УДК 004.056.5

Чигринский Е. О.

ОЦЕНКА РИСКОВ И ИНВЕСТИРОВАНИЕ В ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ В УСЛОВИЯХ ЭКОНОМИЧЕСКОГО КРИЗИСА

Рассматривается влияние экономического кризиса на стратегию компаний в области информационной безопасности. Модернизируется методика оценки рисков путем введения новой переменной, отвечающей за кризисную ситуацию. Выделены предпосылки к дальнейшему изучению проблематики.

Ключевые слова: *информационная безопасность, экономический кризис, оценка рисков.*

Chigrinskiy E. O.

RISK MANAGEMENT AND INFORMATION SECURITY INVESTMENT DURING THE FINANCIAL CRISIS

There is a review of financial crisis impact on company's information security strategy. Risk analysis methodology was modified by introduction of new variable which considers the financial crisis. There are some prerequisites for the further issue study.

Keywords: *information security, financial crisis, risk management*

Количество похищенной или скомпрометированной информации в мире выросло на 78%. В мире зафиксировано 1,5 тыс. утечек информации, итогом которых стала компрометация почти 1 млрд учетных данных. В 2014 году аналитическим центром InfoWatch зарегистрировано 1395 (3,8 в день, 116 в месяц) случаев утечки информации. Скомпрометированными оказалось 767 млн персональных данных (записей ПДн), – номера социального страхования, реквизиты пластиковых карт, иная критически важная информация.

Средний ущерб, который наносит кража информации, оценивается в $25,51 млн. Такие данные приводятся в Индексе критичности утечек данных (BLI; Breach Level Index). Совокупный ущерб от утечек в мире, по данным Zecurion, составляет $17,782 млрд. Реальный ущерб подсчитать невозможно, так как все факты о хищениях информации собрать воедино практически нереально [1].

Все вышеприведенные факты могут быть связаны, в том числе, с финансовым кризисом. Эксперты полагают, что любая стагнация в эко-

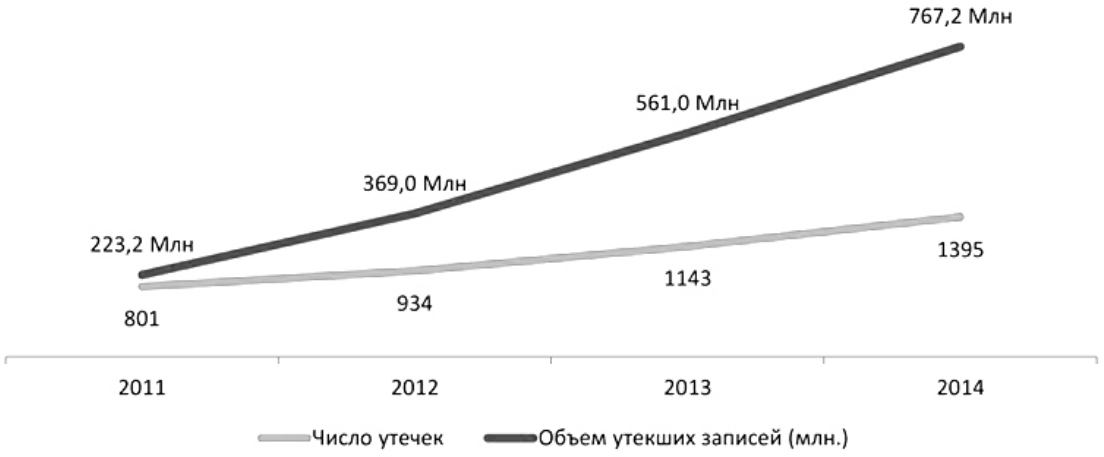

Рис. 1. Число утечек информации и объем утекших записей ПДн, скомпрометированных в результате утечек. 2011 - 2014 гг.

номике приводит к тому, что количество хищений данных из компании, увод клиентов, мошенничество, многократно возрастает. Тайно работая на компанию-конкурента, недобросовестные сотрудники просто подстраховываются от возможных финансовых трудностей.

Многие компании выстраивают свою стратегию защиты информации на основе тех данных, которые были получены в результате оценки рисков информационной безопасности (ИБ). Такой порядок действий логичен и обоснован, риск-менеджмент использует существующие методики и ожидает соответствующих результатов. Тем не менее, согласно приведенным исследованиям, объем потерь не только не сокращается, но и, более того, растет. В таком случае мы можем поставить под сомнение точность существующих методов оценки рисков с учетом явного роста статистики случаев хищения и утечки данных. Можно предположить, что появился некий неучитываемый ранее фактор, влияющий на прогнозы оценочных методов, который может вносить свои коррективы.

