DOI: 10.26794/2587-5671-2018-22-5-105-121
УДК 004.056(045)
JEL C21

Моделирование обеспечения информационной безопасности объекта кредитно-финансовой сферы

С.И. Козьминых,
Финансовый университет, Москва, Россия
https://orcid.org/0000-0003-3903-9562

АННОТАЦИЯ

Предметом исследования является анализ информационной защищенности объекта кредитно-финансовой сферы, выдающего микрозаймы. Построена план-схема типового объекта кредитно-финансовой сферы, приведена организационно-штатная структура организации, занимающейся выдачей микрозаймов. Проведен анализ персонала организации, видов деятельности и зон, в которые он имеет право доступа. На основании полученных данных построена модель угроз информационной безопасности организации, занимающейся выдачей микрозаймов. Определено соответствие видов угроз типам нарушителей информационной безопасности организации. Построена трехмерная модель информационной безопасности. Модель позволяет рассчитать коэффициент уязвимости объекта кредитно-финансовой сферы исходя из полученных данных в компании, выдающей микрокредиты, и имеющейся статистической информации. Выявлены основные параметры, определяющие показатели защищенности: количество и характеристики дестабилизирующих факторов, которые могут проявиться и оказать негативное воздействие на защищаемую информацию; количество и характеристики применяемых методов защиты информации; число и категории лиц, которые потенциально могут быть нарушителями правил защиты информации; виды защищаемой информации. Путем расчета коэффициента защищенности объекта можно создать эффективную систему его информационной безопасности, оптимизировать выбор комплекса технических средств и методов защиты информации. Это позволит значительно сократить ущерб, возникающий из-за реализации угроз информационной безопасности.

Разработанный метод математического моделирования позволяет оценить текущий уровень информационной безопасности в любой организации кредитно-финансовой сферы.

Ключевые слова: информация; безопасность; моделирование; угроза; ущерб; нарушитель; защита; мера; элемент; коэффициент

Для цитирования: Козьминых С.И. Моделирование обеспечения информационной безопасности объекта кредитно-финансовой сферы. *Финансы: теория и практика.* 2018;22(5):105-121. DOI: 10.26794/2587-5671-2018-22-5-105-121

Modelling the Provision of Information Security of the Object of the Credit and Financial Sphere

S.I. Koz'minykh,
Financial University, Moscow, Russia
https://orcid.org/0000-0003-3903-9562

ABSTRACT

The subject of our study was the analysis of information security of the object of a particular credit and financial sphere, issuing microloans. The authors built a plan-scheme of a typical object of the credit and financial sector. We also described the organizational structure and staff structure of the microloans organization. Further, we conducted an analysis of the organization's staff, their activities, and areas in which they have the right to access. On the basis of the obtained data, we constructed a model of threats to information security of the microloans organization. The authors determined the correspondence of the types of threats to the types of violators of information security. We have built a three-dimensional model of information security, which allows us to calculate the vulnerability factor of the object of credit and financial sector, based on the data obtained in the company issuing micro-loans, as well as available statistics. The main parameters that determine the security indicators are identified: the number and characteristics of destabilizing factors that can manifest themselves and have a negative impact on the protected information; the number and characteristics of the methods used to protect information; the number and categories of persons who can potentially be violators of information security rules; types of protected information. By calculating the security

coefficient of the object, it is possible to create an effective system of its information security and to optimize the choice of a set of technical means and methods of protection of information. It can significantly reduce the damage arising from the threats to information security. The method of mathematical modelling developed by the authors allows estimating the current level of information security in any organization of the financial sphere.
Keywords: information; security; modelling; threat; damage; violator; protection; measure; element; coefficient

For citation: Koz'minykh S.I. Modelling the provision of information security of the object of the credit and financial sphere. *Finansy: teoriya i praktika = Finance: Theory and Practice.* 2018;22(5):105-121. (In Russ.). DOI: 10.26794/2587-5671-2018-22-5-105-121

ВВЕДЕНИЕ

Владение информацией может стать ключом для решения большинства проблем мирового сообщества. В то же время ее противоправное использование способно привести к крупномасштабным авариям, дезорганизовать государственное управление и финансовую систему. С другой стороны, эффективное использование информации способствует развитию всех сфер деятельности государства в целом и отдельно взятой организации в частности и в конечном счете приводит к значительным успехам в экономике, бизнесе и финансах [1].

Создание системы защиты информации является основной задачей объекта кредитно-финансовой сферы (КФС). Эта система не должна приводить к ощутимым трудностям в работе объекта, ее создание должно быть экономически оправданным. Вместе с тем она должна обеспечивать защиту важных информационных ресурсов объекта от всех возможных угроз [2].

Одним из наиболее эффективных научных методов создания надежной системы информационной безопасности объектов КФС является моделирование процессов и систем защиты информации [3].

Предметом исследования в данной работе является моделирование системы защиты информации организации, которая предоставляет микрозаймы. Это связано с хранением и обработкой большого количества конфиденциальной информации, как правило, в специально выделенном помещении. Данные особенности необходимо учитывать при моделировании системы защиты информации.

АНАЛИЗ СУЩЕСТВУЮЩЕЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ОРГАНИЗАЦИИ КФС, КОТОРАЯ ПРЕДОСТАВЛЯЕТ МИКРОЗАЙМЫ

Процесс проектирования системы защиты информации объекта необходимо начинать с получения исходных данных.

Ясно, что на результативность системы защиты информации влияет множество показателей. Этими показателями являются наиболее существенные характеристики объекта, такие как этажность, площадь защищаемого объекта, толщина перекрытий, типы остекления, количество входов/выходов и т.д. [4]

Для выбора подходящей модели рассмотрим план-схему типового объекта КФС (*рис. 1*), а также то, на какие рубежи защиты она разбита. Полученная информация будет являться исходными данными для построения модели нарушителя, а в дальнейшем и для создания трехмерной модели системы защиты информации на объекте КФС.

К1 — кабинет охраны (входит в зону 3, там, где проводится прием посетителей, соответственно, на этой территории должен быть организован контроль и учет посетителей).

К2 — кабинет переговоров, также серверная комната (входит в зону 5, в которой проходят переговоры. Такое помещение должно иметь соответствующий уровень защиты, например от прослушивания).

К3 — хранилище (относится к зоне 6, где необходим максимальный уровень защиты информации).

К4 — атриум (входит в зону 3, там, где проводится прием посетителей, соответственно на этой территории должен быть организован контроль и учет посетителей).

К5 — прилегающая территория.

К6 — проходная зона к хранилищу (входит в зону 6, куда не допускаются не уполномоченные сотрудники).

К7 — кабинет директора.

К8 — помещение для обработки персональных данных клиентов.

К9 — техническое помещение.

К10 — санузел.

На плане мы видим, что организация располагается на одном этаже и имеет различные помещения, к каждому из которых имеет доступ только тот персонал, у которого есть соответствующий уровень допуска.

Определенное должностное лицо может пройти в ограниченное число подобных помещений, например рядовой сотрудник, который работает в офисной части (К8) не имеет возможности пройти в хранилище (К3). Исходя из этого, необходимо рассмотреть, кто работает в этой организации, т.е. представить организационно-штатную структуру ее деятельности (*рис. 2*).

