28	30	АйТи	Москва	7.050.000	6.180.000	14,1 %
82	77	Аутсорсинг 24	Москва	1.019.961	914.731	11,5 %

Соответственно, итоги сопоставления сервис-провайдеров, включенных в рейтинги [3, 4] за 2011 г., представлены в таблице 3.

Таблица 3. Рейтинги сервис-провайдеров 2011 г., обработка

Место 2011	Место 2010	Компания	Город	Выручка 2012	Выручка 2011	Рост
5	6	Техносерв	Москва	39.277.591	33.517.571	17,2 %
14	18	Астерос	Москва	17.258.352	11.179.840	54,4 %
15	17	Ай-Теко	Москва	16.900.000	12.510.000	35 %
21	19	Optima	Москва	12.041.966	11.093.876	8,5 %
30	31	АйТи	Москва	6.180.000	4.692.560	31,7 %
77	83	Аутсорсинг 24	Москва	914.732	732.740	24,8%

Далее рассмотрим кратко финансовые итоги за тот же сравнительный период – 2012 и 2013 гг. для ИТ-компаний (совокупно) [1]. Отмечается, что выручка составила 918 млрд. руб. против 919 млрд. руб. годом ранее, но при анализе динамики выручки «первой десятки» рейтинга CNews100 фиксируется снижение (с 55,3% до 51%) против остальных компаний рейтинга, соответственно, отмечается увеличение с 44,7% до 49%.

Итоги сопоставления сервис-провайдеров, включенных в оба рейтинга [1, 5], в части, касающейся заявленных имеющихся компетенций (соответствия требованиям стандартов, применения методик, использования ГОСТов и пр.) представлены в таблице 4.

Таблица 4. Компетенции сервис-провайдеров, обработка

Компания	Заявленные компетенции (стандарты и методики)						Баллы
	ITIL v3	Cobit	9001	20000	27001	ГОСТ	
Техносерв	да		да	да			3
Ай-Теко	да		да	да	да		4
Астерос	да		да			да	3
Maykor	да		да	да			3
АйТи	да	да	да	да			4
Юнит	да		да	да	да		4
Аутсорсинг 24	да		да	да	да	да	5
Optima	да		да				2

Итоговая оценка «Баллы» определялась по правилу наличия какой-либо компетенции у определенной организации, и, в этом случае, начислялся 1 балл. Примечание – по данным обзора [5] все указанные компетенции были заявлены как внедренные (применимые, разработанные или активно используемые) с 2011 г., таким образом, дальнейшее исследование зависимостей вполне обоснованно может опираться на сопоставление данных за последние 3 года – с 2011 по 2013 гг.

4. Исследование зависимостей. Соответственно, в таблице 5 представлены сводные данные по оценке зависимостей сервис-провайдеров за последние 3 года (2011 – 2013 гг.) и заявленные компетенции (предоставлены оценки в баллах).

Важно обратить внимание, что в сводной таблице предпринята попытка «выравнивания» сервис-провайдеров, вошедших в рейтинг [5], но, по ряду причин, не вошедших в рейтинги (во все или частично) – [1, 2, 3]. Соответственно, предложено определять место

компаний, не вошедших в официальный рейтинг «первой сотни», как рейтинг «101», и рост выручки определять как «0». Таким образом, все компании, включенные в рейтинг [5] сервис-провайдеров, имеют сопоставимые баллы, места в рейтинге и оценки роста выручки, что позволяет выполнять оценки корреляции.

Таблица 5. Сводная оценка сервис-провайдеров, обработка

Компания	Баллы	Рост выручки			Место в рейтинге		
		2013	2012	2011	2013	2012	2011
Техносерв	3	-6,90%	6,90%	17,20%	3	4	5
Ай-Теко	4	5,00%	5,00%	35,00%	10	12	15
Астерос	3	3,00%	3,00%	54,40%	15	13	13
Maykor	3	15,70%	15.7%	0,00%	26	25	14
АйТи	4	9,20%	9.2 %	31,70%	28	28	30
Юнит	4	5,00%	5,00%	0,00%	67	101	101
Аутсорсинг 24	5	0,00%	0,00%	24,80%	101	82	77
Optima	2	0,00%	0,00%	8,50%	101	101	21

Результаты исследований сводных данных по оценке сервис-провайдеров за последние 3 года (2011 – 2013 гг.) и заявленных компетенций предоставлены на рисунке 1. Анализ полученных результатов исследований будет представлен далее по тексту.

