МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ОБЕСПЕЧЕНИЯ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ КРЕДИТНО-ФИНАНСОВОЙ СФЕРЫ

Козьминых С.И.¹

Аннотация: В работе представлена методика формирования комплексного подхода к обеспечению информационной безопасности объектов кредитно-финансовой сферы. Рассмотрены основные принципы обеспечения комплексной безопасности объекта информатизации кредитно-финансовой сферы. Отмечено, что при проектировании системы обеспечения комплексной безопасности объекта информатизации кредитно-финансовой сферы, необходимо провести выбор направлений и принципов ее реализации. Приведено математическое моделирование уровня комплексной безопасности объектов информатизации кредитно-финансовой сферы с использованием теории вероятностей, целью которого является получение функциональной зависимости для нахождения численного значения коэффициента уязвимости, оценивающего уровень комплексной безопасности объекта кредитно-финансовой сферы. Процесс математического моделирования разбит на пять этапов, в итоге которого получены составляющие и сама формула коэффициента уязвимости объекта информатизации, которые определяются с помощью математической обработки статистических данных и проведения экспертных опросов. В качестве вывода заключается, что разработанный математический аппарат позволяет получить количественную оценку как существующего, так и прогнозируемого уровня уязвимости объекта информатизации. Кроме того отмечена возможность данного математического подхода для оценки уровня комплексной безопасности объекта информатизации кредитно-финансовой сферы.

Ключевые слова: формирования комплексного подхода к обеспечению информационной безопасности, угроза информационной безопасности объекту кредитно-финансовой сферы, принципы обеспечения комплексной безопасности объекта информатизации, статистические вероятности, экспертные оценки, единый динамический коэффициент возникновения угрозы, коэффициент ущерба, коэффициент уязвимости.

DOI: 10.21681/2311-3456-2018-1-54-63

Введение

Для реализации комплексного подхода к решению проблемы обеспечения информационной безопасности объектов кредитно-финансовой сферы необходимо использование таких научных методов, как моделирования систем и процессов защиты информации. Целями такого моделирования являются поиск оптимальных решений по управлению системой защиты информации, оценка эффективности использования различных механизмов защиты, определение свойств системы защиты, установление взаимосвязей между ее характеристиками и показателями.

Известно, что модель представляет собой логическое или математическое описание компонентов и функций, отображающих свойства моделируемого объекта или процесса и используется как

условный образ, сконструированный для упрощения их исследования.

Моделирование системы защиты информации заключается в ее формализованном отображении в каком-либо виде, адекватном исследуемой системе, и получении с помощью построенной модели необходимых характеристик реальной системы. Таким образом, весь процесс моделирования можно разделить на две составляющие: построение модели и реализацию модели с целью получения необходимых характеристик системы защиты информации.

Часто для определения показателей безопасности информации достаточно знать вероятностные характеристики угроз и возможную эффективность механизмов защиты. Получение таких характеристик, хотя и затруднено, тем не менее, не

¹ Козьминых Сергей Игоревич доктор технических наук, Финансовый университет при Правительстве Российской Федерации, г. Москва, Россия. E-mail: SIKozminykh@fa.ru

является неразрешимой задачей. Однако игнорирование взаимовлияния угроз и средств защиты, а также невозможность определения ожидаемого ущерба от воздействия различных факторов и ресурсов, необходимых для обеспечения защиты, дает возможность использовать методы моделирования в основном для общих оценок при определении степени того внимания, которое должно быть уделено проблеме защиты информации на объекте кредитно-финансовой сферы.

Прежде чем перейти к описанию математической модели обеспечения комплексной безопасности объекта кредитно-финансовой сферы, следует определить, в чем же заключается комплексный подход к обеспечению информационной безопасности.

1. Комплексный подход к обеспечению информационной безопасности объектов кредитно-финансовой сферы

Для того чтобы понять суть комплексного подхода к обеспечению информационной безопасности объектов кредитно-финансовой сферы предлагается перейти к рассмотрению классификации основных направлений обеспечения комплексной безопасности объекта информатизации рис.1.

