На правах рукописи

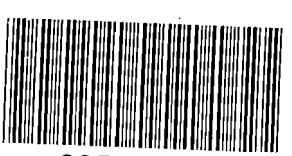
СОБАКИН ИВАН БОРИСОВИЧ

МОДЕЛИРОВАНИЕ ПРОЦЕССА АНАЛИЗА И ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ

Специальность:
08.00.13 – «Математические и инструментальные методы экономики»

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата экономических наук

Москва – 2013



Работа выполнена на кафедре экономики и планирования в организации Федерального государственного бюджетного образовательного учреждения высшего профессионального образования Московского государственного индустриального университета.

Научный руководитель: доктор экономических наук, профессор **Воловиков Сергей Алексеевич**

Официальные оппоненты: доктор экономических наук, профессор **Емельянов Александр Анатольевич,** филиал ФГБОУ ВПО Национальный исследовательский университет «МЭИ» в г. Смоленске, профессор кафедры менеджмента и информационных технологий в экономике

доктор экономических наук **Вершинская Ольга Николаевна,** заведующая лабораторией проблем развития информационного общества ФГБУН Института социально-экономических проблем народонаселения РАН

Ведущая организация: **ФГБОУ ВПО Московский государственный университет экономики, статистики и информатики (МЭСИ)**

Защита состоится 14 ноября 2013 г. в 14-00 часов на заседании диссертационного совета Д 212.129.02 по экономическим наукам в ФГБОУ ВПО Московском государственном индустриальном университете по адресу: 115280, г. Москва, ул. Автозаводская, д. 16, аудитория 1804.

С диссертацией можно ознакомиться в читальном зале библиотеки ФГБОУ ВПО «МГИУ». Электронная копия автореферата размещена на электронном ресурсе МГИУ и на сайте ВАК.

Автореферат разослан 14 октября 2013 г.

Ученый секретарь
диссертационного совета Д 212.129.02
кандидат экономических наук, доцент Т.С. Сальникова

I. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. В современных условиях повсеместная компьютеризация приводит к появлению таких явлений, как финансовое мошенничество с использованием информационных технологий, киберпреступность (хакерские атаки), и даже может привести к возможности совершения террористических атак с использованием Интернета (получение доступа к системам контроля в сфере государственной важности – электростанции, вооружения, финансовые системы и др.). Очевидно, что вопросы обеспечения безопасности информации сегодня являются ключевыми и наиболее актуальны для тех компаний, которые имеют отношение к банковскому сектору, к информационным технологиям, к телекоммуникационным услугам и пр.

Необходимо отметить, что никакие технические, организационные и правовые меры не в состоянии гарантировать полную безопасность и надежность информационных систем. Поэтому основная задача обеспечения информационной безопасности сводится к снижению рисков до приемлемого уровня и созданию некой системы, которая обеспечивала бы целостность, доступность и конфиденциальность критически важной информации, и, как следствие, обеспечивала бы жизнеспособность и эффективность самого бизнеса.

Развитие информационной инфраструктуры предприятия неизменно влечет за собой неконтролируемый рост числа информационных угроз и уязвимостей информационных ресурсов. В этих условиях анализ и оценка рисков информационной безопасности, являясь на сегодняшний день актуальными задачами, позволяет определить необходимый уровень защиты информации, осуществлять его поддержку, а также выработать рекомендации по совершенствованию системы защиты и минимизации рисков. Вместе с тем остается нерешенным целый ряд проблем.

Для компаний коммерческой и банковской сферы наиболее распространенным способом решения вопроса анализа и оценки рисков является применение систем, которые позволяют оценить риски и выбрать якобы оптимальный по эффективности набор защитных мер. В действительности, вопрос экономической обоснованности, который является ключевым при принятии решений о выделении денежных средств на обеспечение информационной безопасности, рассматривается крайне редко.

Несмотря на то, что в современной научной литературе, в международных и национальных стандартах уделяется большое внимание проблемам анализа, оценки и управления рисками информационной безопасности, зачастую предлагаются наиболее общие рекомендации и не учитываются конкретные специфические особенности ИТ-инфраструктуры организации, работающей в том или ином секторе.

В связи с изложенным можно заключить, что на сегодняшний день возникла необходимость рассмотрения вопросов анализа и оценки рисков информационной безопасности применительно к конкретной области рассмотрения и создания некой математической модели, которая бы позволила принимать экономически обоснованные решения.

Степень научной разработанности проблемы. Моделирование и анализ рисков информационной безопасности достаточно давно обсуждается в научных кругах. Большое значение для постановки проблемы исследования имели работы таких авторов, как Астахов А.М., Галатенко В.А., Емельянов А.А., Игнатьев В.А., Курило А.П., Медведовский И.Д., Фатьянова А.А. и др. Они представляют интерес в плане анализа угроз информационной безопасности, их классификации и выработки концептуально-правовых подходов их преодоления. В работе также использовались результаты последних диссертационных исследований в области анализа и управления информационными рисками.

В научной литературе сформировалось множество подходов к исследованию данной темы, большая часть информации находит свое отражение в международных и национальных стандартах по информационной безопасности.

Вместе с тем, принимая во внимание труды таких авторов, как Завгородний В.И., Петренко С.А, Симонов С.В. и др., касающиеся вопросов оценки и управления рисками информационной безопасности, в целом в научной литературе им уделено мало внимания. Так, передовые зарубежные подходы к оценке уровня риска и определения оптимального объема инвестиций в информационную безопасность не рассмотрены вовсе.

Кроме того, до сих пор не предложена и не сформирована общая методика анализа и оценки рисков информационной безопасности организаций кредитно-финансовой системы, в т.ч. банковского сектора, имеющих свою специфику и особенности.

В целом можно сделать вывод об актуальности и недостаточной степени научной разработанности проблемы анализа и оценки рисков информационной безопасности, что обусловило выбор темы настоящего исследования и определило его цели и задачи.