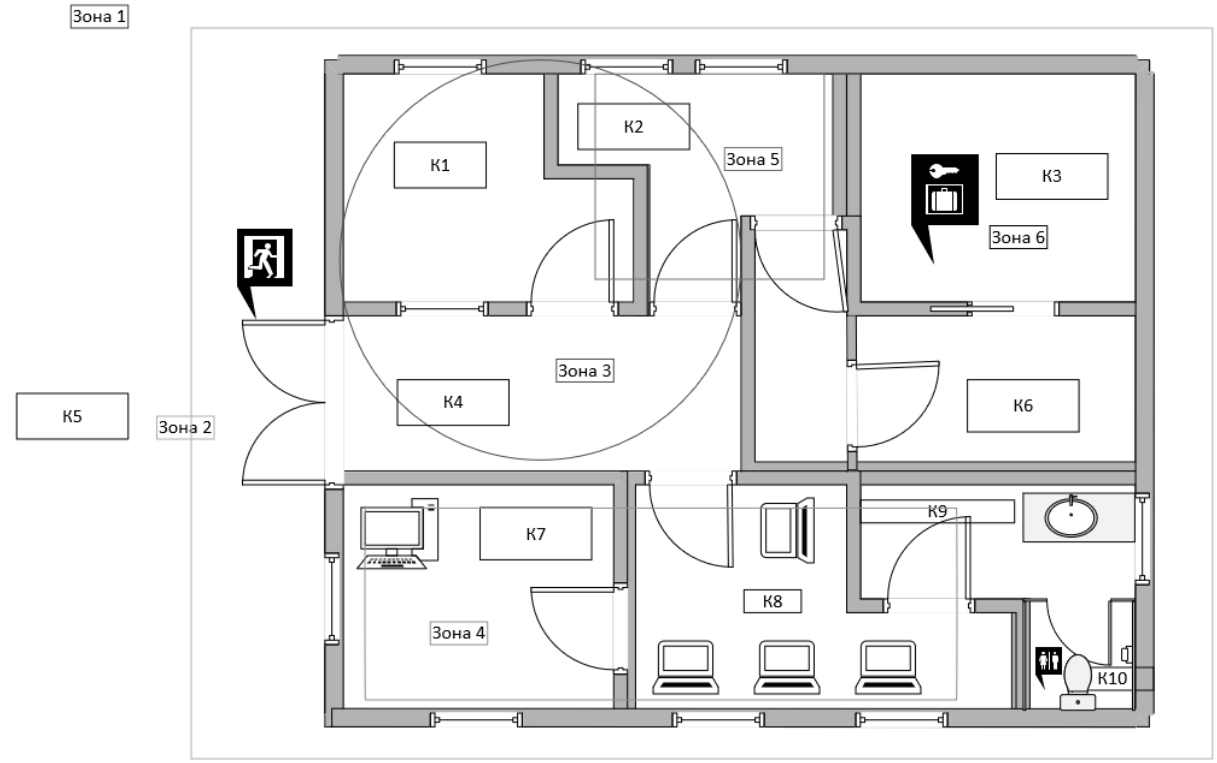


Рис. 1 / Fig. 1. **Расположение основных отделов на поэтажном плане организации, занимающейся выдачей микрокредитов / The location of the main departments on the floor plan of the microloans organization**

Источник / Source: составлено авторами / compiled by the authors.

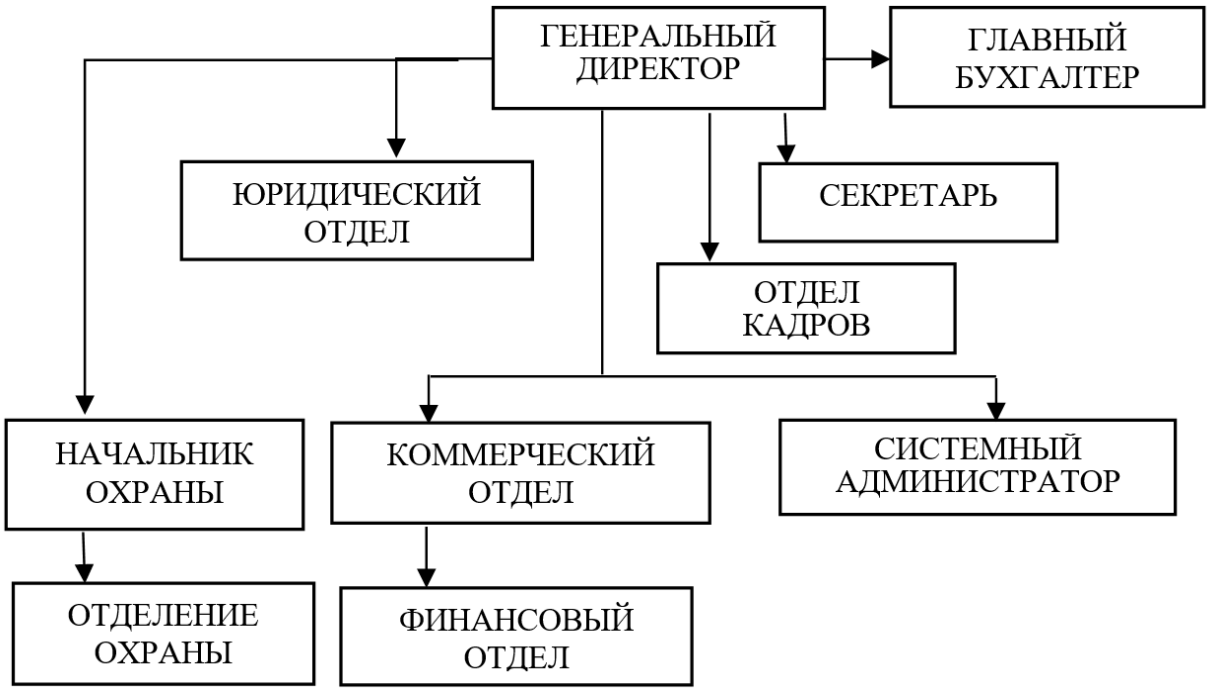


Рис. 2 / Fig. 2. **Организационно-штатная структура организации, занимающейся выдачей микрозаймов / Organizational and staff structure of the microloans organization**

Источник / Source: составлено авторами / compiled by the authors.

Таблица 1 / Table 1

Персонал организации, виды его деятельности и зоны, в которые он имеет право доступа / The personnel of the organization, the types of their activities and the zones in which they have the right of access

№	Должность	Зоны доступа	Количество человек	Вид деятельности
1	Генеральный директор	К1-К10	1	Управление организацией КФС
2	Юридический отдел	К5, К4, К8, К9, К10	1	Подготовка документов
3	Секретарь	К5, К4, К8, К9, К10	1	Помощник генерального директора, работа со звонками клиентов
4	Отдел кадров	К5, К4, К8, К9, К10	1	Прием на работу новых сотрудников
5	Главный бухгалтер	К5, К4, К8, К9, К10, К2, К3, К6	1	Финансовая деятельность организации КФС
6	Начальник охраны	К1-К10	1	Обеспечение защищенности объекта
7	Отделение охраны	Везде, кроме К2, К6, К3	3	Контролирование защищенности объекта
8	Коммерческий отдел	К5, К4, К8, К9, К10	2	Работа с клиентами у стойки для посетителей, занесение ПД в базу данных
9	Финансовый отдел	К5, К4, К8, К9, К10	1	Обработка ПД и финансовых задолженностей
10	Системный администратор	К5, К4, К8, К9, К10, К1, К2, К7	1	Обеспечение работы сервера и всех персональных компьютеров в организации

Источник / Source: составлено авторами / compiled by the authors.