Зарубежный и отечественный опыт обеспечения безопасности свидетельствует, что для борьбы с потенциально возможными и реально возникающими угрозами необходима стройная и целенаправленная организация процесса противодействия. При этом реализация этого процесса должна включать использование всех возможных сил и средств защиты с целью недопущения, пресечения и оперативной ликвидации последствий нештатных ситуаций и чрезвычайных происшествий. То есть процесс защиты от всевозможных угроз должен иметь комплексный характер.

Предлагаемый перечень основных направлений обеспечения комплексной безопасности объектов информатизации кредитно-финансовой сферы наглядно демонстрирует, что если, например, пожарную, охранную, техногенную и другие виды безопасности можно обеспечить независимо друг от друга, то информационную безопасность можно надежно обеспечить только при условии реализации всех указанных на (рис. 1) направлений.

Вместе с тем для некоторых объектов информатизации кредитно-финансовой сферы не все направления обеспечения комплексной безопасности могут быть не актуальны. Например, если объект находится благоприятной климатической зоне и не ведет какую-либо производственную де-

ятельность, то соответствующими направлениями безопасности можно пренебречь.

Чаще всего на объектах информатизации кредитно-финансовой сферы, бывают наиболее актуальны такие направления обеспечения безопасности, как:

- охранный безопасность;
- информационная безопасность;
- пожарная безопасность;
- экономическая безопасность;
- юридическая безопасность;
- безопасность трудовой деятельности (охрана труда).

При выборе необходимых направлений обеспечения комплексной безопасности объекта информатизации кредитно-финансовой сферы необходимо руководствоваться результатами анализа рисков, которым он может быть подвержен, а также анализом элементов защиты, представляющими наибольшую ценность для всего объекта.

Кроме того, при формировании системы обеспечения комплексной безопасности объекта информатизации кредитно-финансовой сферы необходимо определить, в соответствии с какими принципами она будет создаваться. Основными принципами обеспечения комплексной безопасности объекта информатизации кредитно-финансовой сферы должны быть:

Комплексность. Обеспечение безопасности всех наиболее значимых элементов защиты и объекта в целом от различных видов угроз всеми возможными способами и средствами.

Своевременность. Предполагает постановку задач по обеспечению комплексной безопасности объекта информатизации кредитно-финансовой сферы на ранних стадиях проектирования путем разработки системы обеспечения комплексной безопасности на основе анализа и прогнозирования возможных угроз безопасности.

Непрерывность. Постоянное соблюдение мер обеспечения комплексной безопасности в процессе функционирования объекта информатизации кредитно-финансовой сферы, а также осуществление контроля по их выполнению.

Активность. Меры обеспечения информационной безопасности должны иметь упреждающий характер. Необходимо в первую очередь разрабатывать и внедрять меры обеспечения безопасности, не допускающие возникновения угроз на объекте и пресекающие их в момент возникновения. На объекте должно быть обеспечено маневрирование силами и средствами обеспечения безопасности, использование нестандартных мер защиты.

Рис. 1. Классификация основных направлений обеспечения комплексной безопасности объекта информатизации

Целенаправленность. Реализация мер обеспечения безопасности, направленных на защиту объекта информатизации кредитно-финансовой сферы от конкретных, наиболее вероятных угроз его безопасности, способных причинить наибольший ущерб.

Универсальность. Использование таких мер, которые способны защитить объект от наибольшего количества наиболее вероятных и опасных угроз его безопасности.

Надежность. Обеспечивается использование таких мер безопасности, которые способны обеспечить максимально возможное (эффективное) противодействие дестабилизирующим факторам (угрозам);

Законность. Предполагает разработку системы обеспечения комплексной безопасности объекта информатизации кредитно-финансовой сферы на основе федерального законодательства и других действующих нормативных актов в области обеспечения безопасности. Необходима гармонизация норм, требований и правил обеспечения комплексной безопасности объекта информатизации кредитно-финансовой сферы с нормами безопасности Российской Федерации и международными нормами.