Цель диссертационного исследования состоит в разработке модели анализа и оценки рисков информационной безопасности организаций банковской системы. В соответствии с поставленной целью диссертационного исследования, конкретизируются следующие **задачи**:

- провести сравнительный анализ существующих методик и основных подходов к оценке уровня риска и определения оптимального объема инвестиций в информационную безопасность;
- определить вид и построить экономико-математическую модель, наиболее отражающую зависимость общего уровня риска от средств, вложенных в мероприятия по защите информационной безопасности с учетом специфики банковской деятельности;

- разработать модель угроз информационной безопасности в системе дистанционного банковского обслуживания (ДБО);
- апробировать предложенную методику и осуществить расчет общего уровня риска и оптимального объема инвестиций в обеспечение безопасности системы ДБО.

Объект и предмет исследования. Объектом диссертационного исследования является система управления информационной безопасностью организаций банковской системы. Предметом исследования выступают модели и методы оценки рисков информационной безопасности.

Соответствие паспорту специальностей. Диссертационное исследование соответствует основным положениям пунктов паспорта специальности ВАК 08.00.13 – «Математические и инструментальные методы экономики»:

– п. 1.10. Разработка и развитие математических моделей и методов управления информационными рисками;

– п. 2.11. Развитие экономических методов обеспечения информационной безопасности в социально-экономических системах.

Теоретическая и методологическая основа исследования. В процессе исследования были проанализированы и использованы труды как отечественных, так и зарубежных ученых в области теории информации, информационных систем, информационной безопасности и риск-менеджмента. При проведении диссертационного исследования использовались методы дедукции и индукции, сравнительного и системного анализа, а также CASE-моделирование. В работе применялись международные стандарты в области защиты информации и анализа информационных рисков (серия ISO 27000 и др.), а также описания существующих методов и инструментальных средств управления информационными рисками.

В качестве основных методов, использовавшихся для решения поставленных в исследовании задач, необходимо отметить методы теории моделирования, системный подход, экономико-статистический анализ, метод сравнения и научной абстракции.

Информационной базой исследования, обеспечивающей достоверность первичных данных, послужили законодательные и нормативно-правовые акты органов государственной власти, принятые на территории Российской Федерации, руководящие документы Гостехкомиссии России, данные статистических служб зарубежных государств, монографии и публикации в периодической печати, справочно-статистические материалы, а также материалы электронных ресурсов сети Интернет.

Научная новизна. Элементы научной новизны составляют следующие выносимые на защиту результаты работы:

- обоснована необходимость адаптации существующих подходов к анализу и оценке рисков информационной безопасности применительно к исследуемой информационной области в банковских организациях;
- разработана экономико-математическая модель оптимизации затрат на обеспечение информационной безопасности применительно к особенностям организаций банковского сектора, достоинством которой является возможность использования диапазонной оценки вероятности реализации угроз;
- разработана модель угроз в системе дистанционного банковского обслуживания, учитывающая типы нарушителей и характерные для них способы реализации угроз информационной безопасности персональных данных и платежной информации;
- на основе построенных моделей произведен расчет общего уровня риска, что позволяет определить объем инвестиций, обеспечивающий

задаваемый уровень защиты системы дистанционного банковского обслуживания.

Теоретическая и практическая значимость работы. Теоретическая значимость исследования определяется полученными результатами анализа основных подходов к оценке уровня риска и определения оптимального объема инвестиций в информационную безопасность и заключается в обосновании и разработке полученной методики и экономико-математической модели.

Практическая значимость работы состоит в возможности использования полученных методических результатов и математических средств в процессе анализа, оценки и управления рисками информационной безопасности, а также при построении и совершенствовании систем управления информационными рисками организаций банковской сферы.

Апробация результатов исследования. Основные положения диссертации докладывались, обсуждались и получили положительную оценку на теоретических семинарах кафедры информационных технологий и систем в экономике и управлении, а также на межвузовских конференциях и семинарах, в частности: на научно-практической конференции «Экономико-организационные аспекты модернизации промышленности» (Москва, 2012); на межкафедральном научном семинаре факультета экономики менеджмента и информационных технологий МГИУ (Москва, 2013); на 2-ой вузовской межкафедральной научно-практической конференции «Современные технологии обеспечения информационной и экономической безопасности» (Москва, 2013); на всероссийской межвузовской научно-практической конференции «Современные аспекты развития экономики России: проблемы и перспективы» (Москва, 2013).

Проведенное исследование позволило подготовить и внести ряд предложений по совершенствованию существующей методики анализа и

оценки рисков информационной безопасности системы дистанционного банковского обслуживания одного из коммерческих банков.

Публикации. Основные результаты диссертации отражены в 9-ти научных работах, четыре из которых опубликованы в периодических изданиях из Перечня ВАК. Авторский объем составляет 3,5 п.л.

Структура и объем диссертации. Диссертационная работа состоит из введения, трех глав, заключения, списка использованной литературы и приложений, дополняющих основной текст.

Общий объем исследования – 116 страниц машинописного текста, содержит 10 таблиц и 15 рисунков. Список литературы насчитывает 86 наименований, из которых 24 на иностранном языке.

В соответствии с целью и задачами исследования, работа построена следующим образом:

Во введении дано обоснование актуальности темы диссертационного исследования, определены цель, задачи, приведена теоретическая и методологическая основа, информационная база исследования, отмечается научная новизна работы и положения, выносимые на защиту, а также практическая ценность работы, приводятся сведения об апробации полученных результатов.

В Главе 1 «Основные подходы и методические основы анализа и оценки рисков информационной безопасности» рассматривается сущность риск-ориентированного подхода к обеспечению информационной безопасности и методическое обеспечение процесса анализа и оценки рисков. Кроме того, анализируются существующие подходы к оценке уровня риска и инвестиций в информационную безопасность.