Важным показателем является количество сотрудников, работающих в организации [5]. Поэтому в *табл. 1* представлен весь персонал организации, а также виды его деятельности и зоны доступа, в которые он имеет возможность проходить без ограничений.

Для обеспечения приемлемого уровня безопасности рассматриваемая организация обеспечивается техническими средствами и отделением охраны, которое должно своевременно реагировать на нарушения [6]. Охрана расположена в помещении К1.

Исходя из представленных исходных данных можно перейти к построению моделей угроз и нарушителей, которые в дальнейшем позволят перейти к созданию трехмерной модели обеспечения информационной безопасности и расчету коэффициента защищенности объекта КФС.

ПОСТРОЕНИЕ МОДЕЛЕЙ УГРОЗ И НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОБЪЕТКЕ КФС

При обследовании объекта эксперты заполняли специальные анкеты, с помощью которых строилась модель угроз. Для построения модели угроз необходимо было определить элементы защиты объекта информатизации КФС, подверженные воздействиям угроз, и их уязвимость, ущерб элементу и объекту защиты, а также меры безопасности, которые будут противодействовать угрозам.

Модель угроз (*табл. 2*) включает в себя исходные данные для построения трехмерной модели, которая поможет определить коэффициент уязвимости объекта информатизации КФС.

Элементы защиты могут быть различными, в данной организации они представлены в виде персонала, материальных ценностей, информации, экономической деятельности, юридической деятельности и в виде автоматизированных систем обработки информации [7].

Далее рассмотрим подробнее некоторые из угроз и возможные последствия их реализации.

1. **Угрозы персоналу и возможные последствия**. Во время работы персонал ежедневно контактирует с клиентами, предоставляя услуги финансового характера. Не всегда данные контакты проходят без инцидентов, так как некоторые кли-

Таблица 2 / Table 2

Модель угроз информационной безопасности организации, занимающейся выдачей микрозаймов / A model of threats to the information security of the microloans organization

№	Элемент защиты	Угроза безопасности	Ущерб элементу защиты	Ущерб объекту защиты	Меры безопасности
1	Персонал организации (сотрудники)	Кража, грабеж, шантаж	Травма различной степени тяжести, моральный ущерб	Прекращение рабочей деятельности	Проведение профилактических учений, усиленные меры безопасности, системы охранного телевидения, наблюдения
		Конфликтные ситуации	Моральный ущерб	Снижение эффективности рабочей деятельности	Создание охраны, системы видеонаблюдения / охраны (для быстрого реагирования на инцидент или фиксирования нарушителя)
2	Материальные ценности, включая охраняемую территорию	Кража	Хищение элемента защиты (дальнейшее его отсутствие на территории охраняемого объекта)	Снижение эффективности рабочей деятельности (в связи с утратой элемента защиты) или полная неспособность продолжать рабочий процесс	Создание охраны, контроль доступа персонала, системы видеоохраны / наблюдения для фиксации нарушителя или перехвата в момент совершения кражи
		Порча имущества, вандализм	Ограничение функциональности элемента защиты, полная утрата функциональных свойств	Снижение эффективности рабочей деятельности или полная неспособность продолжать рабочий процесс	Создание охраны, контроль доступа персонала, системы видеоохраны / наблюдения для фиксации нарушителя или перехвата в момент совершения акта вандализма
		Пожар, стихийные бедствия, аварии	Уничтожение элемента защиты	Полная неспособность продолжать рабочий процесс, поскольку с наибольшей вероятностью помимо материальных ценностей вместе с пожаром будет уничтожено помещение организации	Страхование (в случае пожара, стихийных бедствий, аварий) системы пожаротушения, датчики определения дыма, автоматический вызов пожарных служб и т.д. (в случае пожара)
3	Информация	Кража / копирование информации	Кража информации	Получение информации конкурентом	Ограничение доступа, пароли, шифрование данных, патрулирование охраняемой территории сотрудниками охраны и выявление нарушителей, системы видеонаблюдения
		Уничтожение информации	Уничтожение объекта защиты, например, материального носителя информации	Невозможность продолжать рабочую деятельность	Ограничение доступа, пароли, шифрование данных, патрулирование охраняемой территории сотрудниками охраны и выявление нарушителей, системы видеонаблюдения
		Несанкционированное ознакомление, модификация информации	Некорректные данные, которые ведут за собой ошибки в процессе рабочей деятельности	Материальный ущерб, получение информации конкурентом	Ограничение доступа, пароли, шифрование данных, патрулирование охраняемой территории сотрудниками охраны и выявление нарушителей

Окончание табл. 2 / End of Table 2

№	Элемент защиты	Угроза безопасности	Ущерб элементу защиты	Ущерб объекту защиты	Меры безопасности
4	Экономическая деятельность	Неправильная оценка рынка	Использование некорректных данных в процессе рабочей деятельности	Материальный ущерб, полное прекращение деятельности организации	Грамотный подход к оценке рынка
		Невозврат кредитных средств	Потеря кредитных средств	Материальный ущерб, при значительном уровне невозврата кредитных средств прекращение рабочей деятельности	Правильная оценка возможности потребителя
5	Юридическая деятельность	Неправильное заполнение документов, ложные персональные данные, внесенные клиентом	Использование некорректных данных в процессе рабочей деятельности	Материальный ущерб, полное прекращение деятельности организации	Внимательность, повторная перепроверка
		Потеря лицензии	Приостановление или полное прекращение рабочей деятельности	Приостановление или полное прекращение рабочей деятельности соответственно получению материального ущерба	Соблюдение всех условий для продления лицензии
6	Автоматизированные средства обеспечения информации (АСОИ) (персональный компьютер	Вирусы	Вывод из строя ПК	Прекращение рабочей деятельности	Антивирусное ПО, межсетевые экраны
		Перепад напряжения, обесточивание помещения	Потеря несохраненных данных	Прекращение рабочей деятельности, ограничение деятельности, материальные затраты	Источник бесперебойного питания
		Вредоносные программы, переносимые на USB устройствах	Вывод из строя ПК	Прекращение, ограничение рабочей деятельности, материальные затраты	Инструктаж безопасности персонала

Источник / Source: составлено авторами / compiled by the authors.

енты могут быть не сдержанны или даже агрессивны. Это может привести к временной нетрудоспособности работника ввиду нанесения ему моральной или физической травмы. Сотрудники охраны должны своевременно отреагировать на сложившуюся ситуацию. В этом может помочь система охранного телевидения, предназначенная для постоянного контроля зоны оказания услуг. Но лучше, если в зале обслуживания клиентов всегда дежурит один сотрудник охраны.

2. **Угрозы материальным ценностям организации** опасны тем, что может произойти хищение, порча или уничтожение материальных ценностей, а это влечет за собой замедление или даже остановку рабочего процесса.