Обеспечение баланса интересов общества, государства, хозяйствующих объектов, потребителей при обеспечении комплексной безопасности объекта информатизации кредитно-финансовой сферы.

Обоснованность. Предлагаемые меры и средства защиты объекта информатизации кредитно-финансовой сферы должны реализовываться в соответствии с современным уровнем развития науки и техники, быть обоснованными с точки зрения заданного уровня безопасности и соответствовать установленным требованиям и нормам.

Экономическая целесообразность. Обеспечивается сопоставимостью возможного ущерба и затрат на обеспечение безопасности. Необходимо руководствоваться критерием эффективности – стоимость.

Специализация. Предполагает привлечение к разработке, внедрению мер и средств защиты на объектах информатизации кредитно-финансовой сферы специализированных организаций, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Эксплуатация технических средств и реализация мер безопасности должны осуществляться профессионально подготовленными специалистами.

Взаимодействие и координация. Предполагает осуществление мер обеспечения безопасности на основе четкого взаимодействия всех заинтересованных подразделений и служб объекта, сторонних специализированных организаций в этой области, а также интеграцию с правоохранительными органами и органами государственного управления.

Централизация управления. Предполагает самостоятельное функционирование подсистем безопасности объекта информатизации кредитно-финансовой сферы по единым организационным, функциональным и методологическим принципам с централизованным управлением деятельностью всей системы обеспечения комплексной безопасности.

Совершенствование. Предусматривает постоянное совершенствование методов, мер и средств обеспечения безопасности объектов на основе собственного опыта, научных достижений, нормативно-технических требований, накопленного отечественного и зарубежного опыта.

Планирование. Предполагает рациональное распределение ресурсов в процессе обеспечения комплексной безопасности объекта информатизации кредитно-финансовой сферы.

Ответственность должностных лиц за выполнение конкретных мер по обеспечению комплексной безопасности объекта информатизации кредитно-финансовой сферы.

Приоритет в обеспечении комплексной безопасности объекта информатизации кредитно-финансовой сферы должен отдаваться охране жизни и здоровья людей, защите конфиденциальной информации.

Таким образом, при проектировании системы обеспечения комплексной безопасности объекта информатизации кредитно-финансовой сферы, необходимо провести выбор направлений и принципов ее реализации. Эти же направления и принципы необходимо заложить в концепцию обеспечения комплексной безопасности объекта информатизации кредитно-финансовой сферы, которая служит основой создания системы обеспечения комплексной безопасности.

2. Использование теории вероятностей для математического моделирования уровня комплексной безопасности объектов информатизации кредитно-финансовой сферы

Существует два варианта создания системы информационной безопасности объектов кредитно-финансовой сферы:

1. Объект информатизации только создается – система информационной безопасности формируется «с нуля».

2. Объект информатизации уже функционирует – система информационной безопасности имеется, требуется повысить ее уровень за счет оптимизации мер защиты.

Для специалистов, работающих в области обеспечения информационной безопасности, проще создавать систему «с нуля» поскольку на первом этапе исключается анализ существующей системы безопасности. Но, к сожалению, чаще всего встречается второй вариант, когда руководители объекта информатизации не уделяют должного внимания безопасности до тех пор, пока не случается какое-либо чрезвычайное происшествие с серьезными последствиями. Тогда он готов на любые затраты, лишь бы этого не повторилось. Самое сложное в данной ситуации найти квалифицированных специалистов, которые смогли бы грамотно провести анализ существующей системы информационной безопасности, выявить причины по которым она дала сбой, разработать план мероприятий по её совершенствованию, провести оптимизацию затрат и наладить контроль за её эффективным функционированием.

Для решения первой из перечисленных задач - проведения анализа состояния системы информационной безопасности и в целом комплексной безопасности объектов кредитно-финансовой сферы, был разработан специальный математический аппарат определения коэффициента уязвимости объекта информатизации.

