УДК 621.34

МЕТОД ОЦЕНКИ РИСКОВ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКОВСКИХ УЧРЕЖДЕНИЙ

Д.В. СЕМЁНОВ, Ф.Л. ДЕМЧЕНКО

Предлагается метод оценки рисков нарушения информационной безопасности на основе опроса кадрового состава предприятия по трем направлениям: текущий уровень информационной безопасности организации; оценка системы управления информационной безопасностью организации; оценка уровня осознания руководством необходимости обеспечения информационной безопасности организации

Ключевые слова: критерий безопасности, оценка рисков, безопасность банковских учреждений.

ВВЕДЕНИЕ

Работа банковских систем вплотную связана с необходимостью постоянно держать в безопасности циркулирующую там информацию. Если говорить о банковской системе, определенно речь идет о крупномасштабной инфраструктуре, каждый элемент которой нуждается в определенной степени защиты. Однако максимально возможная защита всей системы является чрезмерно дорогостоящим мероприятием, и тут встает вопрос оценки рисков. Оценка рисков представляет собой комплексное изучение системы. Результатом оценки рисков является итоговый уровень информационной безопасности организации.

Методика оценки соответствия информационной безопасности организаций банковской системы используется для проведения аудита и оценки уровня обеспечения информационной безопасности организаций, осуществляющих деятельность в банковской сфере [1]. Целью методики является проведение оценки рисков информационной безопасности по направлениям:

- текущий уровень информационной безопасности организации($EV1$);
- менеджмент информационной безопасности организации($EV2$);
- уровень осознания информационной безопасности организации($EV3$).

1. ГРУППОВЫЕ И ЧАСТНЫЕ ПОКАЗАТЕЛИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. СПОСОБЫ ОЦЕНИВАНИЯ ПОКАЗАТЕЛЕЙ

Для оценки информационной безопасности организации используются групповые и частные показатели [2]. Групповые показатели образуют структуру направлений оценки. Оценки групповых показателей (EV_{Mi}) используются для получения оценки по направлениям ($EV1$, $EV2$ и $EV3$). Частные показатели входят в состав групповых показателей и представлены в виде вопросов, ответы на которые дают возможность определить оценки (EV_{Mij}), которые затем формируют оценки EV_{Mi} групповых показателей.

Для проведения оценки используются формы, содержащие вопросы, групповой показатель, входящие в него частные показатели и их категории (обязательность выполнения), метрику (шкалу) для оценивания частных показателей и коэффициенты значимости частных показателей, используемые при вычислении группового показателя.

Оценка EV_{Mij} частного показателя формируется на основании выявленной аудиторской группой степени выполнения требований посредством экспертного оценивания.

При проведении оценки частных показателей используется шкала оценивания, представленная в табл. 1.1, 1.2, 1.3.

Таблица 1.1

Критерии оценки частных показателей для оценки «степени документированности» и «выполнения требований информационной безопасности»

Оценка частного показателя	Критерий выставления оценки частного показателя
0	Требования частного показателя не установлены во внутренних нормативных документах проверяемой организации и не выполняются
0	Требования частного показателя частично установлены в нормативных документах проверяемой организации, но не выполняются
0,25	Требования частного показателя полностью установлены в нормативных документах проверяемой организации, но не выполняются
0,25	Требования частного показателя не установлены во внутренних нормативных документах проверяемой организации и выполняются в неполном объеме
0,25	Требования частного показателя частично установлены во внутренних нормативных документах проверяемой организации и выполняются в неполном объеме
0,5	Требования частного показателя полностью установлены во внутренних нормативных документах проверяемой организации и выполняются в неполном объеме
0,5	Требования частного показателя не установлены во внутренних нормативных документах проверяемой организации, но выполняются в полном объеме

0,75	Требования частного показателя частично установлены во внутренних нормативных документах проверяемой организации, но выполняются в полном объеме
1	Требования частного показателя полностью установлены во внутренних нормативных документах проверяемой организации и выполняются в полном объеме

Таблица 1.2

Критерии выставления оценок частных показателей для оценки «степени документированности требований информационной безопасности»

Оценка частного показателя	Критерий выставления оценки частного показателя
0	Требования частного показателя не установлены во внутренних нормативных документах проверяемой организации
0,5	Требования частного показателя частично установлены в нормативных документах проверяемой организации
1	Требования частного показателя полностью установлены в нормативных документах проверяемой организации

Таблица 1.3

Критерии выставления оценок частных показателей для оценки «степени выполнения требований информационной безопасности»

Оценка частного показателя	Критерий выставления оценки частного показателя
0	Требования частного показателя не выполняются
0,5	Требования частного показателя выполняются в неполном объеме
1	Требования частного показателя выполняются в полном объеме

2. ОЦЕНКА ТЕКУЩЕГО УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Оценка текущего уровня информационной безопасности организации определяется совокупностью групповых показателей, позволяющих оценить степень выполнения требований (табл. 2).