3. **Кража, копирование, уничтожение, модификация информации** может привести к большим материальным потерям, если она, например, попадет в руки конкурирующей организации. Для обеспечения защиты информации на

объекте помимо охраны должны эксплуатироваться технические средства, которые будут обеспечивать защиту информации [8].

4. **Угрозы экономической деятельности** могут быть различны, но в рассматриваемой организации это преимущественно возможность неправильной оценки рынка или невозврат выдаваемых денежных средств. Если случается какая-либо вышеописанная ситуация, это может привести к большим материальным потерям. В случае если неправильно оценен рынок, все сотрудники будут работать, опираясь на ложные данные, и это постепенно приведет к нестабильной ситуации вплоть до банкротства [9]. Если организации не будут возвращены денежные средства одним или несколькими клиентами, она, скорее всего, сможет компенсировать свои потери, поскольку такие ситуации предусмотрены заранее. Но, если это явление массовое, организация может не справиться со сложившейся ситуацией.

5. **Основная угроза юридической деятельности** для рассматриваемой организации — отзыв лицензии на какой-либо вид деятельности из-за несоблюдения законов. До ее восстановления (т.е. ликвидации нарушений) оказание услуг должно быть приостановлено, что приводит к материальным потерям.

6. **Угроза автоматизированным средствам обработки информации** (АСОИ) — важный момент для любой организации, поскольку сейчас везде используются персональные компьютеры для автоматизации процессов обработки информации и минимизации влияния человеческого фактора. Персональный компьютер можно вывести из строя различными способами, самый распространенный из которых — вредоносное программное обеспечение [10]. Для исключения подобной ситуации следует ограничить доступ сотрудникам на посторонние сайты Интернета и запретить использование USB устройств (на физическом и программном уровне). Также следует учитывать риск обесточивания объекта информатизации КФС, в таких ситуациях для поддержания непрерывного рабочего процесса следует использовать источники бесперебойного питания.

Существует большое количество угроз, которые могут нанести ущерб, начиная с неграмотных действий сотрудника и заканчивая возникновением чрезвычайных ситуаций.

Величина ущерба является одним из показателей, который используется при подсчете коэффициента защищенности и построения трехмерной модели. Он может быть максимальным — 100% (если при реализации угрозы останавливается весь процесс работы, что, как правило, приводит к банкротству организации). Может быть средним — до 50% (при реализации угрозы происходят большие финансовые потери) и минимальным — менее 20% (когда при реализации угрозы ущерб незначителен).

По экспертным оценкам, угрозой, при реализации которой может быть нанесен наибольший ущерб, является такой тип нарушителя, как внешний и внутренний злоумышленник (инсайдер) [11]. Внешний злоумышленник целенаправленно проникает на территорию организации и пытается выкрасть наиболее важную информацию (материальные ценности, бумажные носители и т.д.), а инсайдер может передать конкурирующей организации информацию непосредственно со своего рабочего места. Подобные инциденты приводят к большим финансовым потерям.

В рассматриваемой организации возможный внутренний нарушитель представлен сотрудниками этой организации, а внешний — всеми физическими лицами, не работающими в данной организации. Для реализации трехмерной модели необходимо знать, какой ущерб нанесет сотрудник или внешний нарушитель тому или иному виду информации и сможет ли организация после реализации этой угрозы продолжить свою деятельность и при каких материальных затратах это будет возможно.

Поэтому для подсчета величины ущерба при реализации угрозы в рассматриваемой организации необходимо составить таблицу соответствия видов угроз типам нарушителя (*табл. 3*).

Значения для всех видов вышеописанных угроз для рассматриваемой организации взяты, исходя из того, что максимальный ущерб компании — 100%, поэтому:

- минимальный ущерб — 0–3 (до 30%) (D_3). Организация может понести незначительные материальные потери или же можно их полностью исключить;
- средний ущерб — 4–7 (от 40 до 70%) (D_2). Организация понесет значительные материальные потери, но сможет продолжать свою деятельность;
- большой (максимальный) ущерб — 8–10 (от 80 до 100%) (D_1). Организация понесет значительный ущерб и больше не сможет оказывать услуги финансового характера;
- 0 — условное обозначение, когда сотрудник не имеет доступа к информации.

Величина ущерба от внешнего злоумышленника — это максимальное значение, которое взято из величин ущерба всех внутренних злоумышленни-

Таблица 3 / Table 3

Соответствие видов угроз типам нарушителей / The correspondence of types of threats to types of violators

Вид угрозы	Тип нарушителя								
	Внутренний								Внешний
	Сотрудники юр. отдела	Сотрудники фин. отдела	Сотрудник ком. отдела	Секретарь	Системный администратор	Главный бухгалтер	Охранник	Сотрудник отдела кадров	Злоумышленники, не работающие в данной организации
	Относительные значения величины ущерба, причиняемого нарушителем								
Кража информации из сейфа (A_1)	0	0	0	0	0	10	0	0	10
НСД к серверу (A_1)	0	0	0	0	10	0	0	0	10
Кража информации на рабочем месте (A_2)	6	9	2	10	10	10	6	5	10
Копирование информа-ции (A_3)	5	5	5	5	10	10	5	5	10
Несанкционированное ознакомление, модификация информа-ции (A_4)	5	5	5	5	10	10	5	5	10
Провоцирование чрезвычайной ситуации (A_5)	10	10	10	10	10	10	10	10	10
Вывод из строя АСОИ с помощью программных средств (A_6)	4	5	6	9	7	4	7	4	9
Вывод из строя АСОИ путем механических повреждений (A_7)	5	6	7	10	8	5	8	5	10
Кража материальных ценностей (зона K_7) (A_8)	0	0	0	10	0	0	10	0	10
Кража материальных ценностей (зона K_3) (A_9)	0	0	0	0	0	10	0	0	10
Всего (максимальная величина ущерба)	**3,5** (D_2)	**4** (D_2)	**3,6** (D_2)	**5,9** (D_2)	**6,5** (D_2)	**6,9** (D_2)	**4,9** (D_2)	**3,4** (D_2)	**9,9** (D_1)

Источник / Source: составлено авторами / compiled by the authors.

ков, поскольку если внешний злоумышленник реализует любую из них, ущерб будет соразмерным [12].

Из *табл. 3* следует, что наибольший уровень ущерба при реализации угрозы может причинить внешний злоумышленник, остальных можно расположить по убыванию подобным образом:

1. Внешний злоумышленник — (99%) (при неграмотно реализованной системе защиты информации может украсть, модифицировать и т.д. информацию высокой степени важности).
2. Главный бухгалтер — (69%) (имеет доступ к большому количеству информации, включая информацию, хранящуюся в сейфе).
3. Системный администратор — (65%) (имеет возможность, копировать, модифицировать, удалять информацию с сервера, где хранятся все данные о деятельности организации).
4. Секретарь — (59%) (имеет доступ ко всем документам, которые обрабатывает для генерального директора).
5. Охранник — (49%) (контролирует охраняемую территорию, соответственно имеет высокий уровень доступа).
6. Сотрудники финансового отдела — (40%).
7. Сотрудники коммерческого отдела — (36%).
8. Сотрудники юридического отдела — (35%).
9. Сотрудники отдела кадров — (34%).