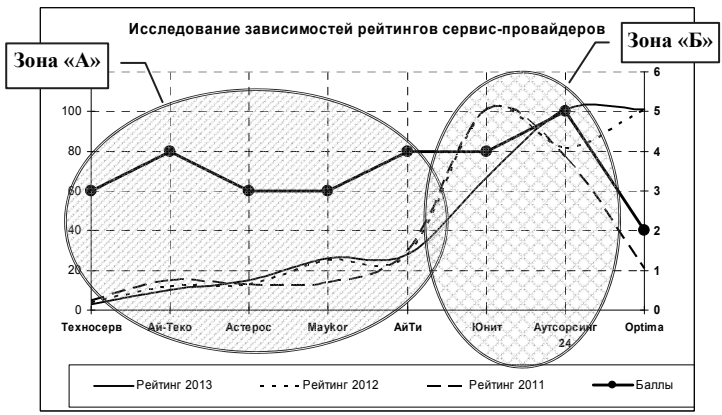

Рис. 1. Исследование зависимостей рейтингов сервис-провайдеров

В соответствии с поставленной проблемой в данной публикации – «как можно оценить уровень ИБ сервис-провайдеров»

при выполнении сопровождения ИС промышленных объектов на основе собственных компетенций?», представляется интересным задать ряд вопросов для изучения возможных зависимостей между имеющимися собственными компетенциями сервис-провайдерами (из первой «сотни» в рейтинге России) и их позицией (в т.ч. в динамике – по росту выручки, по изменению места в рейтинге). Таких вопросов предполагается задать три:

– *Оценка корреляции "Рост выручки и влияние компетенций".*

– *Оценка корреляции "Место в рейтинге и влияние компетенций".*

– *Оценка корреляции "Рост выручки и изменение рейтинга".*

При дальнейших исследованиях возможных зависимостей исходных обработанных данных (таблица 1 – таблица 4) будет применен математический аппарат, изложенный ранее в работе [10], там же можно ознакомиться с рядом примеров вычислений по аналогичному направлению (исследование корреляционных зависимостей стандартизации ISO). Ответы на поставленные вопросы возможно получить с помощью применения корреляционных функций, результаты представлены в таблице 6.

Таблица 6. Результаты оценки корреляции

Исследование оценки корреляции	2013	2012	2011
«Рост выручки и влияние компетенций»	0,0848	0,0033	0,1799
«Место в рейтинге и влияние компетенций	0,1172	0,0779	0,6220
«Рост выручки и изменение рейтинга»	0,1352	0,6239	0,4439

Результаты исследований корреляции оценок рейтингов сервис-провайдеров за последние 3 года (2011 – 2013 гг.) и заявленных компетенций предоставлены на рисунке 2. Анализ полученных результатов исследований будет представлен далее по тексту.

5. Анализ результатов исследований. Анализ результатов исследований зависимостей рейтингов сервис-провайдеров (представлена сводная оценка сервис-провайдеров – таблица 5 и результаты исследований зависимостей рейтингов сервис-провайдеров – рисунок 1) приводят к следующему важному заключению:

– *Фактор только наличия большого количества собственных компетенций (свыше 4-х баллов) не приводит автоматически к высокому месту в рейтингах (2011 – 2013 гг.) и не влияет явным образом на рост выручки («Зона Б» - компании «Юнит», «Аутсорсинг*

24»), но наличие минимального «порогового значения» собственных компетенций (не менее 3-х баллов) приводит к высокому месту во всех рейтингах (2011-2013 гг.) и влияет явным образом на рост выручки («Зона А» - компании «Техносерв», «Астерос», «Ай-Теко», «АйТи», «Maykor»).