Таблица 2

Перечень требований для оценки текущего уровня ИБ организации

Обозначение группового показателя	Наименование группового показателя (требование)
М1	Обеспечение ИБ при назначении и распределении ролей и обеспечении доверия к персоналу
М2	Обеспечение ИБ на стадиях жизненного цикла АС
М3	Обеспечение ИБ при управлении доступом и регистрацией
М4	Обеспечение ИБ средствами антивирусной защиты
М5	Обеспечение ИБ при использовании ресурсов сети Интернет
М6	Обеспечение ИБ при использовании средств криптографической защиты информации
М7	Обеспечение ИБ банковских платежных технологических процессов
М8	Обеспечение ИБ банковских информационных технологических процессов
М9	Обработка персональных данных в организации
М10	Обеспечение ИБ банковских технологических процессов, в рамках которых обрабатываются персональные данные

Оценка группового показателя текущего уровня ИБ организации (EV_{Mi}) вычисляется из оценок входящих в него частных показателей (EV_{Mij}) с учетом коэффициентов значимости α_{ij}, определяющих важность частного показателя для оценивания группового показателя:

$$EV_{Mi} = \sum_j \alpha_{ij} * EV_{Mij} \,. \qquad (1)$$

При формировании коэффициентов значимости учитывается следующее условие нормировки:

$$\sum_{j=1}^{k} \alpha_{ij} = 1 \,, \qquad (2)$$

где k — число частных показателей в i-м групповом показателе.

Оценка степени выполнения требований безопасности, регламентирующих банковский информационный технологический процесс $EV_{\text{БИТП}}$ вычисляется по формуле принимая во внимание результаты оценивания групповых показателей $M1$-$M6$:

$$EV_{\text{БИТП}} = \frac{\sum_i EV_{Mi} + EV_{M8}}{7}, i = 1 \div 6 \qquad (3)$$

Оценка степени выполнения требований безопасности, регламентирующих защиту персональных данных в информационных системах персональных данных $EV^1_{\text{ОЗПД}}$, без учета требований при использовании средств криптографической защиты информации вычисляется по формуле:

$$EV^1 = \frac{\sum_i EV_{Mi} + EV_{M8} + EV_{M10}}{7}, i = 1 \div 5 \,. \qquad (4)$$

Оценка степени выполнения требований, регламентирующих защиту персональных данных $EV^2_{\text{ОЗПД}}$, с учетом оценки степени выполнения требований при использовании криптографической защиты информации вычисляется по формуле:

$$EV^2_{\text{ОЗПД}} = \frac{\sum_i EV_{Mi} + EV_{M8} + EV_{M10}}{8}, i = 1 \div 6 \,. \qquad (5)$$

3. ОЦЕНКА МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Организация должна вводить, выполнять, использовать, контролировать, пересматривать, поддерживать и совершенствовать документированные положения системы управления информационной безопасностью в рамках всей бизнес-деятельности организации, а также рисков, с которыми она сталкивается.

Данные требования, обеспечиваются с помощью процесса, который основывается на модели «Планирование – реализация – оценка - корректировка» (рис. 1).

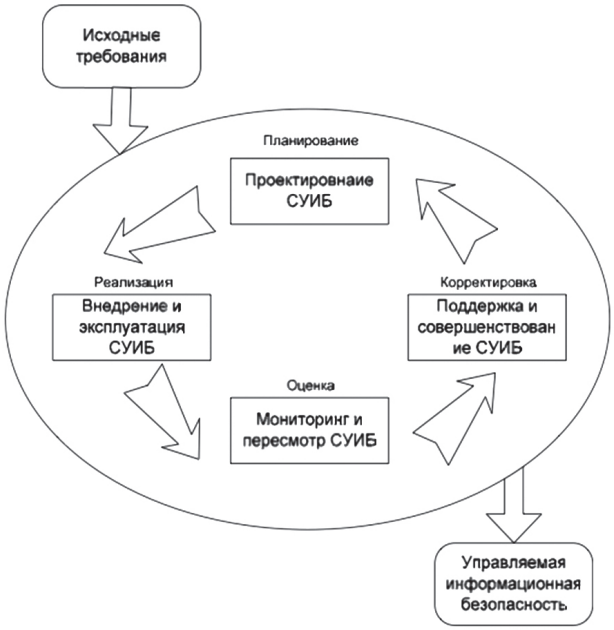

Рис. 1. Модель «Планирование – реализация – оценка – корректировка»

Оценка менеджмента информационной безопасности организации определяется совокупностью групповых показателей, позволяющих оценить степень соблюдения данных требований.