В Главе 2 «Методика анализа и оценки рисков информационной безопасности организаций банковской системы» формируется общая методика анализа и оценки рисков информационной безопасности организаций банковской системы: идентифицируются основные активы,

анализируются основные угрозы и уязвимости, предлагается экономико-математическая модель оптимизации затрат на обеспечение ИБ.

В Главе 3 «Разработка модели анализа и оценки рисков информационной безопасности системы дистанционного банковского обслуживания» применительно к системе ДБО разработана модель угроз информационной безопасности, на основе предлагаемой экономико-математической модели произведен расчет общего уровня риска и оптимального объема инвестиций в обеспечение информационной безопасности.

В Заключении изложены основные выводы и практические предложения, выработанные автором в ходе работы над диссертационным исследованием.

II. ОСНОВНЫЕ НАУЧНЫЕ ПОЛОЖЕНИЯ И РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ, ВЫНОСИМЫЕ НА ЗАЩИТУ

1. Обоснована необходимость адаптации существующих подходов к анализу и оценке рисков информационной безопасности применительно к исследуемой информационной области организаций банковского сектора.

В недавнем прошлом вся мировая, в том числе отечественная, практика регулирования информационной безопасности заключалась в обязательном соблюдении требований всех регулирующих органов. С учетом невозможности охвата всех возможных видов деятельности и предложения универсального набора требований, распространенная практика оказалась неадекватной существующей реальности.

Дальнейший путь эволюции обеспечения информационной безопасности сводился к тому, что топ-менеджмент и руководство отделов ИБ персонально делали выбор в сторону предложенных стандартных наборов защитных мер.

Недостатком указанного подхода послужила неизвестность при принятии риска, а именно отсутствие данных о его величине.

Вскоре эксперты пришли к заключению, что само обеспечение ИБ может порождать дополнительные риски. И последующая эволюция модели ИБ свелась к позиции, согласно которой все риски информационной безопасности должны быть согласованы с рисками организации в целом. Так, появилась задача интеграции системы управления информационными рисками (СУИР) в систему корпоративного управления всей компанией.

При всех своих достоинствах прагматичные модели ИБ (расчет совокупной стоимости владения СУИБ, «возврат» инвестиций и пр.) требуют большого объема статистической и прогностической информацией и не получили широкого распространения в силу ожесточенной конкуренции в бизнес среде.

Рассмотренные количественные подходы, будучи общепринятыми и хорошо зарекомендовавшими себя на практике, позволяют нам выяснить являются ли затраты на информационную безопасность обоснованными с экономической точки зрения. Однако данные подходы не исключают проблему неточности исходных данных, не предоставляют достаточной информации для сравнительного анализа, расстановки приоритетов и для принятия решения в целом.

Остается открытым вопрос оптимальности размера инвестиций в информационную безопасность и определения тех участков системы, повышение затрат на защиту которых наиболее существенно повлияет на снижение риска для системы в целом.

Проведенный анализ позволил сформулировать вывод о необходимости формирования методического инструментария для анализа и оценки рисков информационной безопасности применительно к определенной информационной области или сферы деятельности с учетом динамики параметров риска.

2. С учетом специфики банковской деятельности разработана экономико-математическая модель оптимизации затрат на обеспечение информационной безопасности.

Несмотря на то, что теоретические разработки в области рисков банковской деятельности ведутся уже более 20 лет, законченной или даже сколько-нибудь полной «теории» этих рисков до настоящего времени не создано – проработаны только отдельные направления.

В настоящее время отмечается неточность исходных данных для расчета коэффициентов рентабельности инвестиций в информационную безопасность. Поэтому большинство организаций основываются на качественных методах оценки. Достоинство качественного подхода к измерению величины риска заключается в том, что можно довольно быстро и с точностью, зависящей от квалификации экспертов в области ИБ, расположить риски по приоритетам и выявить те области, где требуется незамедлительное принятие защитных мер.

Однако если кредитная организация ставит перед собой цель – оценка экономического капитала для обеспечения информационной безопасности, то этого будет недостаточно, так как применение качественного подхода не позволяет рассчитать его величину. Качественные подходы не предоставляют достаточной информации для сравнительного анализа, расстановки приоритетов и для принятия решения в целом. Кроме того, они лишь приблизительно указывают на наиболее уязвимые места системы и не дают каких-либо рекомендаций по совершенствованию системы защитных мер, ограничиваясь ссылками на существующие международные и национальные стандарты.

Таким образом, у руководства компаний появляется необходимость количественного расчета для финансового обоснования инвестиций в информационную безопасность. Более того, будучи общепринятыми и хорошо зарекомендовавшими себя на практике количественные подходы

позволяют нам выяснить являются ли затраты на информационную безопасность обоснованными, в частности, с экономической точки зрения.

Если кредитная организация настроена на последовательное внедрение количественной оценки величины риска информационной безопасности, следует выбирать способы моделирования, которые бы позволили учесть как исторические данные о потерях и реализациях угроз, так и экспертные знания.

Риск (R) рассматривается подавляющим большинством экспертов как комплексная величина, которая предполагает существование таких факторов, как угрозы, уязвимости и сам ущерб, и выражается при помощи:

$$R = \lambda \cdot P_T \cdot P_V(z), \quad (1)$$

где λ – размер ущерба (потерь) в случае нарушения безопасности информационного актива; P_T – величина вероятности возникновения угрозы; $P_V(z)$ – функция, описывающая вероятность реализации угрозы для информационного актива в зависимости от затрат на обеспечение защитных мер; z – затраты на обеспечение защиты информационного актива в денежном выражении.

Размер ущерба, таким образом, зависит исключительно от защищаемой информации. Вероятность возникновения угрозы определяется также как фиксированная величина, которая является заданной первоначально. Что касается вероятности реализации угрозы, то путем вливания инвестиций (z) в информационную безопасность актива ее значение может быть снижено.