Цель: Получить функциональную зависимость для нахождения численного значения коэффициента уязвимости, оценивающего уровень комплексной безопасности объекта кредитно-финансовой сферы.

Исходные данные:

1. Статистические вероятности возникновения угроз с учетом региональной компоненты, периодом реализации угроз (данные МВД и МЧС РФ).

2. Экспертные оценки вероятности возникновения угроз.

3. Экспертные оценки подверженности угрозам элементов защиты.

4. Экспертные оценки возможных последствий и коэффициента ущерба от реализации каждой угрозы.

5. Экспертные оценки влияния мер по предотвращению угроз на этапе предупреждения.

6. Экспертные оценки влияния мер на этапе пресечения угроз.

7. Экспертные оценки влияния мер на этапе ликвидации последствий от реализации угроз.

Процесс математического моделирования обеспечения комплексной безопасности объекта кредитно-финансовой сферы включает шесть этапов.

На первом этапе необходимо определить единый динамический коэффициент возникновения угрозы. **Единый динамический коэффициент возникновения угрозы** - учитывает динамику статистического значения, само статистическое значение и вероятность возникновения данной угрозы, полученное экспертным путем. Обозначим его как $P^* \in [0;1]$.

Введем следующие обозначения:

$P_{СТАТ} \in [0;1]$ – статистическая вероятность возникновения угрозы;

$P_{ЭКСП} \in [0;1]$ – экспертная оценка вероятности возникновения угрозы;

$P_{СТАТ}^n$ – статистическая вероятность возникновения угрозы за n год, где $n = 1991, 1992, \dots, 2017$ год.

$\Delta \in [0;1]$ - динамическая составляющая.

Тогда:

$$P^* = P_{ЭКСП} (P_{СТАТ} + \Delta), \quad (1)$$

где:

$$\Delta = \begin{cases} P_{СТАТ}^{n-1} > P_{СТАТ}^n, & \left(\frac{P_{СТАТ}^{n-1} - P_{СТАТ}^n}{P_{СТАТ}^n} \right); \\ P_{СТАТ}^{n-1} \leq P_{СТАТ}^n, & \left(-\frac{P_{СТАТ}^{n-1} - P_{СТАТ}^n}{P_{СТАТ}^n} \right). \end{cases} \quad (2)$$

Используя значения вероятностей возникновения угроз, строится спектр угроз, производится ранжирование угроз по значимости, а также определяются пределы значимости, то есть уровень угроз, которые будут рассматриваться (рис. 2).

На этом рисунке выделены максимальный и минимальный пределы значимости, соответственно: $P'_{\max}$ и $P'_{\min}$, следующим образом:

- если $P_n^* \geq P'_{\max}$, то данная угроза P_n^* принимается к рассмотрению и имеет наивысший приоритет в плане ее предотвращения;

- если $P'_{\min} \geq P_n^* > P'_{\max}$, то данная угроза P_n^* принимается к рассмотрению и имеет средний приоритет;

- если $P_n^* > P'_{\min}$, то данной угрозой P_n^* можно пренебречь совсем, или установить низкий приоритет.

Таким образом, еще на начальном этапе, после анализа и оценки угроз можно произвести перво-

Рис.2. Спектр угроз. Пределы значимости угроз

начальную фильтрацию угроз, имеющих серьезное значение для данного объекта или предпринимательской деятельности.

На втором этапе необходимо определить элементы защиты объекта информатизации органа внутренних дел, подверженные воздействиям угроз, также определить коэффициент уязвимости объекта и построить гистограмму уязвимости объекта информатизации органа внутренних дел.

Под **уязвимостью** будем понимать свойство элемента защиты быть подверженным воздействию угроз (дестабилизирующим факторам). Количественной оценкой уязвимости является **коэффициент уязвимости**, который обозначается как $K_{\text{обс.ам}} \in [0,1]$, где $m = \overline{1, L}$ – количество элементов защиты.

Определяется величина $K_{\text{обс.ам}}$ экспертным путем.