И действительно, на данный момент не существует методик оценки рисков ИБ таких, которые бы учитывали динамические факторы. А именно, такие факторы, которые могут появиться в любой момент времени, в зависимости от состояния окружающей среды и/или изменения некоторой ситуации в частности. Прогнозирование таких факторов – чрезвычайно сложная задача. Однако невозможно не признать, что производить расчет информационных рисков безотносительно всякого учета неожиданного появления новых факторов, способных повлиять на уровень информационного риска в целом, было бы недальновидно. Учитывая текущую ситуацию в стране, на данный момент нас интересует фактор экономического кризиса.

На примере метода оценки рисков ИБ на предприятиях малого и среднего бизнеса рассмотрим включение корректирующего фактора в формулу расчета риска реализации угроз [2]. Алгоритм оценки методики с учетом корректировки, затрагивающей экономический фон, представлен на рис. 2.

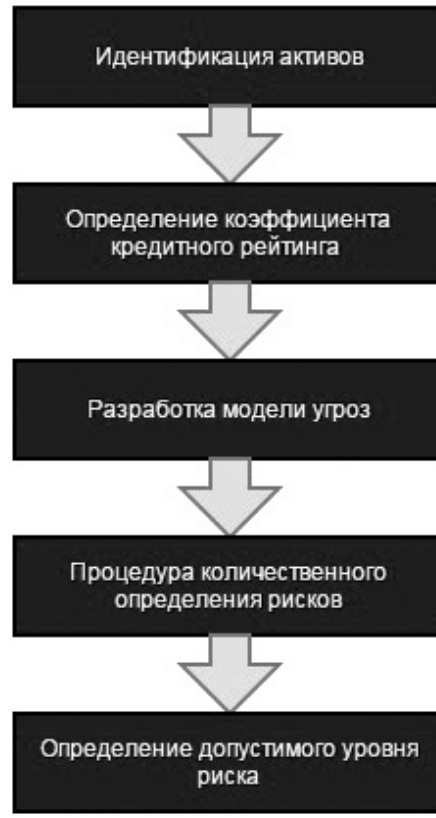

Рис. 2. Алгоритм оценки рисков информационной безопасности.

Шаг 1. Идентификация активов. Руководители отделов и подразделений совместно со специалистами по информационной безопасности определяют все ресурсы, которые имеют ценность или находят полезное применение в организации, обеспечивают непрерывность ее деловых операций.

Шаг 2. Определение риска от кредитного рейтинга. Кредитный рейтинг — мера кредитоспособности частного лица, компании, региона или страны. Кредитные рейтинги рассчитываются на основе прошлой и текущей финансовой истории вышеперечисленных участников рынка, а также на основе оценок размера их собственности и взятых на себя финансовых обязательств. Кредитные рейтинги относительны, поэтому важно учитывать специфику той или иной страны, предприятия, отрасли промышленности. Невысокие кредитные рейтинги, конечно, нежелательны, ибо свидетельствуют о высокой вероятности дефолта [3]. Крупнейшими рейтинговыми агентствами (которые работают во всем мире) являются Moody's, Standard and Poor's и Fitch Ratings. Их системы оценок представлены в таблице 1. Все эти агентства понизили индекс кредитного рейтинга России в 2014 году из-за экономических санкций, замедления темпов экономического роста и сложной геополитической ситуаций между

Таблица 1. Показатели рейтингов крупнейших кредитных агентств.