Среди мнений как зарубежных, так и отечественных экспертов отмечается следующая тенденция: с увеличением объема инвестиций в информационную безопасность вероятность реализации угрозы в отношении информационного актива уменьшается по экспоненциальному закону.

Однако когда речь идет о преднамеренных действиях людей, в частности, о получении несанкционированного доступа к защищаемой

информации, оценка вероятностей возникновения и реализации угрозы, представляет собой определенную трудность. Злоумышленник будет оценивать свои силы, и его действия в данной ситуации будут напрямую зависеть от существующей системы безопасности. Так, если система плохо защищена, он попытается произвести злонамеренные действия, в противном случае – не решится. Таким образом, инвестиции в информационную безопасность будут также оказывать влияние и на вероятность возникновения угрозы.

Предположим, что с увеличением объема денежных средств, выделяемых на информационную безопасность, вероятность возникновения угрозы в отношении информационного актива уменьшается согласно экспоненциальному закону.

Тогда функция и график зависимости (рисунок 1) вероятности возникновения угрозы от затрат на информационную безопасность будут иметь вид:

$$P_T(z) = t \cdot e^{-\varphi z}, \quad \begin{cases} \forall t \in [0;1], \\ \forall z \in R, \end{cases} \tag{2}$$

где t – величина вероятности возникновения угрозы; φ – поправочный коэффициент относительно затрат на ИБ; z – затраты на обеспечение защиты информационного актива в денежном выражении.

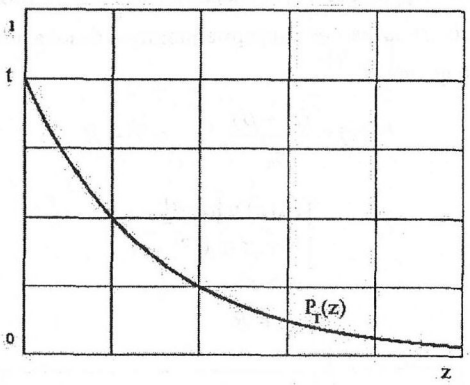


Рисунок 1. Зависимость вероятности возникновения угрозы (P_T) *от инвестиций в ИБ* (z).

С учетом опыта информационных атак прослеживается четкий тренд – со значительным ростом инвестиций в информационную безопасность актива, имеющего особую ценность для организации, вероятность возникновения угрозы действительно снижается, а вероятность ее реализации увеличивается.

Данное утверждение основывается на тех фактах, что организация взлома правительственных и официальных сайтов, баз данных правоохранительных органов, систем безопасности банков и корпораций, а также ряда крупных информационных порталов осуществляется в подавляющем большинстве профессиональными хакерами и злоумышленниками.

Профессиональные хакеры характеризуются тем, что они имеют большой опыт, обладают, как правило, высокими или выдающимися способностями в своей сфере, используют продвинутые разработки для совершения действий, постоянно изучают слабости (уязвимости) своих потенциальных «клиентов».

Предлагаемая функция и график зависимости (рисунок 2) вероятности реализации угрозы от затрат на информационную безопасность будет иметь вид квадратичной функции:

$$P_V(z) = \frac{(\alpha - \beta)}{z_0^2} \cdot (z - z_0)^2 + \beta, \tag{3}$$

$$\begin{cases} P_V(z) \in [\alpha; \beta], \\ \forall \alpha, \beta \in [0;1], \\ \alpha \geq \beta, \\ \forall z \in R. \end{cases}$$

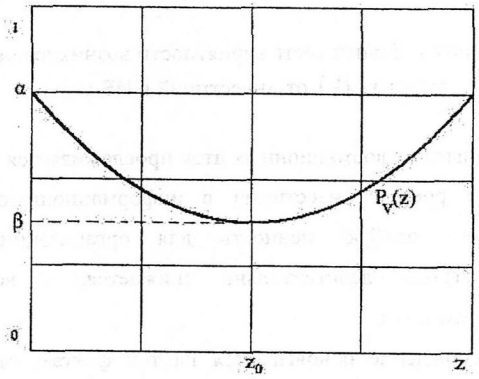


Рисунок 2. Зависимость вероятности реализации угрозы (P_V) от инвестиций в ИБ (z).

Параметр z обозначает объем денежных средств, выделяемый на обеспечение защиты информационного актива. Параметры α и β являются верхней и нижней границами вероятности реализации угрозы соответственно и определяются методом экспертных оценок.

Следует отметить, что именно отсутствие возможности указать нижний предел вероятности реализации угрозы является одним из недостатков известных моделей. В современном мире даже очень значительный объем

инвестиций, направленный на обеспечение безопасности, не может снизить вероятность нанесения ущерба до нулевого значения. Примером в данном случае может служить вероятность возникновения, к примеру, какой-либо аварии, катастрофы и т.п.

Определение объема денежных средств, выделяемых на защитные меры, при котором значение функции вероятности реализации угрозы достигает нижней границы β, т.е. точки z_0, представляет собой определенную трудность.

Известная экономическая модель Гордона-Лоеба показывает, что оптимальный уровень инвестиций не превышает $\frac{1}{e} \approx 36{,}8\%$ от общих потерь в случае нарушения безопасности информационного актива. Кроме того, другие авторы[1] дали оценку и экспериментально подтвердили представленные в указанной модели предположения, доказав данный факт эмпирическим путем.

С учетом отсутствия статистических данных, и исходя из интуитивных соображений, представляется целесообразным увязать значение z_0 с величиной равной $\frac{1}{e} \approx 36{,}8\%$ от размера ущерба вследствие нарушения ИБ актива.

Таким образом функция зависимости вероятности реализации угрозы от затрат на информационную безопасность будет иметь следующий вид:

$$P_V(z) = \frac{(\alpha - \beta)}{(\lambda/e)^2} \cdot (z - \lambda/e)^2 + \beta, \qquad (4)$$

где λ – размер потерь в случае нарушения безопасности информационного актива.