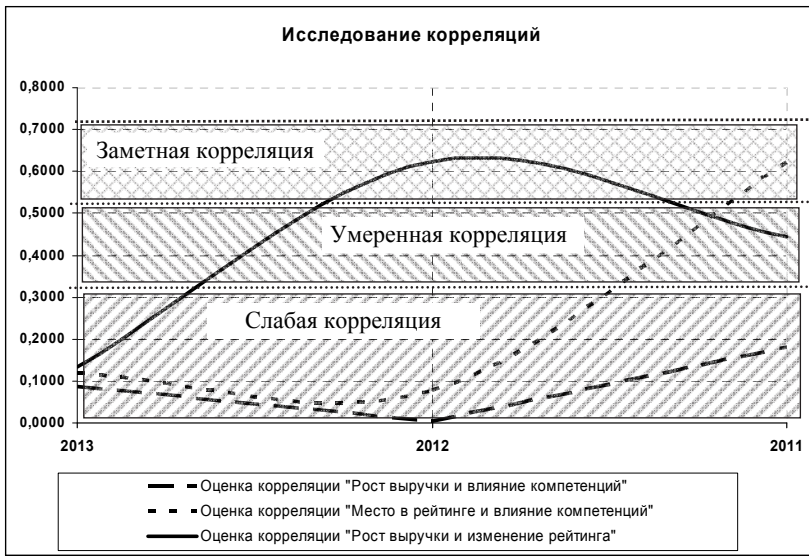

Рис. 2. Исследование корреляций компетенций сервис-провайдеров

Анализ результатов исследований корреляций компетенций сервис-провайдеров (представлены результаты оценок корреляции сервис-провайдеров – таблица 6 и результаты исследований корреляции компетенций сервис-провайдеров – рисунок 2) приводят к следующим важным заключениям:

– *Оценка корреляции "Рост выручки и влияние компетенций" – слабая во всем диапазоне исследований (по шкале Чеддока, менее 0,3), что свидетельствует о минимальной роли набора собственных компетенций (стандартов, методик, «лучших практик») при оценке влияния на увеличение выручки всех компаний, вошедших в рейтинг;*

– *Оценка корреляции "Место в рейтинге и влияние компетенций" – подвержена значительному изменению: от заметной в 2011 г. (по шкале Чеддока, свыше 0,5), до слабой (по шкале Чеддока, менее 0,3) в 2012 и 2013 гг. Вероятно, эта корреляция является ложной, т.к. компетенции сервис-провайдеры к 2011 г. уже обладали,*

но на рост выручки и место в рейтинге этот фактор имеет слабое влияние, что также подтверждается для «Зоны А» на рисунке 1.

– Оценка корреляции "Рост выручки и изменение рейтинга" – подвержена значительному изменению: от умеренной в 2011 г. (по шкале Чеддока свыше 0,3 и менее 0,5), до заметной в 2012 г. (по шкале Чеддока, свыше 0,5) и до слабой в 2013 (по шкале Чеддока, менее 0,3). Эта корреляция дает достаточные основания предполагать, что основное влияние на рост выручки с течением времени оказываю разные факторы, особенно в условиях нулевого роста всего ИТ-рынка.

Общая тенденция – с учетом данных таблиц 5 и 6 может быть кратко сформулирована так: на основе имеющейся статистики за 2011 – 2013 гг. явная и стабильная во времени корреляционная зависимость между собственными компетенциями сервис-провайдеров в области ИБ и достижениями коммерческих результатов в росте выручки или в рейтингах не прослеживается. Весьма вероятно, отсутствие корреляции может быть связано с другими причинами и носит, объективно, скрытый и системный характер.

6. Парадокс ИБ. С учетом фактов, отражающих возрастание угроз ИБ и использования уязвимостей современных ИС, серьезных сбоев критичных ИС и их компонент (как было отмечено выше), а также требований, содержащихся в применяемых стандартах и доступных методиках, возможно предложить формулировку «*Парадокса ИБ*»: на современном этапе развития ИС наиболее значимые (критичные) угрозы жизненного цикла ИС являются прямым следствием доминирования зарубежных компонент в программном и аппаратном обеспечении ИС, и, в то же время, механизм эффективного противодействия данным угрозам содержится в доступных международных стандартах, прежде всего, в современных риск-ориентированных стандартах ISO.

Ранее были рассмотрены примеры проявления данного парадокса – на проекте НПС, еще раз отметим, что системы Visa и/или MasterCard имеют всю критичную базовую техническую инфраструктуру и процессинг вне зоны разумного контроля в РФ, т.е., объективно, в любой момент возможны прерывания доступности и ощутимые финансовые издержки кредитным организациям РФ. В более широком аспекте – на фазе сопровождения и эксплуатации любых ИС в РФ роль сервис-провайдера (даже при наличии максимального количества компетенций ИБ) не может полностью парировать все риски ИБ, т.к. значительная часть ПО является иностранной (по данным экспертов [7] доля ПО иностранной разработки составляет до 50 %). А этот риск очень серьезный, т.к. ряд

зарубежных производителей ПО (например, Microsoft, Oracle, Symantec и Hewlett-Packard), были готовы присоединиться к техническим санкциям в отношении ряда российских банков в апреле 2014 г. [7, 11].