Исключениями являются генеральный директор и начальник охраны, поскольку они, несмотря на то, что имеют самый высокий уровень доступа, всегда заинтересованы в том, чтобы нейтрализовать угрозы, а не создавать их.

Описание и формализация возможных угроз и уровня ущерба является важным этапом создания трехмерной модели. Далее перейдем к ее разработке.

РАЗРАБОТКА ТРЕХМЕРНОЙ МОДЕЛИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ОБЪЕКТЕ КРЕДИТНО-ФИНАНСОВОЙ СФЕРЫ

Моделирование — формализованное отображение какого-либо процесса с целью его изучения, управления и совершенствования [13]. Таким образом, весь процесс моделирования можно разделить на два этапа: построение модели и ее верификация с целью получения необходимых характеристик системы защиты информации.

Для начала необходимо учесть, на каком этапе происходит создание либо усовершенствование системы информационной безопасности:

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

2. Объект уже функционирует, система информационной безопасности имеется, требуется повысить ее уровень за счет оптимизации мер защиты. Остановимся на втором варианте, который чаще всего встречается в практической деятельности.

После этого необходимо выбрать тип модели: аналитический или статистический.

Аналитические модели представляются в виде некоторой совокупности аналитических и (или) логических зависимостей, позволяющих определять по ним необходимые характеристики путем проведения логических сравнений и / или вычислений. Статистические модели основываются на использовании статистических данных [14].

В данной работе трехмерная модель (*рис. 3*) по сути является и аналитической, и статистической.

Одной из первоочередных задач, предшествующих расчету коэффициента безопасности, является задача выбора системы показателей, которая должна отражать все требования к защите информации, структуру объекта информатизации (ОИ), технологию и условия обработки, хранения и передачи информации, а также учитывать возможности противника по добыванию информации.

Основными параметрами, определяющими показатели защищенности информации, являются:

- количество и характеристики дестабилизирующих факторов, которые могут проявиться и оказать негативное воздействие на защищаемую информацию [15];
- количество и характеристики применяемых методов защиты информации;
- число и категории лиц, которые потенциально могут быть нарушителями правил защиты информации;
- виды защищаемой информации.

Из основных параметров, определяющих показатели защищенности информации, можно выделить следующие элементы и, систематизируя их, построить трехмерную модель. Путем анализа показателей далее можно будет рассчитать коэффициент защищенности информации.

Введем следующие обозначения, предназначенные для построения трехмерной модели:

1) A — угрозы;
2) B — меры защиты;
3) C — элементы защиты;
4) D — ущерб, причиняемый элементу защиты в результате воздействия на него угрозы.

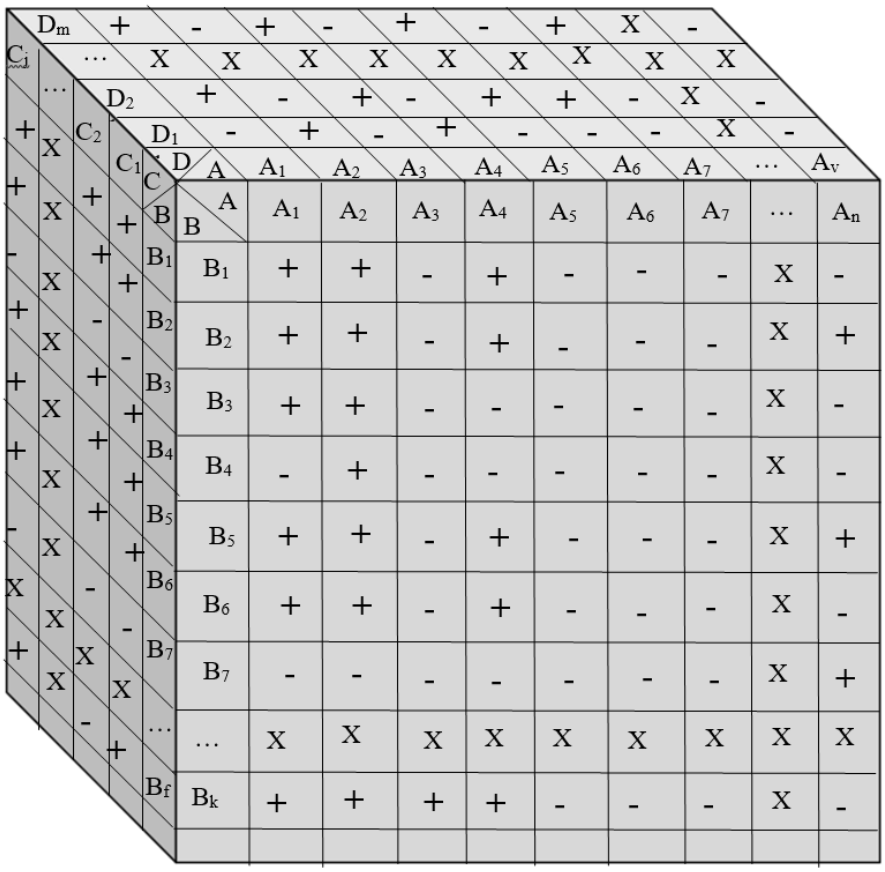
Уровень безопасности зависит от того, насколько эффективны меры, способные противостоять вероятным угрозам, которые могут причинить ущерб наиболее важным элементам защиты [16].

Таблица 4 / Table 4

Определение коэффициента значимости меры безопасности / Determination of the significance factor of the security measure

Наименование и обозначение меры безопасности	Этап предупреждения Вес-3	Этап пресечения Вес-2	Этап ликвидации последствий Вес-1	Сумма рейтинга мер безопасности
Охранное телевидение (В1)	3	2	1	6
Охранная сигнализация (В2)	3	2	0	5
Пожарная сигнализация (В3)	3	2	0	5
Система пожаротушения (В4)	0	2	1	3
СКУД (В5)	3	2	1	6
Замки на дверях (В6)	3	0	0	3
Непрозрачное стекло	3	0	0	3
Источник бесперебойного питания	0	2	0	2
Антивирусные программы	3	2	1	6
Резервное копирование данных	3	0	1	4
Оптико-электронный охранный излучатель	3	0	0	3
Биометрическая система распознавания личности	3	2	0	5
Экранирование ПЭМИН (побочные электромагнитные излучения и наводки)	3	2	0	5
Генераторы шума	3	2	0	
Скремблеры, осуществляющие стойкие алгоритмы шифрования речевых сообщений	3	2	0	5
Системы имитации охранного телевидения	0	2	0	2

Источник / Source: составлено авторами / compiled by the authors.



D	A	A_1	A_2	A_3	A_4	A_5	A_6	A_7	…	A_v
C	B	A_1	A_2	A_3	A_4	A_5	A_6	A_7	…	A_n
B_1	B_1	+	+	-	+	-	-	-	X	-
B_2	B_2	+	+	-	+	-	-	-	X	+
B_3	B_3	+	+	-	-	-	-	-	X	-
B_4	B_4	-	+	-	-	-	-	-	X	-
B_5	B_5	+	+	-	+	-	-	-	X	+
B_6	B_6	+	+	-	+	-	-	-	X	-
B_7	B_7	-	-	-	-	-	-	-	X	+
…	…	X	X	X	X	X	X	X	X	X
B_f	B_k	+	+	+	+	-	-	-	X	-

Рис. 3 / Fig. 3. **Трехмерная модель защищенности объекта кредитно-финансовой сферы / The three-dimensional model of the security of the object of the credit and financial sphere**

Источник / Source: составлено авторами / compiled by the authors.