Гистограмм уязвимости строятся по каждому элементу защиты. Рассматриваются следующие элементы защиты:

- персонал организации, посетители;
- материальные ценности, включая недвижи-

мость и транспортные средства;

- информация;
- финансовая деятельность (оказание услуг);
- экономическая деятельность;
- юридическая деятельность;
- инновационная деятельность.

Аналогично, как и для вероятностей возникновения угроз вводятся пределы значимости уязвимости, которые отображены на (рис. 3).

На третьем этапе необходимо определить последствия угроз и провести расчет коэффициента ущерба объекта информатизации органа внутренних дел.

В случаях, когда угроза реализуется, то есть наступает та или иная чрезвычайная ситуация в деятельности организации: грабеж, убийство, кража важной информации, несанкционированный доступ к конфиденциальным данным и т.п., следует рассматривать **последствия от реализации угроз**, то есть моральные, материальные, физические, информационные и другие потери, который несет объект кредитно-финансовой сферы.

Рис. 3. Гистограмма уязвимости. Пределы значимости уязвимости элементы защиты объекта информатизации

Оцениваются последствия конкретной i угрозы единым безразмерным параметром - **коэффициентом ущерба** от реализации соответствующей угрозы, которую обозначаем как $K_{ущij} \in [0,1]$, где $i = \overline{1, N}$ – номер рассматриваемой угрозы, $j = \overline{1, M}$ – номер возможного последствия соответствующей угрозы.

На четвертом этапе проводится определение риска, связи вероятности угрозы с коэффициентом ущерба, определение уровня риска и построение спектра рисков.

Риск - это вероятностная величина, определяемая в условиях возникновения ущерба, уменьшения прибыли и возникновения других возможных предполагаемых потерь в случае реализации угроз на объекте.

Под риском понимается производное выражение от двух величин: вероятности возникновения угрозы и коэффициента ущерба.

Количественное значение риска называется **уровнем риска** и обозначается $R_{ij} \in [0,1]$, где соответственно $i = \overline{1, N}$ – номер рассматриваемой угрозы, $j = \overline{1, M}$ – номер возможного последствия соответствующей угрозы.

$$R_{ij} = P_i^* \cdot K_{ущij} \quad (3)$$

После получения количественного значения уровней риска строится спектр рисков для элементов защиты объекта кредитно-финансовой сферы. Определяются уровни значений, по которым каждый риск соотносят с лингвистическими переменными, типа: очень опасно, опасно, достаточно опасно, и тому подобное, если оценка рисков проводится экспертами.

Это делается для определения пределов допустимого (приемлемого) риска. Под ним понимаются угрозы, последствия которых сохраняют работоспособность объекта кредитно-финансовой сферы и не приводят к серьезным потерям.

На четвертом этапе проводится оценка организационных и технических мероприятий по защите информации, расчет весовых коэффициентов защитных мероприятий, определяются этапы их проведения.

Противодействие угрозам, как уже было отмечено ранее, осуществляется комплексом организационных и технических мероприятий. К ним относятся все действия объекта кредитно-финансовой сферы, направленные на предупреждение, пресечение и ликвидацию последствий различного рода угроз.

Реализацию системы обеспечения информационной безопасности, как было представлено на модели процесса борьбы с противоправными действиями, направленными на защищаемую информацию можно поделить на три этапа:

1. Этап предупреждения. Время до возникновения угрозы: используются превентивные меры безопасности, проводится обучение и тренировки персонала объекта кредитно-финансовой сферы, службы безопасности объекта, внедряются инженерно-технические средства защиты объекта, такие как охранно-пожарная сигнализация, видеонаблюдение, системы контроля и управления доступом и другие.

2. Этап пресечения. Время реализации угрозы: используются меры по пресечению дестабилизирующих факторов, как правило, это меры оперативного реагирования.

3. Этап ликвидации последствий. Время после реализации угрозы: осуществляется оперативные действия «по горячим следам», проводятся аварийно-спасательные работы, используются оперативные планы выхода из кризисных ситуаций, подключаются резервные источники электропитания, восстанавливается потерянная информация и т.п.