В этой ситуации роль сервис-провайдера в аспекте гарантированного обеспечения требуемого уровня ИБ для ИС, принятых на сопровождение, должна объективно измениться – что логично приведет к повышению объема доходов и, следовательно, рыночной доли по сравнению с конкурентами. На данный момент, как показало проведенное исследование за 3 года, наблюдается стабильное крайне низкая корреляция между имеющимися компетенциями сервис-провайдеров и ростом их выручки, соответственно, есть потенциал развития в новой области сопровождения критичных ИС с дополнительными функциями обеспечения ИБ.

В качестве нормативной и методической поддержки можно рекомендовать тот же перечень стандартов, которые, как заявлено, применяются сервис-провайдерами – это ряд международных стандартов (например, ISO серии 9001, 20000 и 27001), которые приняты в РФ в качестве национальных ГОСТ Р, соответственно, могут и должны (наряду с внутренними мерами защиты, системами сертификации средств защиты по требованиям ФСТЭК и/или ФСБ), применяться для результативного обеспечения требуемого уровня ИБ и парирования негативного воздействия в рамках «Парадокса ИБ» на критичные ИС. Однако имеется объективный фактор, значительно усиливающий «*Парадокс ИБ*» – многие организации, прежде всего государственные, не спешат с «принятием на вооружение» и не практикуют широкое применение новых стандартов ISO, хотя бы и в виде «локализованных» ГОСТ Р ИСО, предпочитая опираться на систему руководящих документов ФСТЭК, ряд которых утвержден еще в 1992 г.

7. Пример решения «Парадокса ИБ». В качестве примера одного из вариантов практического решения «Парадокса ИБ» рассмотрим основные международные стандарты в области ИБ – ISO/IEC 27001:2013 (в РФ принят ГОСТ Р ИСО/МЭК 27001-2006) и ISO/IEC 20000:1-2011 (в РФ принят ГОСТ Р ИСО/МЭК 20000:1-2011) и покажем, какие меры и средства ИБ необходимо применять для обеспечения должного уровня ИБ для действующих ИС (таблица 7). Соответственно, требования рассмотрены только по пунктам стандартов, без анализа применения конкретных и соответствующих мер (средств) обеспечения ИБ, т.к. модель рисков ИБ не формализована.

Таблица 7. Применение стандартов ISO для обеспечения ИБ в ИС

Компонент ИБ	Требования стандартов		Пример
	ISO/IEC 27001: 2013	ISO/IEC 20000: 1-2011	
Определение контекста	4.1	-	Перечень зарубежных поставщиков компонент критичных ИС. Дополнительно – перечень аналогов (производства «доверенных» стран)
Планирование поддержки и развития ИС	-	4.5.2	План создания, внедрения и поддержки ИС (с учетом законодательства, ограничений по привлечению третьих лиц, аутсорсинга в ИБ)
Потребности заинтересованных сторон	4.2	4.1.1 d)	Перечень требований поставщиков компонент критичных ИС в части ИБ. Дополнительно – перечень аналогов (производства «доверенных» стран)
Политика ИБ	5.2 c)	4.1.2 b)	Декларирование обязательств поставщиков компонент критичных ИС в части ИБ
Оценка рисков ИБ	6.1.2	6.6.2 d)	Реестр рисков (идентификация, анализ, оценка, сравнение с критериями) в части компонент ИС
Обработка рисков ИБ	6.1.3	6.6.3	Решение о приемлемом варианте обработки рисков (меры обеспечения ИБ, формирование плана, согласование с владельцем риска) в части компонент ИС
Компетенция	7.2. a)	4.4.2 a)	Определение необходимой компетенции персонала в части, касающейся ИБ и ИС
Коммуникация	7.4	4.1.3 b)	Процесс коммуникации в рамках обеспечения ИБ для компонент ИС
Операционное планирование и контроль	8.1	4.2	План контроля процессов аутсорсинга в части касающейся ИБ и ИС
Внутренний аудит ИБ	9.2 f)	4.5.4.2 b)	Процесс информирования высшего руководства в части касающейся ИБ и ИС. Дополнительно – привлечение внешних аудиторов в рамках аудитов 2-й стороной.
Анализ со стороны руководства	9.3 d)	4.5.4.3 c)	Обеспечение обратной связи от поставщиков компонент критичных ИС
Управление несоответствиями	10.1 b)	4.5.4.2	Предпринятые действия для устранения причин выявленных несоответствий ИБ. Дополнительно – привлечение внешних аудиторов в рамках аудитов 2-й стороной и/или экспертов (ФСБ и/или ФСТЭК)