Если мера безопасности направлена на защиту какого-либо элемента, то ее рейтинг зависит от:

- важности элемента защиты;
- вероятности и количества угроз, которые могут воздействовать на этот элемент защиты;
- величины ущерба, который может быть причинен элементу защиты при воздействии на него угроз.

Меры безопасности могут осуществляться на трех этапах:

1. **Этап предупреждения**. Время до возникновения угрозы: используются превентивные меры безопасности, проводятся обучение и тренировки сотрудников, службы безопасности объекта, осуществляется инженерно-техническая укрепленность объекта, устанавливается охранно-пожарная сигнализация и другие технические средства защиты объекта информатизации.

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: осуществляются 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.

Чтобы рассчитать коэффициент значимости элемента безопасности, необходимо учесть, на каком этапе было обеспечено противодействие угрозе. Каждому этапу можно присвоить свой вес в зависимости от его важности [17]. Например, этап предупреждения имеет вес 3, этап пресечения — 2 и этап ликвидации последствий — 1. Присвоение веса именно таким образом обусловливается тем, что намного лучше нейтрализовать угрозу на этапе предупреждения, нежели потом ликвидировать последствия. Исходя из этого, можно построить таблицу, которая поможет рассчитать коэффициент значимости меры безопасности (*табл. 4*).

Далее можно перейти к построению трехмерной модели (см. *рис. 3*).

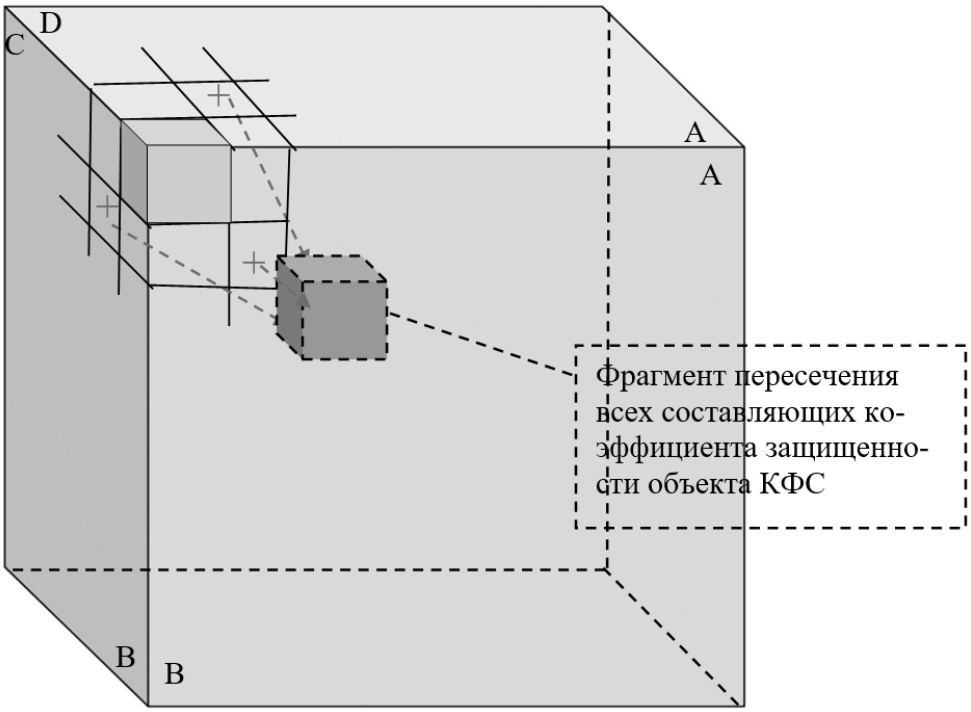


Рис. 4 / Fig. 4. **Фрагмент трехмерной модели коэффициента защищенности объекта информатизации КФС / Part of the three-dimensional model of the security coefficient of the information object of the CFS**

Источник / Source: составлено авторами / compiled by the authors.

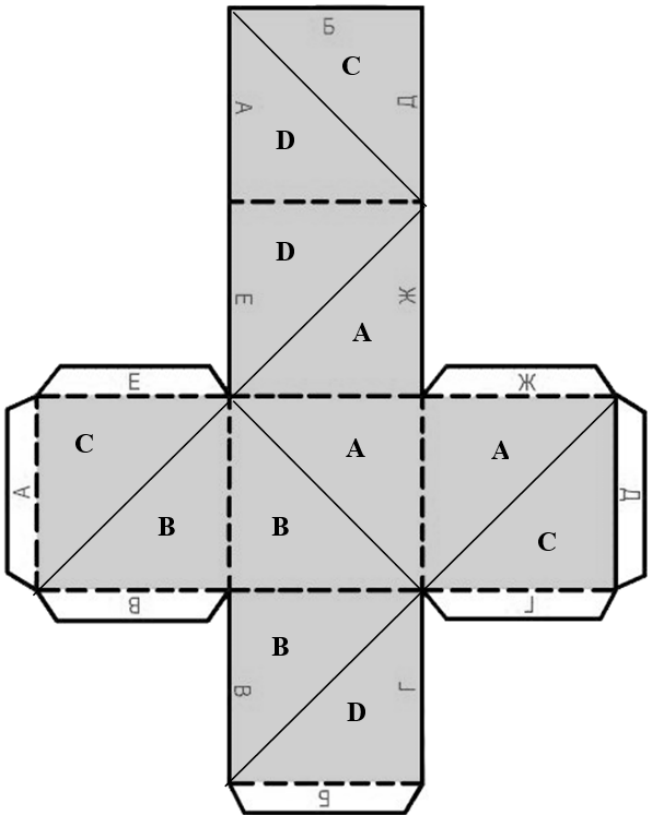


Рис. 5 / Fig. 5. **Фрагмент трехмерной модели защищенности объекта информатизации КФС / Part of the three-dimensional model of the security of the information object of the CFS**

Источник / Source: составлено авторами / compiled by the authors.

В результате анализа трехмерной модели можно сделать вывод, что эффективность мер безопасности — это отношение важности элемента защиты, вероятности и количества угроз, величины ущерба, к полезности мер, направленных на обеспечение безопасности этих элементов защиты.

Более подробно место пересечения составляющих коэффициента защищенности изображено на *рис. 4*. Фрагмент представляет собой куб в развернутом состоянии, где шрифтом русского алфавита обозначены буквы соединения сторон, а шрифтом латинского алфавита — коэффициенты угрозы, мер защиты, величины ущерба. Данный фрагмент позволяет понять, каким именно образом взаимодействуют все составляющие коэффициента защищенности объекта информатизации КФС.

На *рис. 5* видно, что каждая составляющая коэффициента защищенности зависит от других, что хорошо видно на всех плоскостях трехмерного фрагмента. К примеру, чем выше угроза, тем больше будет ущерб при ее реализации.

Если представить вышеописанный фрагмент в трехмерном виде, то соотношение граней фрагмента модели можно представить в виде формулы коэффициента защищенности объекта информатизации КФС.