Необходимо отметить, что в исследовании рассмотрены несколько альтернативных классов функций зависимости вероятности реализации

[1] Tanaka, H., Matsuura, K. (2005). Vulnerability and effects of information security investment: A firm level empirical analysis of Japan. In Paper presented at forum on financial information systems and cyber security, College Park, Maryland, May.

угрозы от затрат на информационную безопасность. Выбор же квадратичной зависимости в работе обусловлен сложностью определения дополнительных параметров (коэффициентов) в альтернативных функциях и их интерпретации для дачи экспертных оценок.

Для нахождения оптимального уровня инвестиций в информационную безопасность необходимо решить задачу минимизации значения общих потерь и затрат при имеющихся ограничениях, что графически показано на рисунке 3.

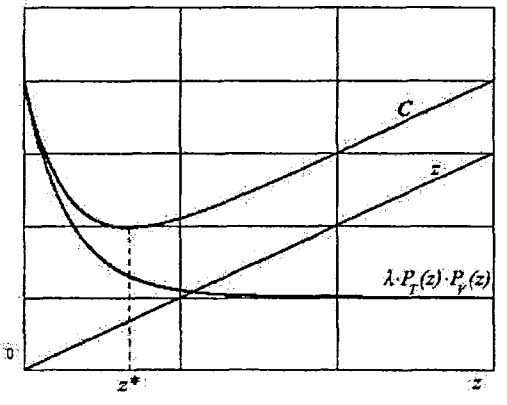


Рисунок 3. Оптимальный уровень инвестиций в ИБ (z^*).

Задача нахождения оптимального уровня инвестиций в информационную безопасность будет тогда иметь вид:

$$C = \lambda \cdot P_T(z) \cdot P_V(z) + z = \lambda \cdot t \cdot e^{-\varphi z} \cdot \left(\frac{(\alpha - \beta)}{(\lambda/e)^2} \cdot (z - \lambda/e)^2 + \beta \right) + z \to \min, \quad (5)$$

при имеющихся ограничениях.

3. Разработана модель угроз информационной безопасности в системе дистанционного банковского обслуживания.

Разработку модели угроз информационной безопасности в системе дистанционного банковского обслуживания коммерческого банка целесообразно осуществлять, основываясь на стандартах и рекомендациях Банка России.

Согласно терминологии, приведенной в СТО БР ИББС-1.0, модель угроз информационной безопасности содержит в себе описание источников угроз; угроз безопасности; уровень реализации угрозы безопасности; типов объектов, пригодных для реализации угроз ИБ.

Таким образом, процесс разработки модели угроз можно разделить на следующие этапы:

- идентификация типов информационных активов, входящих в область оценки рисков;
- определение перечня типов объектов среды, соответствующих каждому из типов информационных активов;
- определение источников угроз для каждого из типов объектов среды, определенных в рамках выполнения предыдущего этапа.

С учетом особенностей мошенничества в системе ДБО, все информационные активы целесообразно объединить в единый тип – платежная и аутентификационная информация пользователей системы ДБО, сведения, составляющие коммерческую и банковскую тайны.

Согласно стандарту Банка России (СТО БР ИББС 1.0) реализация угроз безопасности данных возможна на следующих уровнях информационной инфраструктуры:

— физический уровень;
— сетевой уровень;
— уровень сетевых приложений и сервисов;
— уровень операционных систем;
— уровень систем управления базами данных;
— уровень банковских технологических процессов и приложений.

Формирование перечня типов объектов среды выполняется согласно иерархии уровней информационной инфраструктуры организации. В частности, указанный перечень содержит следующие типы объектов среды:

— линии связи и сети передачи данных;

— сетевые, программные и аппаратные средства, в том числе сетевые серверы;

— файлы данных, базы данных, хранилища данных;

— носители информации, в том числе бумажные носители;

— прикладные и общесистемные программные средства;

— программно-технические компоненты автоматизированных систем;

— помещения, здания, сооружения;

— платежные и информационные технологические процессы.

Выявление источников угроз с соответствующим уровнем детализации зависит от реальных потребностей организации в защите информации, т.е. от соотношения стоимости самой защиты и стоимости риска.

Процесс идентификации риска является циклическим. Первоначально составляется грубая схема цепочек «угроза→величина риска» без детализированного описания моделей угроз, проводится сравнительная стоимостная оценка экспертным способом с привлечением данных по потерям банка. На основе этой оценки выделяются наиболее значимые факторы риска и для них уже строятся детальные модели нарушителей.

Угрозы, исходящие от человека, являются наиболее разнообразными, что определяет необходимость высокой детализации в их описании. Факторы риска, связанные с действиями внешних (хакеры, промышленные шпионы и пр.) и внутренних нарушителей (сотрудники компании), необходимо описывать более детально, включая их потенциальные мотивы, стереотипы поведения и типичные действия в связке с уязвимостями.

С учетом рекомендаций Банка России целесообразно выделить следующие источники угроз для системы ДБО:

— внешний нарушитель, компьютерный злоумышленник;

— внутренний нарушитель (сотрудник банка), нелояльный сотрудник организации (клиента).

Фрагмент разработанной модели представлен в таблице 1.