На основании данных [4, 5] можно констатировать, что крупнейшие сервисные провайдеры прекрасно отдают себе отчет в важности применения нормативных требований в части ИБ – как на уровне ГОСТ, так и на уровне соответствия современных риск-ориентированных стандартов ISO. К сожалению, такой подход приносит свои «плюсы» только фрагментарно – в отношении уже созданных (закупленных) и развернутых «в продуктиве» реальных ИС; но совершенно не обеспечивается контроль всех стадий ЖЦ для ИС (например, обеспечение ИБ в стадии сопровождения), соответственно, в критических ситуациях пользователи ИС могут оказаться в уязвимом положении и вынуждены постоянно обновлять «патчи» безопасности и внедрять дорогостоящие эшелонированные системы ИБ.

8. Концепция оценки уровня ИБ сервис-провайдеров. На основании приведенных выше фактов актуальных угроз, краткого анализа нормативно-технических документов, оценки влияния компетенций ИБ сервис-провайдеров и предложенного «*Парадокса ИБ*», представляется возможным сформировать концепцию оценки уровня ИБ сервис-провайдеров ИС для промышленных объектов. Концепция состоит из 2-х базовых принципов и нескольких расширений (которые могут отражать конкретные требования по специализации при обслуживании государственных, отраслевых и иных заказчиков).

1. Базовый минимальный принцип – сервис-провайдер должен реализовать в своей деятельности систему управления, основанную на международных стандартах (или аналогичных ГОСТ Р), минимально достаточных для построения СМИБ и обеспечения требуемого комплекса мер и средств ИБ, адекватно выявленным, оцененным и ранжированным рискам ИБ. Этот принцип может быть оценен (качественно или количественно) в рамках плановых аудитов СМИБ.

2. Базовый достаточный принцип – сервис-провайдер должен реализовать в своей системе управления комплекс международных стандартов (или аналогичных ГОСТ Р), достаточных для оказания услуг на согласованном уровне качества, с учетом определенных рисков ИБ и с учетом дополнительных требований заинтересованных сторон. Рекомендуется создание интегрированной системы менеджмента, в рамках аудитов которой реализация этого принципа может быть оценена (качественно или количественно).

3. Расширенный принцип «Государственного регулирования» – сервис-провайдер должен реализовать в своей системе управления комплекс требований, установленных регуляторами (ФСБ, ФСТЭК,

МО, СВР, МЧС и пр.), с учетом специфики ИБ при функционировании ИС, требований к их доступности и надежности, требований к аттестации и пр. Этот принцип может быть оценен (качественно или количественно) в рамках плановых проверок лицензиатов (аттестаций) со стороны регуляторов.

4. Расширенный принцип «Отраслевого регулирования» – сервис-провайдер должен реализовать в своей системе управления комплекс требований, установленных в отрасли (ЦБ, ГОСТ РВ 0015-002-2012, ISAGO и пр.), с учетом специфики ИБ при функционировании ИС, требований к их доступности и надежности, требований к периодичности проверок («аудиты второй стороной» и пр. Этот принцип может быть оценен (качественно или количественно) в рамках плановых проверок лицензиатов со стороны независимых аудиторов.

5. Расширенный принцип «Лучших практик» – сервис-провайдер должен реализовать в своей системе управления комплекс «лучших практик», принятых в отрасли (ITIL, Cobit, SOX, Basel, COSO и пр.), с учетом специфики функционирования ИС, требований к их доступности и надежности, требований к периодичности проверок и пр. Этот принцип может быть оценен (качественно или количественно) в рамках плановых проверок на добровольной основе со стороны независимых аудиторов.