<table>
<tr><th colspan="3">Индекс кредитного рейтинга</th><th rowspan="2">Характеристика</th></tr>
<tr><th>Moody's</th><th>S&P</th><th>Fitch</th></tr>
<tr><td>Aaa</td><td>AAA</td><td>AAA</td><td>Обязательства наивысшего качества</td></tr>
<tr><td>Aa1</td><td>AA+</td><td>AA+</td><td rowspan="3">Обязательства высокого качества</td></tr>
<tr><td>Aa2</td><td>AA</td><td>AA</td></tr>
<tr><td>Aa3</td><td>AA-</td><td>AA-</td></tr>
<tr><td>A1</td><td>A+</td><td>A+</td><td rowspan="3">Обязательства выше среднего качества</td></tr>
<tr><td>A2</td><td>A</td><td>A</td></tr>
<tr><td>A3</td><td>A-</td><td>A-</td></tr>
<tr><td>Baa1</td><td>BBB+</td><td>BBB+</td><td rowspan="3">Обязательства ниже среднего качества</td></tr>
<tr><td>Baa2</td><td>BBB</td><td>BBB</td></tr>
<tr><td>Baa3</td><td>BBB-</td><td>BBB-</td></tr>
<tr><td>Ba1</td><td>BB+</td><td>BB+</td><td rowspan="3">Рискованные обязательства с чертами спекулятивных</td></tr>
<tr><td>Ba2</td><td>BB</td><td>BB</td></tr>
<tr><td>Ba3</td><td>BB-</td><td>BB-</td></tr>
<tr><td>B1</td><td>B+</td><td>B+</td><td rowspan="3">В высокой степени спекулятивные</td></tr>
<tr><td>B2</td><td>B</td><td>B</td></tr>
<tr><td>B3</td><td>B-</td><td>B-</td></tr>
<tr><td>Caa1</td><td>CCC+</td><td rowspan="5">CCC</td><td>Очень высокий кредитный риск</td></tr>
<tr><td>Caa2</td><td>CCC</td><td>Крайне спекулятивные</td></tr>
<tr><td>Caa3</td><td>CCC-</td><td rowspan="3">Близки к дефолту</td></tr>
<tr><td rowspan="2">Ca</td><td>CC</td></tr>
<tr><td>C</td></tr>
<tr><td>C</td><td rowspan="3">D</td><td>DDD</td><td rowspan="3">В состоянии дефолта</td></tr>
<tr><td>/</td><td>DD</td></tr>
<tr><td>/</td><td>D</td></tr>
</table>

Россией и Украиной. При присвоении рейтинга финансовому институту учитывается следующее:

• Экономические риски – сильные и слабые стороны экономической и политической ситуации в стране (размер экономики, ее состав, перспективы развития), а также какие эффекты (как прямые, так и косвенные) они могут оказать на банковский/финансовый сектор в стране – изменение процентной ставки, спроса на кредиты и др.

• Риски внутри сектора – уделяется отдельное внимание размеру банковского сектора в стране, его структура, его административное регулирование, количество агентов, прозрачность, процент фондов в экономике, проходящих через сектор, динамики конкуренции, барьеры на входе, количество банков и дочерних компаний, иностранное присутствии в данном секторе экономики.

• Ситуация на рынке – положение оцениваемого банка на рынке. Выводы делаются на основании уровня рыночной власти, диверсификации, стратегии, управления рисками, клиентской базы и др [4].

Таким образом, кредитный рейтинг наглядным образом отражает изменения в экономике предприятия или страны и не остается без внимания при надвигающемся или наступившем экономическом кризисе (Табл. 1).

Риск, связанный с экономической обстановкой в стране, влияет на общий риск информационной безопасности компании. Если рассматриваемая компания фигурирует в рейтинге одного из представленных агентств, то следует брать ее соответствующий показатель для определения значения риска согласно таблице 2. Это даст более точные конечные результаты. В противном случае, берется рейтинг страны в целом, в которой осуществляется бизнес. Также возможен вариант, при котором выставить рейтинг предприятия могут собственные эксперты в экономической сфере.

К примеру, мы определяем риск реализации угрозы для ОАО «РЖД». На этом шаге нам нужно определить коэффициент кредитного рейтинга. В январе 2015 года рейтинговое агентство Fitch Ratings присвоило им индекс кредитного рейтинга равным «BBB-», что является по таблице 1 «обязательством ниже среднего качества». Согласно таблице 2 коэффициент кредитного рейтинга ОАО «РЖД» будет равняться 0,4.

Таблица 2. Определение коэффициента кредитного рейтинга.

Категория кредитного рейтинга	Коэффициент кредитного рейтинга (R_k)
Обязательства наивысшего качества	0,1
Обязательства высокого качества	0,2
Обязательства выше среднего качества	0,3
Обязательства ниже среднего качества	0,4
Рискованные обязательства с чертами спекулятивных	0,5
В высокой степени спекулятивные	0,6
Очень высокий кредитный риск	0,7
Крайне спекулятивные	0,8
Близки к дефолту	0,9
В состоянии дефолта	1

Шаг 3. Разработка модели угроз. Необходимо разработать частную модель угроз информационной безопасности экспертным составом специалистов в области защиты информации, в которой также определяется актуальность угроз ИБ. Затем составляется перечень актуальных угроз на каждый выделенный актив из вышеупомянутого шага с определением вероятности реализации угрозы.