Таблица 1

Фрагмент модели угроз информационной безопасности в системе ДБО

Источник угрозы ИБ	Уровень реализации угрозы безопасности	Объекты среды	Угрозы	Способ реализации
Внешний нарушитель, компьютерный злоумышленник	Сетевой уровень	Активное оборудование ЛВС	Нарушение конфиденциальности	А1.Несанкционированный доступ к ресурсам ЛВС извне (перехват данных на маршрутизаторе, создание ложного маршрутизатора); сетевые атаки с целью получения НСД
			Нарушение доступности	А2.Приведение межсетевого экрана, оборудования ЛВС, каналов связи к отказу в обслуживании (удаленные сетевые атаки)
	Уровень сетевых приложений и сервисов	Программные компоненты передачи данных между клиентом и банком	Нарушение доступности	А3.Внедрение по сети на ПК клиента программ, влияющих на работу системы ДБО; подмена платежного поручения посредством использования вредоносного ПО
				А4.Внедрение по сети вредоносных программ в компьютерную систему банка
	Уровень операционных систем	Файлы данных	…	…
	Уровень систем управления базами данных	Базы данных	…	…
	Уровень технологических приложений и сервисов	Прикладные программы доступа и обработки информации, бумажные носители, клиентские АРМ	…	…
Внутренний нарушитель (сотрудник банка), нелояльный сотрудник организации (клиента)	…	…	…	…

4. На основе построенных моделей произведен расчет общего уровня риска и оптимального объема инвестиций в обеспечение безопасности системы дистанционного банковского обслуживания.

Риск нарушения информационной безопасности определяется на основании экспертных оценок:

— степени вероятности возникновения угрозы (СВВ);

— степени возможности реализации угроз ИБ (СВР);

— степени тяжести последствий (СТП).

В таблице 2 и таблице 3 показаны соотношения количественной и качественной оценки для каждой из вышеуказанных вероятностей.

Таблица 2

Соотношение количественной и качественной оценки СВВ и СВР

Величина СВР (СВВ)	**Количественная оценка величины СВР (СВВ)**
Минимальная	0-20%
Низкая	20-40%
Средняя	40-60%
Высокая	60-80%
Критическая	80-100%

Таблица 3

Соотношение количественной и качественной оценки СТП

Величина СТП	**Количественная оценка величины СТП**
Низкая	До 0,5% от капитала банка
Средняя	0,5-1,5% от капитала банка
Высокая	1,5-3,0% от капитала банка
Критическая	Более 3% капитала банка

В рассматриваемом банке величина капитала составляет 1,6 млрд. руб.

Количественная оценка риска информационной безопасности системы ДБО в целом представлена в таблице 4.

Таблица 4

Источник угрозы ИБ	Объекты среды актива	Угрозы	СВВ		СВР		СТП		Оценка риска
			Качеств.	Колич.	Качеств.	Колич.*	Качеств.	Колич., руб.	(колич.), руб.
Внешний нарушитель, компьютерный злоумышленник	Активное оборудование ЛВС	A1	Средняя	0,5	Критич.	0,8 (0,2)	Средняя	15 млн.	6 000 000
		A2	Высокая	0,7	Критич.	0,9 (0,3)	Низкая	6 млн.	3 780 000
	Программные компоненты передачи данных между клиентом и банком	A3	Высокая	0,75	Критич.	0,85 (0,2)	Высокая	24 млн.	15 300 000
		A4	Средняя	0,5	Критич.	0,8 (0,2)	Средняя	21 млн.	8 400 000
	Файлы данных	A5	Средняя	0,41	Средняя	0,5 (0,2)	Средняя	23 млн.	4 715 000
		A6	Низкая	0,3	Средняя	0,5 (0,1)	Высокая	44 млн.	6 600 000
		A7	Высокая	0,6	Средняя	0,45 (0,1)	Высокая	47 млн.	12 690 000
	Базы данных	A8	Миним.	0,1	Низкая	0,35 (0,1)	Критич.	53 млн.	1 855 000
		A9	Низкая	0,28	Низкая	0,2 (0,05)	Средняя	18 млн.	1 008 000
		A10	Низкая	0,3	Низкая	0,2 (0,05)	Средняя	17 млн.	1 020 000
	Прикладные программы доступа и обработки информации, бумажные носители, клиентские АРМ	A11	Высокая	0,6	Критич.	0,9 (0,2)	Средняя	20 млн.	10 800 000
		A12	Высокая	0,7	Критич.	0,8 (0,2)	Высокая	26 млн.	14 560 000
		A13	Высокая	0,7	Критическая	0,9 (0,3)	Средняя	14 млн.	8 820 000
Внутренний нарушитель (сотрудник банка), нелояльный сотрудник организации (клиента)	Линии связи, аппаратные и технические средства, физические носители информации	A14	Низкая	0,2	Высокая	0,6 (0,1)	Средняя	16 млн.	1 920 000
		A15	Низкая	0,25	Высокая	0,7 (0,4)	Средняя	15 млн.	2 625 000
		A16	Низкая	0,22	Высокая	0,6 (0,1)	Высокая	38 млн.	5 016 000
		A17	Низкая	0,25	Средняя	0,5 (0,1)	Низкая	5 млн.	625 000
	Активное оборудование ЛВС	A18	Миним.	0,1	Высокая	0,7 (0,2)	Высокая	42 млн.	2 940 000
		A19	Миним.	0,12	Высокая	0,7 (0,2)	Высокая	43 млн.	3 612 000
		A20	Миним.	0,13	Высокая	0,6 (0,2)	Высокая	36 млн.	2 808 000
	Программные компоненты передачи данных между клиентом и банком	A21	Миним.	0,15	Высокая	0,6 (0,1)	Средняя	14 млн.	1 260 000
		A22	Миним.	0,16	Высокая	0,6 (0,1)	Средняя	12 млн.	1 152 000
	Файлы данных	A23	Средняя	0,5	Критич.	0,8 (0,4)	Высокая	30 млн.	12 000 000
		A24	Низкая	0,3	Высокая	0,65 (0,1)	Высокая	34 млн.	6 630 000
	Базы данных	A25	Средняя	0,41	Критич.	0,8 (0,4)	Критич.	49 млн.	16 072 000
		A26	Низкая	0,2	Высокая	0,63 (0,1)	Средняя	8 млн.	1 008 000
		A27	Низкая	0,25	Высокая	0,62 (0,1)	Средняя	9 млн.	1 395 000
	Прикладные программы доступа и обработки информации, бумажные носители, клиентские АРМ	A28	Высокая	0,65	Критич.	0,8 (0,3)	Высокая	32 млн.	16 640 000
		A29	Средняя	0,5	Критич.	0,9 (0,2)	Высокая	28 млн.	12 600 000
		A30	Миним.	0,18	Средняя	0,5 (0,2)	Низкая	4 млн.	360 000
		A31	Миним.	0,15	Высокая	0,6 (0,3)	Средняя	10 млн. руб.	900 000

* – в скобках количественной оценки СВР указана минимальная величина степени реализации угрозы при максимальном объеме выделяемых средств.