К представленной концепции можно дать хороший пример. Применение лучших международных стандартов в области ИБ (ISO серии 27001, 20000, 15408 и пр.), принятых в РФ в качестве национальных ГОСТ Р, оказало влияние на систему требований в государственном оборонном заказе. В новом ГОСТ РВ 0015-002-2012 в разделе 4.3 содержатся требования к ИБ и дана прямая ссылка на «целевой» стандарт ГОСТ Р ИСО/МЭК 27001-2006. Соответственно, наблюдается логичное и обоснованное направление по включению требований по ИБ там, где это наиболее важно и критично – в области государственного оборонного заказа, т.к. требования ГОСТ РВ 0015-002-2012 там обязательны. Представляется рациональным принятие таких же требований для иных критичных отраслей экономики РФ – отрасли связи, энергетики, транспорта, добычи (транспортировки) углеводородного сырья и пр. Приоритет обязательного применения национальных стандартов в области ИБ может также определяться «*Парадоксом ИБ*» – т.е. теми угрозами, проявление которых может привести к наибольшему негативным последствиям (ущербу) на промышленных объектах.

Внесение изменений в практику экспертизы уровня защищенности, оценки соответствия и аудита в области ИБ для существующих ИС должно обязательно базироваться на действующих руководящих документах ФСТЭК и/или ФСБ. Соответственно, изменения должны касаться, помимо риск-ориентированного подхода (содержащегося в новых стандартах ISO), также и углубленного анализа моделей ЖЦ ИС, в том числе оценки уровня достаточности и контроля средств (мер) обеспечения ИБ, заложенных на стадии проектирования, создания, тестирования – т.е. до приемки ИС в «продуктив» и активной эксплуатации. В том же направлении необходимо требовать периодической оценки защищенности ИС – в рамках обязательной аттестации в соответствии с действующими руководящими документами ФСТЭК и/или ФСБ.

Предлагается распространить практику «инструментального» аудита ИБ (по аналогии с требованиями PCI DSS) на критичные ИС и сформировать национальные правила для оценки текущего состояния уровня защищенности ИБ на периодической основе. Определенно, выполнение таких аудитов (тестов) должно быть лицензируемым видом деятельности в РФ и выполняться под надзором соответствующих специальных служб – ФСТЭК и/или ФСБ.

9. Выводы:

1. Опубликованная статистика за 2011-2013 гг. не позволяет сделать вывод о наличии явной и что особенно важно – стабильной во времени зависимости между собственными компетенциями в области ИБ у сервис-провайдеров и достижениями коммерческих результатов в росте выручки или в рейтингах. Фактор наличия определенного количества собственных компетенций не приводит автоматически к высокому месту в рейтингах. Весьма вероятно, отсутствие корреляции может быть связано с другими причинами и носит, объективно, скрытый и системный характер.

2. Предложенная формулировка «*Парадокса ИБ*» на современном этапе развития ИС позволяет учесть наиболее значимые (критичные) угрозы ИБ и предложить подход, основанный на широком использовании современных риск-ориентированных стандартов, прежде всего международных стандартах ISO.

3. Предложенная концепция оценки уровня ИБ сервис-провайдеров ИС для промышленных объектов состоит из 2-х базовых принципов и нескольких расширений, которые позволяют учесть конкретные требования по специализации при обслуживании государственных, отраслевых и иных заказчиков с учетом специфики ИБ при функционировании ИС, и предоставляют возможность

оценки (качественно или количественно) в рамках плановых проверок (аудитов).