Учитывается то, что каждое мероприятие может воздействовать не только на одну конкретную угрозу, а также то, что каждую угрозу может блокировать только набор мероприятий.

Также учитывается, что каждое мероприятие имеет различные преимущества на конкретном этапе, например, охранная сигнализация играет важную роль как средство обнаружения и не имеет принципиального значения при ликвидации последствий, если кража информации уже совершена. Поэтому каждое мероприятие представляется вектором с весовыми коэффициентами вклада по блокированию угроз на каждом этапе.

На пятом этапе необходимо определить коэффициент уязвимости объекта информатизации кредитно-финансовой сферы.

Принцип формирования составляющих коэффициента уязвимости объекта информатизации приведен на (рис. 4).

Коэффициент уязвимости объекта информатизации кредитно-финансовой сферы - это количественная оценка уровня безопасности объекта защиты на исследуемый момент времени в конкретных условиях его функционирования.

Рис. 4. Принцип формирования составляющих коэффициента уязвимости объекта информатизации кредитно-финансовой сферы

Значение коэффициента уязвимости будет рассчитываться следующим образом:

$$K_{\text{о} \beta \zeta \lambda} = \sum_{i=1}^N K_{\text{о} \beta \zeta \lambda i} \cdot \beta_i, \quad (4)$$

где $K_{\text{о} \beta \zeta \lambda i}$ – коэффициент уязвимости по i -ой угрозе;

β_i – весовой коэффициент угрозы по ее максимальному коэффициенту ущерба, определяется как:

$$\beta_i = \frac{\sum_j^M K_{\text{ущ}ij}}{\max_j \sum_j^M K_{\text{ущ}ij}}. \quad (5)$$

Значения коэффициента уязвимости объекта информатизации по i -ой угрозе будет определяться:

$$K_{\text{о} \beta \zeta \lambda i} = \sum_{j=1}^M \frac{K_{ij} \cdot [(P_{\text{н} \text{о} \lambda \text{о} \lambda} + \Delta_i) P_{\text{й} \text{е} \text{н} \text{т} \text{ } i}]}{\alpha_{1ij} K_{M1ij} + \alpha_{2ij} K_{M2ij} + \alpha_{3ij} K_{M3ij}}, \quad (6)$$

где: $K_{M1ij}, K_{M2ij}, K_{M3ij}$ – полезность использования j -го мероприятия на соответствующих 1,2 или 3 этапах блокировки i -ой угрозы;

$\alpha_{1ij}, \alpha_{2ij}, \alpha_{3ij}$ – весовые коэффициенты степени влияния j -го мероприятия на соответствующих этапах блокировки i -ой угрозы.

Численные значения составляющих коэффициента уязвимости объекта информатизации определяются с помощью математической обработки статистических данных и проведенных экспертных опросов.

Выводы

Представленный математический аппарат позволяет получить количественную оценку как существующего, так и прогнозируемого уровня уязви-

мости объекта информатизации. Если формулу (6) перевернуть «кверху ногами» то мы можем получить численное значение коэффициента защищенности объекта информатизации, поскольку уязвимость объекта информатизации есть величина обратная его защищенности.

Кроме того, следует отметить возможность данного математического подхода для оценки уровня комплексной безопасности объекта информатизации, поскольку при оценке вероятности угроз безопасности могут выбираться все возможные угрозы безопасности, которые напрямую могут быть не связаны с информационной безопасностью объекта, но в случае их реализации могут значительно снизить уровень информационной безопасности. Опять же если мы оцениваем полный перечень возможных угроз, то и перечень выбранных для их нейтрализации мер безопасности позволит обеспечить комплексную безопасность объекта информатизации.

В заключении следует сказать, что в настоящее время разработан программный продукт, позволяющий в автоматизированном режиме проводить экспертные опросы, с использованием математического аппарата обрабатывать результаты, выводить их в виде таблиц и графиков. И в конечном результате определять, как существующий уровень информационной безопасности объекта, так и прогнозируемый при реализации дополнительных мер безопасности. Применение данного программного продукта на целом ряде объектов позволило обеспечить эффективный подход к созданию надежной системы информационной безопасности способной противостоять всем возможным рискам.