Шаг 4. Процедура количественной оценки рисков. Данная процедура включает в себя следующие этапы: выбор актуальных угроз частной модели угроз, определение вероятности наступления угрозы, определение ценности актива, определение возможности использования организационных и технических уязвимостей, вычисление численного значения риска.

Вероятность реализации угрозы на актив равна разности между единицей и произведением вероятностей противоположных событий.

Как правило, точную ценность актива определить достаточно сложно, либо совсем невозможно, поэтому рекомендуется присваивать ему значение от 0 до 1, исходя из того, какое соотношение цены актива к стоимости всего бизнеса. На этом этапе в состав экспертной комиссии рекомендуется включать руководителя компании.

Соответствие выполняемых организационных и технических мер по защите информации к коэффициентам организационных и технических уязвимостей представлены в таблицах 3 и 4 соответственно.

Таблица 3. Определение коэффициента организационных уязвимостей

Сумма выполняемых мер защиты	Коэффициент уязвимости (K_0)
14-17	0,01
8-13	0,25
менее 8	0,5
не выполняются	0,9

Таблица 4. Определение коэффициента технических уязвимостей

Сумма выполняемых мер защиты	Коэффициент уязвимости (K_t)
15-19	0,01
сен.14	0,25
менее 9	0,5
не выполняются	0,9

Формула (1) расчета риска реализации хотя бы одной угрозы из перечня определенных актуальных угроз с учетом наличия уязвимостей по отношению к конкретному активу выглядит следующим образом:

$$R = P_{\text{угр}} R_k C \frac{K_0 + K_t}{2} 100\%, \qquad (1)$$

где R – численная величина риска реализации угроз ИБ; $P_{\text{угр}}$ – вероятность реализации хотя бы одной угрозы из всего перечня актуальных угроз; R_k – коэффициент кредитного рейтинга; C – ценность актива; K_0 – вероятность использования организационных уязвимостей; K_t – вероятность использования технических уязвимостей.

Допустимым принято считать риск, который в данной ситуации считают приемлемым при существующих общественных ценностях. Для компаний малого и среднего бизнеса рекомендованное значение не должно превышать 5%. Считается, что реализация актуальной угрозы, повлекшей ущерб более 5% выручки за отчетный период (1 год), является неприемлемым и требуется принятие эффективных мер.

Заключение.

При внедрении переменной R_k, отвечающей за изменения экономического фона на предприятии или в стране, где ведется бизнес, результаты проведения оценки риска для важных активов станут более точными и позволят более гибко реагировать на экономические колебания. Абсолютно все факторы учесть очень сложно или практически невозможно, но стремиться к этому стоит при корректировке существующих методик или создании новых. В конечном итоге действенность любого метода доказывается на практике. Наблюдение эффекта, оказываемого на общий расчет введением такого коэффициента, а также его влияние на выбор стратегии ИБ и финальный результат планируются к дальнейшему рассмотрению. Идеальным итогом в последующем развитии работы над данной проблематикой было бы создание динамической модели, которая будет учитывать в себе изменения различных внешних факторов, влияющих на конечный результат определения показателя информационного риска в режиме реального времени. Это существенно снизит убытки компаний и позволит оперативно реагировать на изменения внешней среды.

Примечания.

1. Как кризис влияет на количество инцидентов ИБ // Портал СмартСорсинг. URL: http://smartsourcing.ru/blogs/informatsionnaya_

2. bezopasnost/2791/ (дата обращения: 29.04.2015).

3. Плетнев П.В., Белов В.М. Методика оценки рисков информационной безопасности на предприятиях малого и среднего бизнеса // Доклады ТУСУРа. – №1(25), 2012. – С. 83-86.

4. Международный кредитный рейтинг // Портал Кредиты 2014. URL: http://itb2014.org/международный-кредитный-рейтинг/ (дата обращения: 29.04.2015).

5. Титкова Е.С. Методика формирования финансовых рейтингов // Журнал «Мировое и национальное хозяйство» - №4(19), 2011.

Чигринский Евгений Олегович, главный специалист отдела защиты информации МБУ «Электронный Екатеринбург», г. Екатеринбург. E-mail: echigrinskiy@gmail.com