Литература

1. Крупнейшие ИТ-компании России 2013. URL: http://www.cnews.ru/reviews/new/2013/ (дата обращения 07.07.2014).
2. Крупнейшие ИТ-компании России 2012. URL: http://www.cnews.ru/reviews/new/rynok_it_itogi_2012/review_table/1d5d1838fd010e16936649555e52b4dd1655219b/ (дата обращения: 07.07.2014).
3. Крупнейшие ИТ-компании России 2011. URL: http://www.cnews.ru/reviews/free/2011/rating/rating1.shtml/ (дата обращения: 07.07.2014).
4. Стандарты ИТ-сервисов в России: готовность провайдеров. URL: http://www.cnews.ru/reviews/new/2013/articles/standarty_itservisov_v_rossii_gotovnost_provajderov/ (дата обращения: 07.07.2014).
5. Подходы к стандартизации ИТ-сервиса в России 2014. URL: http://www.cnews.ru/reviews/free/table/table1.htm (дата обращения 07.07.2014).
6. Федеральный закон от 05.05.2014 № 112-ФЗ «О внесении изменений в Федеральный закон «О национальной платежной системе» и отдельные законодательные акты Российской Федерации».
7. «Oracle и Microsoft могут прекратить поддержку попавших под санкции банков». URL: www.rbc.ru (дата обращения: 07.07.2014).
8. Лившиц И. Применение моделей СМИБ для оценки защищенности интегрированных систем менеджмента // Труды СПИИРАН. 2013. Вып. 8(31). С. 147–163.
9. Лившиц И. Подходы к решению проблемы учета потерь в интегрированных системах менеджмента // Информатизация и Связь. 2013. Вып. 1. С. 55–60.
10. Лившиц И.И., Молдовян А.А., Танатарова А.Т. Исследование зависимости сертификации по международным стандартам ISO от типов организации для ведущих отраслей промышленности // Труды СПИИРАН. 2014. Вып. 3(34). С. 160–178.
11. Лившиц И. Методическое обеспечение процесса оценки банковских продуктов в соответствии с требованиями современных стандартов ISO // Деньги и Кредит. 2014. Вып. 6. С. 75–77.

References

1. Krupnejshie IT-kompanii Rossii 2013 [Biggest Russian IT-company 2013]. Available at: http://www.cnews.ru/reviews/new/2013/ (accessed 07.07.2014). (In Russ.).
2. Krupnejshie IT-kompanii Rossii 2012 [Biggest Russian IT-company 2012]. Available at: http://www.cnews.ru/reviews/new/rynok_it_itogi_2012/review_table/1d5d1838fd010e16936649555e52b4dd1655219b/ (accessed 07.07.2014). (In Russ.).
3. Krupnejshie IT-kompanii Rossii 2011 [Biggest Russian IT-company 2011]. Available at: http://www.cnews.ru/reviews/free/2011/rating/rating1.shtml/ (accessed 07.07.2014). (In Russ.).
4. Standarty IT-servisov v Rossii: gotovnost' provajderov [IT-services standards in Russia: ready on providers]. Available at: http://www.cnews.ru/reviews/new/2013/articles/standarty_itservisov_v_rossii_gotovnost_provajderov/ (accessed 07.07.2014). (In Russ.).

5. Podhody k standartizacii IT-servisa v Rossii [IT-service approach for standardization in Russia]. Available at: http://www.cnews.ru/reviews/free/table/table1.htm (accessed 07.07.2014). (In Russ.).
6. Federal Law of 05.05.2014 № 112-FZ "On Amending the Federal Law "On the National Payment System" and Certain Legislative Acts of the Russian Federation."(In Russ.).
7. «Oracle i Microsoft mogut precratit' podderzku bankov» [«Oracle and Microsoft may discontinue support for banks which fell under sanctions»]. Available at: www.rbc.ru (accessed 07.07.2014). (In Russ.).
8. Livshits I. [Application of models of the ISMS to assess the security of Integrated Systems of Management]. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2013. vol. 8(31). pp. 147–163 (In Russ).
9. Livshits I. [Approaches to solving the problem of accounting of losses in integrated systems of management]. *Informatisatia i Svyaz – Informatization and Communication*. 2013. vol. 1. pp 55–60 (In Russ).
10. Livshits I., Moldovyan A., Tanatarova A. [Analysis of certification dependency of international standards ISO for leading industries]. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2014. vol. 3(34), pp. 160–178 (In Russ).
11. Livshits I. [Methodical provision of the evaluation process of banking products in accordance to requirements of modern standards ISO]. *Den'gi i Kredit – Money and Credit*. 2014. vol. 6. pp. 75–77.

Лившиц Илья Иосифович — к-т техн. наук, эксперт-аудитор ИТСК. Область научных интересов: системный анализ, защита информации, риск-менеджмент. Число научных публикаций — 30. Livshitz_il@Hotbox.ru; Санкт-Петербург, Богатырский пр., д. 61, к.1, кв. 17тел.: +7 812 934-48-46.

Livshitz Ilya Iosifovich — Ph.D, lead auditor, ITSC. Research interests: system analyses, IT-security, risk-management. The number of publications — 30. Livshitz_il@Hotbox.ru; 197082, Russia, St.Petersburg, Bogatirsky str. 61-1-17; phone: +7 812 934-48-46.