Рецензент: Марков Алексей Сергеевич, доктор технических наук, старший научный сотрудник, профессор МГТУ им. Н.Э. Баумана, Москва, Россия. E-mail: a.markov@pro-echelon.ru

Литература

1. Аверченков В.И., Рытов М.Ю. Организационная защита информации: учеб. пособие для вузов. Брянск: БГТУ, 2009.
2. Андрианов В.В., Зефилов С.Л., Голованов В.Б., Колдуев Н.А. Обеспечение информационной безопасности бизнеса / 2-е издание перераб. и доп. М.: Альпина Паблишерз, 2011. 265 с.
3. Гафнер В.В. Информационная безопасность: учебное пособие. – Ростов н/Д: Феникс, 2010. 324 с.
4. Лапин В.В. Основы информационной безопасности органов внутренних дел [Текст]: учеб. пособие (в вопросах и ответах) / В. В. Лапин; МосУ МВД России. – М.: МосУ МВД России, 2012.
5. Козьминых С.И. Методологические основы обеспечения комплексной безопасности объекта, фирмы, предпринимательской деятельности. Монография. М-во внутренних дел Российской Федерации, Московский ун-т. Москва, 2005. 21 С.
6. Козьминых С. И. Организация защиты информации в российской полиции. Учебное пособие. М.: Юнити-Дана, 2017. 407 с.
7. Барабанов М.В., Денисенцев С.А., Кашин В.Б. и др. Радиоэлектронная борьба. От экспериментов прошлого до решающего фронта будущего. М.: Центр анализа стратегий и технологий, 2015. 248 с.
8. Скиба В.Ю., Курбатов В.А. Руководство по защите от внутренних угроз информационной безопасности. СПб.: Питер, 2008. 318 С.
9. Тихонов В.А., Райх В.В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты. Учебное пособие. М.: «Гелиос АРВ», 2006. 528 С.
10. Партыка Т.Л., Попов И.И. Информационная безопасность. Учебное пособие. М.: Форум - ИНФРА-М, 2007. 607 С.
11. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации. Учебное пособие. М.: Академия, 2007. 331 С.
12. Шиверский А.А. Защита информации: проблемы теории и практики. М.: Юристъ, 1996. 112 с.
13. Аглицкий И. Состояние и перспективы информационного обеспечения российских банков // Банковские технологии, №1, 1997. С.25-28.
14. Абрамов А.В. Новое в финансовой индустрии: информатизация банковских технологий. – СПб: Питер, 1997 г.
15. Заратуйченко О.В. Концепции построения и реализации информационных систем в банках // СУБД, №4.1996.
16. Кузнецов В.Е. Измерение финансовых рисков // Банковские технологии, №9. 1997. 76-78 С.
17. Тарасов П.И. Диасофт предлагает комплексные решения для банков // Мир ПК, №5. 1998.

MATHEMATICAL MODELING OF CREDIT AND FINANCE COMPLEX SECURITY SOLUTIONS

Kozminykh S.I.²

Abstract. This paper presents a methodology for an integrated approach to information security facilities credit and financial sphere. The basic principles of an integrated security information of the object credit and financial sphere. It is noted that the design of the system to provide a comprehensive security information of the object of credit and the financial sector, it is necessary to conduct choice of directions and principles for its implementation. The mathematical modeling of complex security level information of the objects–bank financial sphere using probabilities Torii, whose aim is to obtain a functional relationship to find the numerical value of the coefficient vulnerability evaluating level complex security object–bank financial sphere. The process of mathematical modeling is divided into five stages, as a result of which the components are obtained and the formula of the coefficient vulnerability information of the object which are determined by mathematical statistical data processing and peer poll. As a conclusion is that the developed mathematical formalism allows to obtain a quantitative assessment of both the existing and projected vulnerability information of the object. Also noted the possibility of the mathematical approach to assess a complex object–level security information of the credit and financial sphere.

