МЕТОДИЧЕСКИЙ ПОДХОД К ЭКОНОМИЧЕСКОЙ ОЦЕНКЕ ВНЕДРЕНИЯ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В КРЕДИТНО-ФИНАНСОВОЙ ОРГАНИЗАЦИИ

Козьминых С. И.[1]

Аннотация. *В данной статье рассмотрены меры по внедрению на объекте кредитно-финансовой сферы (КФС) технических средств защиты информации, предназначенных для снижения существующих «высоких» рисков в организации КФС до приемлемого уровня. В результате проведенного анализа были выбраны дополнительные технические средства для защиты информационных ресурсов организации, рассчитана стоимость их реализации, произведен расчет экономической эффективности рекомендуемых для внедрения технических средств защиты. Проанализирован и рассчитан ущерб, который может понести организация КФС при реализации потенциальных угроз ИБ. По результатам анализа сделан вывод о необходимости и целесообразности внедрения указанных технических средств защиты информации. Было проведено сравнение уровня риска до внедрения новых средств защиты и уровня риска после их внедрения. Также была построена экономико-математическая модель выбора оптимального набора технических средств защиты для организации КФС. Для этого изначально была построены экономико-математическая модель отбора оптимального набора проектов с оценкой NPV, выбран и описан метод решения поставленной задачи – метод Фора и Мальгранжа, сформирован алгоритм реализации применяемого метода и проведена апробация метода на примере для выбора ПАК. Дополнительно была проведена оценка срока окупаемости выбранных проектов и проиллюстрирована на графике.*

В выводах по статье сказано, что постановка и решение подобных задач могут применяться для оценки целесообразности инвестиций в потенциальные проекты с учетом ограничений бюджета, фиксированных затратах и возможной будущей прибыли организаций КФС не только в вопросах обеспечения информационной безопасности, но и в других сферах деятельности.

Ключевые слова: *информационная безопасность, экономическая эффективность, ущерб организации КФС, уровни риска, экономико-математическая модель, метод Фора и Мальгранжа, оценка срока окупаемости.*

DOI: 10.21681/2311-3456-2020-03-87-96

Введение

Внедрения новых информационных технологий во всех сферах жизни общества тесно связано с вопросами обеспечения информационной безопасности. Широкомасштабное использование вычислительной техники и телекоммуникационных технологий, переход к электронному документообороту, увеличение объемов обрабатываемой информации и расширение круга пользователей приводят к развитию новых форм несанкционированного доступа к информационным ресурсам и к их высокой уязвимости.

Компьютеризация банковской деятельности позволила внедрить новые финансовые продукты и технологии, несомненно, значительно повысить удобство пользования для клиентов и увеличить производительность труда сотрудников банка. Однако совершение преступлений в области высоких информационных технологий возрастает также быстро, как развитие банковских технологий. В настоящее время свыше 90% всех преступлений в этой области направлено на автоматизированные системы обработки информации. Это значит, что при создании и модернизации автоматизированных систем обработки информации банка (АСОИБ) необходимо уделять особое внимание обеспечению их безопасности [1].

Данная проблема является особенно актуальной в нашей стране. На Западе, как правило, для каждого банка разрабатывается индивидуальное программное обеспечение, и устройство АСОИБ составляет коммерческую тайну. В России же получили распространение «стандартные» банковские пакеты, информация о которых хоть и является конфиденциальной, но вместе с тем становится известной злоумышленникам, что увеличивает вероятность несанкционированного доступа к банковским компьютерным системам.

В данной статье рассматривается система обеспечения информационной безопасности кредитно-финансового учреждения, методы и способы защиты, связанные с осуществлением мероприятий по внедре-

1 Козьминых Сергей Игоревич, доктор технических наук, профессор, заместитель заведующего кафедрой «Информационная безопасность» Финансового университета при Правительстве Российской Федерации, г. Москва, Россия. E-mail: SIKozminykh@fa.ru; mvdprof@mail.ru

Таблица 1

Рекомендованные к реализации в кредитно-финансовой организации меры безопасности и технические средства защиты информации

Ценный актив	№ угр. ИБ	$У_р$	Уровень риска	Приемлемый риск	Меры по снижению уровня риска	Ост. риск
A – конфиденциальная информация, а также сведения, составляющие коммерческую тайну или персональные данные	04	24	Высокий	От 1 до 18	Установка систем охранного телевидения, инженерно-технической защиты. Осуществление организационных мер безопасности.	15
	08	32	Высокий	От 1 до 18	Межсетевое экранирование, применение системы доверенной загрузки, обновление антивирусной защиты. Осуществление организационных мер безопасности.	17
G – Сеть	04	24	Высокий	От 1 до 18	Совершенствование системы защиты от НСД	14
	08	32	Высокий	От 1 до 18	Обновление антивирусной защиты, использование межсетевого экранирования. Осуществление организационных мер безопасности.	18

нию технических средств обеспечению безопасности информации. Проводится расчет экономической целесообразности внедрения таких средств.