Задача нахождения оптимального уровня инвестиций в информационную безопасность при известных ограничениях относится к классу задач нелинейного программирования. Для ее решения был использован программный продукт «Mathcad». Фрагмент области рабочего листа программы проиллюстрирован на рисунке 4. Расчет оптимального объема инвестиций в обеспечение информационной безопасности системы ДБО представлен в таблице 5.

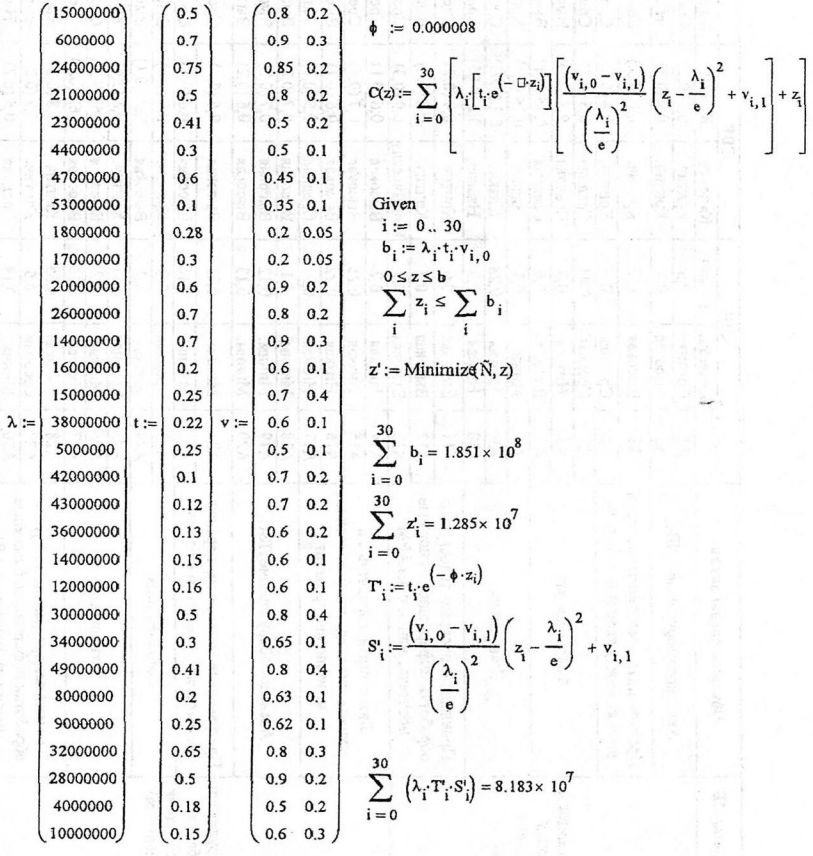


Рисунок 4. Фрагмент области рабочего листа «Mathcad».

Таблица 5

Расчет оптимального объема инвестиций в обеспечение информационной безопасности системы дистанционного банковского обслуживания

Уг-розы	t (СВВ)	v (СВР)		λ, руб. (СТП)	Риск (R) ДО, руб.	z^*, руб.	$P_T(z^*)$	$P_V(z^*)$	Риск (R) ПОСЛЕ, руб.
A1	0,5	0,8	0,2	15 000 000	6 000 000	471 926	0,22	0,78	2 623 354
A2	0,7	0,9	0,3	6 000 000	3 780 000	404 342	0,31	0,85	1 598 190
A3	0,75	0,85	0,2	24 000 000	15 300 000	590 642	0,34	0,84	6 756 321
A4	0,5	0,8	0,2	21 000 000	8 400 000	516 228	0,22	0,78	3 701 553
A5	0,41	0,5	0,2	23 000 000	4 715 000	448 081	0,18	0,49	2 088 717
A6	0,3	0,5	0,1	44 000 000	6 600 000	491 290	0,13	0,50	2 936 348
A7	0,6	0,45	0,1	47 000 000	12 690 000	572 224	0,27	0,45	5 650 834
A8	0,1	0,35	0,1	53 000 000	1 855 000	335 302	0,04	0,35	827 414
A9	0,28	0,2	0,05	18 000 000	1 008 000	257 193	0,13	0,20	442 741
A10	0,3	0,2	0,05	17 000 000	1 020 000	258 407	0,13	0,20	447 411
A11	0,6	0,9	0,2	20 000 000	10 800 000	545 846	0,27	0,88	4 750 852
A12	0,7	0,8	0,2	26 000 000	14 560 000	585 422	0,31	0,79	6 440 168
A13	0,7	0,9	0,3	14 000 000	8 820 000	518 981	0,31	0,88	3 861 480
A14	0,2	0,6	0,1	16 000 000	1 920 000	333 978	0,09	0,58	838 491
A15	0,25	0,7	0,4	15 000 000	2 625 000	375 745	0,11	0,69	1 161 333
A16	0,22	0,6	0,1	38 000 000	5 016 000	456 595	0,10	0,59	2 227 059
A17	0,25	0,5	0,1	5 000 000	625 000	193 221	0,11	0,46	257 067
A18	0,1	0,7	0,2	42 000 000	2 940 000	391 698	0,04	0,69	1 308 853
A19	0,12	0,7	0,2	43 000 000	3 612 000	417 212	0,05	0,69	1 608 366
A20	0,13	0,6	0,2	36 000 000	2 808 000	385 755	0,06	0,59	1 249 061
A21	0,15	0,6	0,1	14 000 000	1 260 000	282 366	0,07	0,58	548 011
A22	0,16	0,6	0,1	12 000 000	1 152 000	270 621	0,07	0,58	498 306
A23	0,5	0,8	0,4	30 000 000	12 000 000	565 321	0,22	0,79	5 343 313
A24	0,3	0,65	0,1	34 000 000	6 630 000	490 165	0,13	0,64	2 938 906
A25	0,41	0,8	0,4	49 000 000	16 072 000	603 872	0,18	0,80	7 181 664
A26	0,2	0,63	0,1	8 000 000	1 008 000	251 567	0,09	0,59	427 470
A27	0,25	0,62	0,1	9 000 000	1 395 000	290 719	0,11	0,59	595 537
A28	0,65	0,8	0,3	32 000 000	16 640 000	605 254	0,29	0,79	7 397 780
A29	0,5	0,9	0,2	28 000 000	12 600 000	567 919	0,22	0,89	5 576 462
A30	0,18	0,5	0,2	4 000 000	360 000	131 090	0,08	0,46	149 015
A31	0,15	0,6	0,3	10 000 000	900 000	242 750	0,07	0,58	393 553
					185 111 000	**12 851 731**			**81 825 630**

