«ОЦЕНКА РИСКА НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРИМЕРЕ БАНКА»

Казаков Павел Михайлович
Студент 2 курса, факультет «Информационные системы и технологии»
МИРЭА – Российский технологический университет, Россия, г. Москва

Аннотация

Опираясь на междисциплинарный анализ произошло формирование перечня, касающихся рисков безопасности информационной деятельности банковских организаций.

Такие составляющие вполне могут быть использованы с целью построения модели угроз для многих банков. Модели угроз в основных методиках по оценке количественной эффективности систем, относящихся к информационной безопасности, а также в оценках влияния степени информационной безопасности на эффективную деятельность банковских организаций.

В данной статье разобрана научно-практическое значение по разработке методов оценки роли, а также значения систем по информационной безопасности. В полной мере раскрыты как содержание, так и сущность существующей связи, касающейся эффективности действий банка, а также принимаемыми мерами по информационной безопасности.

Особое внимание обращено на объективность оценок риска, которые способны позволить не только выстроить системно работу в банковской сфере, касающуюся информационной безопасности, но также и привлечь особое внимание руководящих должностей этого банка к данному вопросу. Ведь создание эффективных систем по информационной безопасности в наши дни нуждается как в финансовой поддержке, так и в поддержке, исходящей со стороны учредителей банка, а также других руководителей, директоров, органов по исполнению.

Annotation

Based on an interdisciplinary analysis, a list was compiled concerning the security risks of information activities of banking organizations.

Such components may well be used to build a threat model for many banks. Threat models in the main methods for assessing the quantitative effectiveness of systems related to information security, as well as in assessing the impact of information security on the effective operation of banking organizations.

This article discusses the scientific and practical importance of developing methods for assessing the role, as well as the importance of information security systems. Both the content and the essence of the existing connection regarding the effectiveness of the bank's actions, as well as the measures taken on information security, are fully disclosed.

Special attention is paid to the objectivity of risk assessments, which are capable of allowing not only to systematically work in the banking sector regarding information security, but also to draw special attention to the management positions of this bank on this issue. After all, the creation of effective information security systems today needs both financial support and support coming from the founders of the bank, as well as other managers, directors, and enforcement agencies.

Ключевые слова: безопасность, банковская сфера, финансы, эффективность, устойчивость, показатели, эксперт, ориентиры, деятельность, информация, сущность, программа, количество, информатизация, специалист, источник, система, стоимость, анализ, проблема, должность.

Key words: safety, banking, finance, efficiency, sustainability, indicators, expert, benchmarks, activity, information, essence, program, quantity, informatizaion, specialist, source, system, cost, analysis, problem, position.

Необходимость оценки эффективности мер информационной безопасности

Многие специалисты банковской сферы утверждают, что наличие в кредитной организации систем информационной безопасности является важным параметром, это происходит из-за того, что риски информационной безопасности способны значительно затруднить банковскую деятельность. Наряду с этим, в наши дни остается открытым вопрос, касающийся облику систем, его составе и программного обеспечения, так как стоимость систем информационной безопасности способно достигать порядка 20 процентов стоимости всей информационной системы банка.

Учитывая это, можно утверждать, что создание систем информационной безопасности требует значительные финансовые вложения, а это в свою очередь должно быть обосновано надлежащим образом в вышестоящих инстанциях. В современном мире данный метод аргументирования специалистами информационной безопасности банков практически отсутствует. Создание бюджета подразделений информационной безопасности, а также построение систем информационной безопасности производится, практически всегда, не вникая в глубокий научный анализ.

Обычно, финансовые возможности банка, опыт использования систем информационной безопасности, компетенции руководящих должностей служб безопасности, а также рекламные усилия компании, продвигающие системы информационной безопасности на рынке, являются определяющими. Учитывая широкое распространение проблемы информационной безопасности, в научных источниках проблема количественной оценки мер влияния информационной безопасности на эффективность деятельности банков не нашла широкого освещения.

Прежде чем создать систему информационной безопасности банка, необходимо сделать оценку эффективности ее предстоящей деятельности по параметру «эффективность – стоимость». Это происходит по причине того, что архитектура, оснащение техники, ПО, а также сама стоимость системы информационной безопасности регионального банка и банка, имеющего федеральное значение, будут значительно различаться. В данной связи также важным является факт создания методики оценки эффективности системы информационной безопасности.

Анализ рисков информационной безопасности

Опираясь на Методику ЦБ РФ, которая касается оценки рисков нарушения информационной безопасности (РС БР ИББС-2.2-2009), выделены 7 групп, которые насчитывают 40 рисков информационной безопасности, которые в свою очередь зависят от различных причин или же источников возникновения.

При формировании перечня рисков информационной безопасности, требуется учитывать факторы, способствующие созданию рисков, а также влияющих на уровень защиты информации (ГОСТ-Р 51275- 99 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию»), а они в свою очередь, градируются на классы: объективные и субъективные, внутренние и внешние.

Во время решения задач с целью обеспечения информационной безопасности, обеспечению безопасности персональных данных придается особое значение, которые делятся на 4 категории в соответствии с Федеральным законом «О персональных данных»:

1. персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;
2. персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию;
3. персональные данные, позволяющие идентифицировать субъекта персональных данных;
4. обезличенные или общедоступные персональные данные.

Согласно Отраслевой частной модели угроз безопасности персональных данных (Рекомендации Центрального Банка Российской Федерации РС БР ИББС-2.4-2010), эти риски классифицируются по направлениям или же объектам воздействия.

Заключение

Опираясь на дисциплинарный анализ, разработан перечень, который состоит из 50 рисков информационной безопасности. Данный перечень можно использовать в практической деятельности банка, так как нейтрализация рисков информационной безопасности составляет сущность, а также содержание процесса обеспечения информационной безопасности банка.

На основе данного перечня также могут быть сформированы и модели угроз, опираясь на анализ которых, осуществляется постановка задач для создания систем информационной безопасности. Также, перечень конкретных рисков, возможно, использовать во время оценки влияния принимаемых мер информационной безопасности на эффективность деятельности банка.

Банковская сфера является главным заказчикам систем информационной безопасности, ведь банк – это практическая самая часто принимающая на себя удары мошенников и хакеров сфера человеческой деятельности в современном мире.

Список использованных источников

1. Федеральный закон «О безопасности» 390-ФЗ от 28.12.2010.
2. Федеральный закон «О банках и банковской деятельности» 395-1 от 02.12.1990.
3. Петенко С.А., Терехова Е.М. Оценка затрат на защиту информации // Защита информации. – 2005 г.
4. Конев И. Практическая оценка информационных рисков. Директор ИС. 15.09.2008. http://www.osp.ru/cio/2007/09/4370713 10
5. Сертификация по ISO 27001. Перевод. Информационная безопасность. http://dorlov.blogspot.ru/2011/06/iso-27001.html
6. ГОСТ-Р 51275-99. Защита информации. Объект информатизации.