Соответственно, коэффициент защищенности можно выразить следующей формулой:

$$K_{ABCD} = \sum_{j=1}^{m} \frac{B_1 + B_2 \ldots + B_n}{(A_{Эксп} * A_{Стат}) * K_{ущерба}}, \qquad (1)$$

где:

$A_{эксп.}$ — угроза, подсчитанная экспертным путем;

$A_{стат.}$ — угроза, подсчитанная статистическим путем;

$K_{ущерба}$ — коэффициент ущерба;

M — номер возможного последствия;

J — номер возможной угрозы;

B — весомость мероприятия по обеспечению безопасности с учетом коэффициентов, учитывающих компетентность экспертов, количество экспертов, выбравших данную меру безопасности, значимость элементов защиты, вероятность и количество угроз и величину ущерба.

Следовательно, B можно найти, произведя расчет по формуле

$$B = K_1 \times K_2 \times K_3 \times K_4 \times K_5, \qquad (2)$$

где:

K_1 — учитывает компетентность экспертов;

K_2 — количество экспертов;

K_3 — значимость элементов защиты;

K_4 — вероятность и количество угроз;

K_5 — величина ущерба.

Для того чтобы посчитать коэффициент защищенности в рассматриваемой организации, необходимо ввести численные значения для формулы (в данной работе они посчитаны методом оценки статистических данных).

K_3 — основным элементам защиты можно присвоить вес исходя из полученных данных *табл. 4*.

K_4 — угрозы (можно рассчитать по данным статистики реализации угроз, представленных на *рис. 6*, и экспертных оценок), вероятность возникновения угрозы считается статистически (берется статистика предыдущих реализаций угроз).

K_5 — величина ущерба (можно посчитать в *табл. 3*).

Весовые значения элементов защиты представлены на *рис. 7*.

При этом если дробь формулы перевернуть «кверху ногами», появляется возможность рассчитать иной показатель: коэффициент уязвимости объекта информатизации.

И тогда формула будет выглядеть подобным образом:

$$K_{ABCD} = \sum_{j=1}^{m} \frac{(A_{Эксп} * A_{Стат}) * K_{ущерба}}{B_1 + B_2 \ldots + B_n}. \qquad (3)$$

Далее перейдем к расчету коэффициента защищенности по формуле (1).

Численные значения составляющих коэффициента защищенности объекта информатизации помимо обработки статистических данных определяются с помощью и проведения экспертных опросов [18].

Как было сказано ранее, в рассматриваемой организации используются некоторые технические устройства, обеспечивающие существующий уровень безопасности на объекте.

- непрозрачное стекло на окнах;
- оптико-электронные охранные извещатели;
- видеокамеры с углом обзора 180°.

Исходя из данных *табл. 4*, присвоим каждой мере свой вес.

Даже не рассчитывая коэффициент безопасности, уже можно понять, что уровень защиты недостаточно высок, так как ни одна из представленных мер не имеет самый высокий показатель — 6 единиц.

Рис. 6 / Fig. 6. **Статистические данные реализации угроз в организации, занимающейся выдачей микрозаймов / Statistics of the implementation of threats in the microloans organization**

Источник / Source: составлено авторами / compiled by the authors.

Рис. 7 / Fig. 7. **Весовые значения элементов защиты объекта КФС / The weight values of the elements of the protection of the object CFS**

Источник / Source: составлено авторами / compiled by the authors.

Коэффициент защищенности объекта информатизации — это количественная оценка уровня безопасности объекта защиты на исследуемый момент времени в конкретных условиях его функционирования [16]. Значение коэффициента защищенности, исходя из формулы и данных, представленных в *табл. 3, 4*, будет рассчитываться следующим образом:

Переводим все численные показатели в проценты.

$$K_{ABCD} = \sum_{J-1}^{M} \frac{(83,3\times11\times12\times36)+(50\times11\times12\times36)+(66,6\times11\times12\times36)}{(45\times30)\times36} = 19,54576.$$

Итого состояние защищенности информации в кредитно-финансовой организации на данный момент времени составляет 19,5%.

Из вышеприведенных подсчетов мы можем сделать вывод, что нынешняя система защиты информации совершенно не эффективна и практически никак не соответствует предъявляемым требованиям к объектам КФС. Уровень защищенности информации в кредитно-финансовой организации не должен быть ниже 50% с учетом, что остаточные риски подлежат страхованию [19].

Для повышения уровня защищенности объекта информатизации КФС необходимо выбирать такие меры безопасности, которые «работают» на двух или трех этапах: предупреждения, пресечения и ликвидации последствий. К таким мерам можно отнести системы охранного телевидения и охранной сигнализации, а также технические средства защиты информации от утечки по техническим каналам. Внедряя наиболее эффективные меры защиты информации и рассчитывая при этом коэффициент защищенности объекта информатизации, можно создать оптимальную систему информационной безопасности.

Разработка аналогичной трехмерной модели на практике при формировании или анализе системы информационной безопасности объекта кредитно-финансовой сферы не представляет большого труда. Для этого необходимо ответить на три вопроса: что защищать? от чего или от кого защищать? как защищать? В результате модель наполняется перечнем наиболее значимых элементов защиты объекта, набором возможных угроз безопасности этим элементам защиты, возможным ущербом, который причиняют угрозы и мерами безопасности, реализованными на объекте. Чем большее количество угроз безопасности, направленных на элементы защиты, блокируется мерами безопасности (чем больше будет плюсов «+» на кубике), тем меньше ущерба причиняется объекту информатизации и меньше величина риска, которому может быть подвержен объект. А следовательно, объект лучше защищен. Коэффициент защищенности объекта информатизации подсчитывается по формуле (3).

Внедряя наиболее эффективные меры защиты информации и рассчитывая при этом коэффициент защищенности объекта информатизации, можно создать оптимальную систему информационной безопасности.

ЗАКЛЮЧЕНИЕ

В настоящее время разработаны программные продукты, позволяющие в автоматизированном режиме проводить экспертные опросы с использованием математического аппарата, обрабатывать результаты экспертизы, выводить их в виде таблиц и графиков, а также предназначенные для проведения автоматизированного анализа состояния защищенности объектов информатизации [20].

Общие требования по созданию подобных компьютерных программ должны быть направлены на решение целого ряда задач, конечной целью которых является повышение уровня информационной безопасности на объекте.

В заключение следует отметить, что на основе анализа построенной трехмерной модели и расчета коэффициента защищенности объекта создается эффективная система его информационной безопасности, проводится оптимизация выбора комплекса технических средств и методов защиты информации, позволяющих значительно сократить ущерб, возникающий из-за реализации угроз информационной безопасности.

В результате можно сделать вывод, что разработанный метод математического моделирования позволяет оценить текущий уровень информационной безопасности в любой организации кредитно-финансовой сферы.