Оптимальный объем инвестиций в обеспечение ИБ системы ДБО составляет 12 851 731 руб. Таким образом, вложив указанную сумму, возможные потенциальные потери снизятся с 185 111 000 руб. до 81 825 630 руб.

III. ОСНОВНЫЕ РЕЗУЛЬТАТЫ И ВЫВОДЫ

1. Проведен сравнительный анализ наиболее распространенных, в т.ч. передовых зарубежных, подходов к оценке уровня риска и определения оптимального объема инвестиций в информационную безопасность. Анализ показал ограниченность в применяемости подходов и позволил сформулировать вывод о необходимости формирования методического инструментария для анализа и оценки рисков информационной безопасности применительно к определенной информационной области или сферы деятельности с учетом специфики функционирования организаций.
2. Разработана экономико-математическая модель оптимизации затрат на обеспечение информационной безопасности организаций банковского сектора. Предложенная модель описывает зависимость общего уровня риска от объемов инвестиций в обеспечение информационной безопасности, достоинством которой, является возможность использования диапазонной оценки вероятности реализации угроз.
3. Разработана частная модель угроз информационной безопасности в системе дистанционного банковского обслуживания, учитывающая специфику обработки персональных данных в рассмотренной кредитной организации.
4. На основе построенных моделей произведен расчет общего уровня риска и оптимального объема инвестиций в обеспечение безопасности системы дистанционного банковского обслуживания.

IV. ОСНОВНЫЕ ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

Журналы, рекомендованные ВАК для публикации научных работ:

1. Собакин И.Б. Характеристика современных международных стандартов по управлению рисками информационной безопасности // Проблемы информационной безопасности. Компьютерные системы. №4, 2010. – 0,5 п.л.

2. Собакин И.Б. Идентификация активов как ключевых факторов риска информационной безопасности // Вопросы защиты информации. №2, 2011. – 0,5 п.л.

3. Собакин И.Б. Эволюция стандартов в области управления рисками информационной безопасности // Информационные системы и технологии. №3, 2011. – 0,6 п.л.

4. Собакин И.Б. Анализ подходов к определению оптимального объема инвестиций в информационную безопасность // Труды ИСА РАН: Информационные технологии. Численные методы решения. Математические модели социально-экономических процессов. Управление рисками и безопасностью. Динамические системы. Т.62. Вып.3, 2012. – 0,4 п.л.

Другие издания:

5. Собакин И.Б. Разработка математической модели оптимизации затрат на обеспечение информационной безопасности организаций кредитно-финансовой системы // Организация и направления научно-исследовательской работы студентов (направление 090900 «Информационная безопасность»). Выпуск 2. Сборник научных статей / Под ред. проф. Лося В.П., проф. Масленникова Д.П., доц. Федорова Н.В. М.: МГИУ, 2013. – 0,6 п.л., лично авт. 0,5 п.л.

6. Собакин И.Б. Оценка рисков и расчет оптимального объёма инвестиций в информационную безопасность системы дистанционного

банковского обслуживания // Организация и направления научно-исследовательской работы студентов (направление 090900 «Информационная безопасность»). Выпуск 2. Сборник научных статей / Под ред. проф. Лося В.П., проф. Масленникова Д.П., доц. Федорова Н.В. М.: МГИУ, 2013. – 0,4 п.л., лично авт. 0,3 п.л.

7. Собакин И.Б. Системный подход к управлению рисками информационной безопасности // Актуальные проблемы современной науки – М.: Издательство «Спутник+», №3, 2013. – 0,2 п.л.

8. Собакин И.Б. Риск-ориентированный подход к обеспечению информационной безопасности // Экономика. Управление. Право. – М.: ИНГН, №4 (40), 2013. – 0,3 п.л.

9. Собакин И.Б. Процессная модель управления рисками информационной безопасности // Вопросы экономических наук – М.: «Спутник+», №3, 2013. – 0,2 п.л.

СОБАКИН ИВАН БОРИСОВИЧ

МОДЕЛИРОВАНИЕ ПРОЦЕССА АНАЛИЗА И ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ

Автореферат

Подписано в печать 11.10.13
Формат бумаги 60×84/16
Усл. печ. л. 2,0. Уч.-изд. л. 2,0. Тираж 100. Заказ № 299

Издательство МГИУ, 115280, Москва, Автозаводская, 16
www.izdat.msiu.ru; e-mail: izdat@msiu.ru; тел. (495) 276-33-67

Отпечатано в типографии издательства МГИУ