² Sergey Kozminykh, Dr.Sc. (Technical Sc), Professor University of Finance under the Governments of the Russian Federation, Moscow, Russia. E-mail: SlKozminykh@fa.ru

Keywords: *an integrated approach to information security, information security threat object credit and financial sphere, the principles of providing comprehensive security information of an object, statistical probability, expert evaluation, a single dynamic coefficient of a threat, damage ratio, coefficient of vulnerability.*

References

1. Averchenkov V.I., Rytov M.Yu. Organizatsionnaya zashchita informatsii: ucheb. posobie dlya vuzov. Bryansk: BGTU, 2009.
2. Andrianov V.V., Zefirov S.L., Golovanov V.B., Kolduev N.A. Obespechenie informatsionnoy bezopasnosti biznesa / 2-e izdanie pererab. i dop. M.: Al'pina Pablishez, 2011. 265 P.
3. Gafner V.V. Informatsionnaya bezopasnost': uchebnoe posobie. – Rostov n/D: Feniks, 2010. 324 P.
4. Lapin V.V. Osnovy informatsionnoy bezopasnosti organov vnutrennikh del [Tekst]: ucheb. posobie (v voprosakh i otvetakh) / V. V. Lapin; MosU MVD Rossii. - M.: MosU MVD Rossii, 2012.
5. Koz'minykh S.I. Metodologicheskie osnovy obespecheniya kompleksnoy bezopasnosti ob'ekta, firmy, predprinimatel'skoy deyatel'nosti. Monografiya. M-vo vnutrennikh del Rossiyskoy Federatsii, Moskovskiy un-t. Moskva, 2005. 21 P.
6. Koz'minykh S. I. Organizatsiya zashchity informatsii v rossiyskoy politsii. Uchebnoe posobie. M.: Yuniti-Dana, 2017. 407 P.
7. Barabanov M.V., Denisentsev S.A., Kashin V.B. i dr. Radioelektronnaya bor'ba. Ot eksperimentov proshlogo do reshayushchego fronta budushchego. M.: Tsentr analiza strategiy i tekhnologiy, 2015. 248 P.
8. Skiba V.Yu., Kurbatov V.A. Rukovodstvo po zashchite ot vnutrennikh ugroz informatsionnoy bezopasnosti. SPb.: Piter, 2008. 318 P.
9. Tikhonov V.A., Raykh V.V. Informatsionnaya bezopasnost': kontseptual'nye, pravovye, organizatsionnye i tekhnicheskie aspekty. Uchebnoe posobie. M.: «Gelios ARV», 2006. 528 S.
10. Partyka T.L., Popov I.I. Informatsionnaya bezopasnost'. Uchebnoe posobie. M.: Forum - INFRA-M, 2007. 607 P.
11. Mel'nikov V.P., Kleymentov S.A., Petrakov A.M. Informatsionnaya bezopasnost' i zashchita informatsii. Uchebnoe posobie. M.: Akademiya, 2007. 331 P.
12. Shiverskiy A.A. Zashchita informatsii: problemy teorii i praktiki. M.: Yurist", 1996. 112 P.
13. Aglitskiy I. Sostoyanie i perspektivy informatsionnogo obespecheniya rossiyskikh bankov, Bankovskie tekhnologii, No 1, 1997, pp. 25-28.
14. Abramov A.V. Novoe v finansovoy industrii: informatizatsiya bankovskikh tekhnologiy. - SPB: Piter, 1997.
15. Zarutuychenko O.V. Kontseptsii postroeniya i realizatsii informatsionnykh sistem v bankakh, SUBD, No 4. 1996.
16. Kuznetsov V.E. Izmerenie finansovykh riskov // Bankovskie tekhnologii, No 9. 1997, 76-78 pp.
17. Tarasov P.I. Diasoft predlagaet kompleksnye resheniya dlya bankov, Mir PK, No 5. 1998.