Таблица 3

Перечень требований для оценки менеджмента ИБ организации

Обозначение группового показателя	Наименование группового показателя (требование)
M11	Организация и функционирование службы ИБ организации
M12	Определение/коррекция области действия системы обеспечения информационной безопасности (СОИБ)
M13	Выбор/коррекция подхода к оценке рисков нарушения ИБ и проведение оценки рисков нарушения ИБ
M14	Разработка планов обработки рисков нарушения ИБ
M15	Разработка/коррекция внутренних документов, регламентирующих деятельность в области обеспечения ИБ
M16	Принятие руководством организации решений о реализации и эксплуатации СОИБ
M17	Организация реализации планов внедрения СОИБ
M18	Разработка и организация реализации программ по обучению и повышению осведомленности в области ИБ
M19	Организация обнаружения и реагирования на инциденты безопасности
M20	Организация обеспечения непрерывности бизнеса и его восстановления после прерываний
M21	Мониторинг и контроль защитных мер
M22	Проведение самооценки ИБ
M23	Проведение аудита ИБ
M24	Анализ функционирования СОИБ
M25	Анализ СОИБ со стороны руководства организации
M26	Принятие решений по тактическим улучшениям СОИБ
M27	Принятие решений по стратегическим улучшениям СОИБ

Итоговая оценка $EV2$, отражающая степень выполнения требований по направлению “менеджмент информационной безопасности организации”, вычисляется по формуле:

$$EV2 = \frac{\sum_{i=11}^{27} EV_{Mi}}{17}. \qquad (6)$$

4. ОЦЕНКА УРОВНЯ ОСОЗНАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Оценка уровня осознания информационной безопасности организации определяется совокупностью групповых показателей, позволяющих оценить степень выполнения требований для следующих областей (см. табл. 4).

Таблица 4

Перечень требований для оценки уровня осознания ИБ организации

Обозначение группового показателя	Наименование группового показателя (требование)
M28	Оценка деятельности руководства организации по поддержке функционирования службы ИБ организации
M29	Оценка деятельности руководства организации по принятию решений о реализации и эксплуатации СОИБ
M30	Оценка деятельности руководства организации по поддержке планирования СОИБ
M31	Оценка деятельности руководства организации по поддержке реализации СОИБ
M32	Оценка деятельности руководства организации по поддержке проверки СОИБ

M33	Оценка деятельности руководства организации по анализу СОИБ
M34	Оценка деятельности руководства организации по поддержке совершенствования СОИБ

Итоговая оценка EV3, отражающая степень выполнения требований по направлению “уровень осознания ИБ организации”, вычисляется по формуле:

$$EV3 = \frac{\sum_{i=28}^{34} EV_{Mi}}{7}. \quad (7)$$

5. ОПРЕДЕЛЕНИЕ УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКОВСКОЙ ОРГАНИЗАЦИИ. ОТОБРАЖЕНИЕ ОЦЕНОК

Если оценка *EV*1, *EV*2 или *EV*3 лежит в интервале от 0 до 0,25, то данному направлению оценки присваивается нулевой уровень обеспечения информационной безопасности.

Если оценка *EV*1, *EV*2 или *EV*3 лежит в интервале от 0,25 до 0,5, то данному направлению оценки присваивается первый уровень обеспечения информационной безопасности.

Если оценка *EV*1, *EV*2 или *EV*3 лежит в интервале от 0,5 до 0,7, то данному направлению оценки присваивается второй уровень обеспечения информационной безопасности.

Если оценка *EV*1, *EV*2 или *EV*3 лежит в интервале от 0,7 до 0,85, то данному направлению оценки присваивается третий уровень обеспечения информационной безопасности.

Если оценка *EV*1, *EV*2 или *EV*3 лежит в интервале от 0,85 до 0,95, то данному направлению оценки присваивается четвертый уровень обеспечения информационной безопасности.

Если оценка *EV*1, *EV*2 или *EV*3 лежит в интервале от 0,95 до 1 включительно, то данному направлению оценки присваивается пятый уровень обеспечения информационной безопасности.

Итоговый уровень обеспечения информационной безопасности - Значение *R* определяется по наименьшему значению из трех оценок по направлениям оценки:

- оценки уровня осознания информационной безопасности организации (*EV*3);
- оценки менеджмента информационной безопасности организации (*EV*2);
- оценки текущего уровня информационной безопасности организации (*EV*1).

Полученное в результате оценки соответствия организации уровню обеспечения информационной безопасности, значение *R* является основой для формирования аудиторского заключения по результатам аудита информационной безопасности.

Чем больше значение *R*, тем соответствующий этому значению уровень обеспечения информационной безопасности организации выше.

Для отображения результатов оценивания используется круговая диаграмма (см. рис. 3.2).