СПИСОК ИСТОЧНИКОВ

1. Андрианов В.В., Зефиров С.Л., Голованов В.Б., Голдуев Н.А. Обеспечение информационной безопасности бизнеса. 2-е изд. М.: Альпина Паблишер; 2011.
2. Johnson J.R., Johnson R.W., Rodriguez D., Tolimieri R. A methodology for designing, modifying, and implementing Fourier transform algorithms on various architectures. *Circuits, Systems and Signal Processing*. 1990;9(4):449–500. DOI: 10.1007/BF01189337
3. Козьминых С.И. Методологические основы обеспечения комплексной безопасности объекта, фирмы, предпринимательской деятельности. М.: Моск. ун-т МВД России; 2005. 432 с.
4. Скиба В.Ю., Курбатов В.А. Руководство по защите от внутренних угроз информационной безопасности. СПб.: Питер; 2008. 235 с.
5. Акимов В.А., Лесных В.В., Радаев Н.Н. Основы анализа и управления риском в природной и техногенной сферах. М.: Деловой экспресс; 2004. 352 с.
6. Габричидзе Т.Г. Комплексная многоступенчатая система безопасности критически важных, потенциально опасных объектов. Ижевск: Научная книга; 2007. 154 с.
7. Радько Н.М., Скобелев И.О. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа. М.: Радио Софт; 2010. 234 с.
8. Farrier D.R., Durrani T.S., Nightingale J.M. Fast beam forming techniques for circular arrays. *The Journal of the Acoustical Society of America*. 1975;58(4):920–922. DOI: 10.1121/1.380745
9. Cooley J.W., Tukey J.W. An algorithm for the machine calculation of complex Fourier series. *Mathematics of Computation*. 1965;19(90): 297–301. DOI: 10.2307/2003354
10. Балдин К.В., Воробьев С.Н. Управление рисками. М.: Юнити-Дана; 2005. 512 с.
11. Емельянов А.А. Имитационное моделирование в управлении рисками. СПб.: Инжэкон; 2000. 376 с.
12. Степанов О.А., Баранов В.В., Клементьев А.С., Некишев А.В., Шмонин А.В. Актуальные проблемы противодействия преступлениям в сфере высоких технологий. М.: Акад. упр. МВД России; 2013. 124 с.
13. Hart D., Shirley G., eds. Information systems foundations: Theory, representation and reality. Canberra: ANU Press; 2007.
14. Tipton H.F., Krause M. Information security management handbook. 6th ed. Boca Raton, FL: Auerbach Publ.; 2007.
15. Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Проверка и оценка деятельности по управлению информационной безопасностью. М.: Горячая Линия — Телеком; 2012. 166 с.
16. Горошко И.В., Сичкарук А.В., Флока А.Б. Методы и модели анализа данных в правоохранительной деятельности. М.: АС-Траст; 2007. 224 с.
17. Schwartau W. On a threshold of world information war. Framingham, MA: Network World; 2007. 321 p.
18. Weidman G. Penetration testing: A hands-on introduction to hacking. San Francisco, CA: No Starch Press, Inc.; 2014. 528 p.
19. Knoke M.E., Peterson K.E., eds. Physical security principles. Alexandria, VA: ASIS International; 2015. 584 p.
20. Гусев В.С., Демин В.А., Кузин Б.И. и др. Экономика и организация безопасности хозяйствующих объектов. 2-е изд. СПб.: Питер; 2004. 288 с.

REFERENCES

1. Andrianov V.V., Zefirov S.L., Golovanov V.B., Golduev N.A. Ensuring information security of business. 2nd ed. Moscow: Alpina Publ.; 2011. (In Russ.).
2. Johnson J.R., Johnson R.W., Rodriguez D., Tolimieri R. A methodology for designing, modifying, and implementing Fourier transform algorithms on various architectures. *Circuits, Systems and Signal Processing*. 1990;9(4):449–500. DOI: 10.1007/BF01189337
3. Koz'minykh S.I. Methodological bases for ensuring complex security of an object, firm, business activity. Moscow: Moscow Univ. of the MIA of Russia; 2005. 432 p. (In Russ.).
4. Skiba V. Yu., Kurbatov V.A. A guide to protection against internal threats to information security. St. Petersburg: Piter Publ.; 2008. 235 p. (In Russ.).
5. Akimov V.A., Lesnykh V.V., Radaev N.N. Fundamentals of risk analysis and management in the natural and man-made spheres. Moscow: Delovoi ekspress; 2004. 352 p. (In Russ.).
6. Gabrichidze T.G. Complex multi-stage security system for critically important, potentially hazardous objects. Izhevsk: Nauchnaya kniga; 2007. 154 p. (In Russ.).

7. Rad'ko N.M., Skobelev I.O. Risk-models of information and telecommunication systems in the realization of threats of remote and direct access. Moscow: Radio Soft; 2010. 234 p. (In Russ.).
8. Farrier D.R., Durrani T.S., Nightingale J.M. Fast beam forming techniques for circular arrays. *The Journal of the Acoustical Society of America*. 1975;58(4):920–922. DOI: 10.1121/1.380745
9. Cooley J.W., Tukey J.W. An algorithm for the machine calculation of complex Fourier series. *Mathematics of Computation*. 1965;19(90): 297–301. DOI: 10.2307/2003354
10. Baldin K.V., Vorob'ev S.N. Management of risks. Moscow: Unity-Dana; 2005. 512 p. (In Russ.).
11. Emel'yanov A.A. Simulation modelling in risk management. St. Petersburg: ENGECON; 2000. 376 p. (In Russ.).
12. Stepanov O.A., Baranov V.V., Klement'ev A.S., Nekishev A.V., Shmonin A.V. Actual problems of counteraction to crimes in the sphere of high technologies. Moscow: Acad. of Manag. of the MIA of Russia; 2013. 124 p. (In Russ.).
13. Hart D., Shirley G., eds. Information systems foundations: Theory, representation and reality. Canberra: ANU Press; 2007.
14. Tipton H.F., Krause M. Information security management handbook. 6th ed. Boca Raton, FL: Auerbach Publ.; 2007.
15. Miloslavskaya N.G., Senatorov M. Yu., Tolstoi A.I. Inspection and assessment of information security management. Moscow: Goryachaya Liniya — Telekom; 2012. 166 p. (In Russ.).
16. Goroshko I.V., Sichkaruk A.V., Floka A.B. Methods and models of data analysis in law enforcement. Moscow: AS-Trast; 2007. 224 p. (In Russ.).
17. Schwartau W. On a threshold of world information war. Framingham, MA: Network World; 2007. 321 p.
18. Weidman G. Penetration testing: A hands-on introduction to hacking. San Francisco, CA: No Starch Press, Inc.; 2014. 528 p.
19. Knoke M.E., Peterson K.E., eds. Physical security principles. Alexandria, VA: ASIS International; 2015. 584 p.
20. Gusev V.S., Demin V.A., Kuzin B.I. et al. Economics and organization of security of business entities. 2nd ed. St. Petersburg: Piter; 2004. 288 p.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Сергей Игоревич Козьминых — доктор технических наук, профессор кафедры информационной безопасности, Финансовый университет, Москва, Россия
SIKozminykh@fa.ru

ABOUT THE AUTHOR

Sergei I. Koz'minykh — Professor, Department of Information Security, Financial University, Moscow, Russia
SIKozminykh@fa.ru

Статья поступила 07.05.2018; принята к публикации 08.10.2018.
Автор прочитал и одобрил окончательный вариант рукописи.
The article was received 07.05.2018; accepted for publication 08.10.2018.
The author read and approved the final version of the manuscript.