РЕФЕРАТ

Лившиц И.И., **Концепция оценки уровня информационной безопасности сервис-провайдеров информационных систем для промышленных объектов.**

В настоящее время, объективно, для ИС достаточно стабильно проявляется значительное количество значимых (критичных) угроз, что обусловлено появлением новых векторов атак («*таргетированные атаки*»), а также недостаточной проработкой и управлением рисками в отношении ранее известных угроз и уязвимостей. Соответственно, представляет определенный интерес изучение проблемы безопасности ИС не только на фазе эксплуатации уже у конечного потребителя (на промышленном объекте), но и обращение внимания к «культуре производства» поставщиков (сервис-провайдеров) ИС, на их компетенции – методическое обеспечение, наличие и уровень внедрения стандартов и методик (применимых для целей создания и обеспечения уровня ИБ при сопровождении ИС).

В публикации рассмотрены актуальные риски в процессе жизненного цикла создания ИС и показано влияние современных угроз на уровень ИБ. На основании приведенных фактов, анализа нормативно-технических документов (ГОСТ, ГОСТ Р, стандартов ISO), анализа рисков – предложена формулировка «Парадокса ИБ» на современном этапе развития ИС – все наиболее значимые (критичные) угрозы для ИС являются прямым следствием доминирования зарубежных компонент в программном и аппаратном обеспечении, и в то же время, механизм эффективного противодействия данным угрозам содержится в доступных международных стандартах, прежде всего, в современных риск-ориентированных стандартах ISO.

В качестве парирования негативного эффекта «Парадокса ИБ» предложены перспективные направления обеспечения ИБ для ИС, среди которых – повсеместное применение лучших международных стандартов в области ИБ; внесение изменений в практику оценки компетенций ИБ сервис-провайдеров, оценки соответствия и аудита ИБ для существующих ИС на базе действующих руководящих документов ФСТЭК и/или ФСБ; распространение практики «инструментального» аудита ИБ. На основании приведенных фактов актуальных угроз, краткого анализа нормативно-технических документов, оценки влияния компетенций ИБ сервис-провайдеров и предложенного «Парадокса ИБ», представлена концепция оценки уровня ИБ сервис-провайдеров ИС для промышленных объектов. Концепция состоит из 2-х базовых принципов и нескольких расширений (которые могут отражать конкретные требования по специализации при обслуживании государственных, отраслевых и иных заказчиков).

SUMMARY

Livshits I.I., **The concept of assessing the IT service providers information security level for industrial facilities.**

Currently, objectively, fairly IS stable is considerable number of significant (critical) threats due to the emergence of new attack vectors ("*Targeted Attack*"), as well as insufficient study and risk management in relation to the previously known threats and vulnerabilities. Respectively, is of particular interest to research the IT-Security problem not only in the phase of operation for the end user (at the facility), but also paying attention to the "culture of production" providers (service providers) IT-Security on their competence - methodological support, availability and level of implementation of standards and procedures (applicable for the purposes of establishing and maintaining the IT-Security level of accompanying IS).

The publication considered relevant risks during the life cycle of IP creation and the influence of modern threats to the level of information security. On the basis of these facts, analysis of regulatory and technical documents (GOST, GOST R ISO standards), risk analysis - proposed wording "IT-Security Paradox" at the present stage of development of IP - all important (critical) threat to IT-Security are the direct result of foreign domination component both in hardware and software, and at the same time, the mechanism effectively counter these risks is contained in the available international standards, especially in today's risk-based ISO standards.

As parry negative impact of "IT-Security Paradox" offered promising areas of information security for IT-Security, among them - the widespread use of the best international standards in the field of information security; changes in the practice of competency assessment IS service providers, conformity assessment and audit information security for existing IT-Security based on existing guidelines FSTEC and / or FBS; spread practice of "instrumental" IT-Security audit.

Based on the facts relevant threats, a brief analysis of normative and technical documents assessing the impact of IT-Security competencies of service providers and the proposed "IT-Security Paradox", introduces the concept of assessing the level of information security service IS providers for industrial facilities. The concept consists of 2 basic principles and a few extensions (which may reflect the specific requirements of specialization in servicing government, industry and other customers).