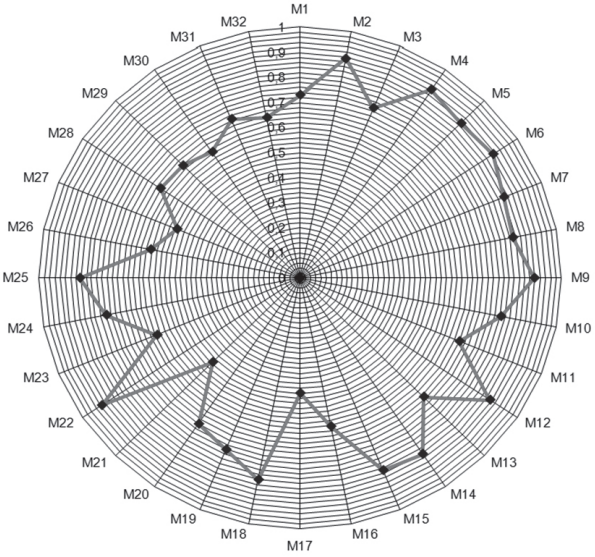

Рис. 2. Круговая диаграмма для отображения результатов оценивания

Секторы с 1-го по 10-й используются для отображения оценки текущего уровня обеспечения информационной безопасности организации.

Секторы с 11-го по 27-й используются для отображения оценки процессов менеджмента информационной безопасности организации.

Секторы с 28-го по 34-й используются для отображения оценки уровня осознания информационной безопасности организации.

ЗАКЛЮЧЕНИЕ

В данной статье предложен метод оценки состояния информационной безопасности банковской организации. Оценка уровня информационной безопасности проводилась по трем направлениям: текущий уровень информационной безопасности организации; оценка системы управления информационной безопасностью организации; оценка уровня осознания руководством необходимости обеспечения информационной безопасности организации. Проведенные работы показали, что целесообразным является проведение оценки не только текущего уровня информационной безопасности организации, но и проведение оценки осознания необходимости обеспечения информационной безопасности, а также оценки системы управления информационной безопасностью организации. Предлагаемая методика оценки рисков характеризуется высокой гибкостью применения и глубиной раскрытия, как частных, так и групповых показателей информационной безопасности. Данная методика может быть использована специалистами, проводящими аудит информационной безопасности банковских учреждений.

В целом рассмотренные в данной статье вопросы позволяют оценить уровень текущего состояния защищенности информационных

ресурсов предприятия, а также выработать рекомендации по обеспечению (повышению) информационной безопасности, в том числе снизить потенциальные потери предприятия путем повышения устойчивости функционирования, автоматизированной системы, разработать концепцию и политику безопасности компании. Предлагаемая методика оценки рисков информационной безопасности банковской организации позволяет сформировать меры защиты конфиденциальной информации компании.

Литература

[1] *С.А. Петренко, С.В. Симонов.* Анализ и управление информационными рисками. – ДМИ Пресс, 2004.

[2] *Белкин А.Р., Левин М.Ш.* Принятие решений: комбинаторные модели апроксимации информации. – М.: Наука, 1990.

Поступила в редколлегию 17.04.2012

Семёнов Дмитрий Владимирович, магистрант кафедры БИТ ХНУРЭ. Область научных интересов: управление информационной безопасностью.

Демченко Фёдор Леонидович, магистрант кафедры БИТ ХНУРЭ. Область научных интересов: защита информации в информационно-телекоммуникационных системах.

УДК 621.34

Метод оцінки ризиків порушення інформаційної безпеки банківських закладів / С.Г. Семенов, Ф.Л. Демченко // Прикладна радіоелектроніка: наук.-техн. журнал. – 2012. – Том 11. № 2. – С. 304–308.

Пропонується метод оцінки ризиків порушення інформаційної безпеки на основі опитування кадрового складу підприємства за трьома напрямками: поточний рівень інформаційної безпеки організації; оцінка системи управління інформаційною безпекою організації; оцінка рівня усвідомлення керівництвом необхідності забезпечення інформаційної безпеки організації.

Ключові слова: критерій безпеки, оцінка ризиків, безпека банківських установ.

Табл. 06. Іл. 02. Бібліогр.: 2 найм.

UDC 621.34

Method of evaluating risks of violating information security of banking establishments / D.V. Semenov, F.L. Demchenko // Applied Radio Electronics: Sci. Journ. – 2012. Vol. 11. № 2. – P. 304–308.

The paper suggests a method of evaluating risks of information security violation on the basis of questioning an enterprise's personnel in three directions: current level of an organization's information security; evaluating a control system of an organization's information security; evaluating the level of the governing body's realization of the need for ensuring the organization's info security.

Keywords: security criterion, evaluation of risks, security of banking establishments.

Tab. 06. Fig. 06. Ref.: 2 items.