1. Внедрение технических средств, направленных на снижение уровня существующих рисков информационной безопасности в кредитно-финансовой организации

Для снижения риска информационной безопасности (ИБ) с «высокого» уровня до приемлемого в одной из кредитно-финансовых организаций было рекомендовано внедрение ряда технических средств защиты информации.

Руководителем этой организации было определено, что риск будет считаться приемлемым, если его значение в относительных единицах лежит в диапазоне от 1 до 18. После внедрения технических средств защиты информации была произведена оценка остаточного риска. Внедренные технические средства защиты информации и новые значения риска представлены в таблице 1.

Для решения поставленной задачи было предложено внедрение и установка следующих дополнительных технических средств защиты информации.

1) КриптоПро JCP

Это продукт компании КриптоПро, предназначенный для криптографической защиты информации. Реализует российские криптографические стандарты, разработан в соответствии со спецификацией JCA (Java Cryptography Architecture).

Использование КриптоПро JCP в данном случае необходимо для:

- создания и проверки электронно-цифровой подписи (ЭЦП);
- обеспечения конфиденциальности и контроля целостности информации путем шифрования;
- обеспечения аутентичности, конфиденциальности и имитозащиты соединений TLS;
- осуществления контроля целостности системного и прикладного ПО.

Стоимость лицензии начинается от 30 000 руб.

2) Электронный ключ JaCarta PKI

Токен в формате USB-носителя, который используется для аутентификации пользователей и для защищенного хранения информационных ресурсов организации. Поддерживает работу с различными цифровыми сертификатами и с электронными подписями.

Стоимость одного токена от 1550 руб.

3) Приемно-контрольный охранно-пожарный прибор Астра-712/4

Данный прибор предназначен для контроля шлейфов сигнализации с включенными в него охранными или пожарными извещателями, управления звуковыми и световыми оповещателями, выдачи извещений о нарушении режима охраны на пункт централизованной охраны.

Стоимость прибора 2600 руб.

4) Межсетевой экран Dallas Lock

Данный модуль входит в состав системы защиты конфиденциальной информации от НСД в процессе ее хранения и обработки Dallas Lock 8.0. Он предназначен для защиты рабочих станций и серверов от НСД по сети. Осуществляет контроль и фильтрацию проходящих через ПК сетевых пакетов, блокирует нежелательную сетевую активность и уведомляет о нарушениях.

При покупке от 10 лицензий стоимость системы с модулем межсетевого экрана 8 300 руб.

2. Расчет экономической эффективности применяемых средств защиты

Стоимость технических средств защиты информации, которые были ранее установлены на объекте информатизации КФС, составляет 453 620 руб.:

$$R(A,04) = 0{,}6 * 0{,}5 * 750\,000 = 225\,000 \text{ руб}$$
$$R(A,08) = 0{,}75 * 0{,}65 * 250\,000 = 121\,875 \text{ руб.}$$
$$R(G,04) = 0{,}6 * 0{,}55 * 350\,000 = 115\,500 \text{ руб.}$$
$$R(G,08) = 0{,}75 * 0{,}7 * 290\,000 = 152\,250 \text{ руб.}$$

Всего: 614 625 руб.

Таблица 2

Расчет стоимости ранее установленных технических средств защиты

Средство защиты	Количество (шт.)	Стоимость (руб.)
Электронный замок «Соболь»	3	38 250
СКЗИ «Верба-OW»	15	33 000
СКЗИ Secret Disk Server NG	3	54 000
Средство создания модели системы разграничения доступа «Ревизор 1-XP	15	18 000
Средство фиксации и контроля исходного состояния программного комплекса «ФИКС» 2.0.2	15	54 750
Программа поиска и гарантированного уничтожения информации на дисках «TERRIER» версии 3.0	15	29 250
Kaspersky Endpoint Security Cloud	1	26 370
Криптомаршрутизатор Zelax-ST	1	200 000
Итого:		453 620

Теперь рассчитаем стоимость рекомендуемых для повышения уровня информационной безопасности в организации технических средств защиты информации.

Таблица 3

Расчет стоимости рекомендуемых технических средств защиты

Рекомендуемое средство защиты	Количество (шт.)	Стоимость (руб.)
КриптоПро JCP	7	30 000
Электронный ключ JaCarta PKI	15	1 550
Приемно-контрольный охранно-пожарный прибор Астра-712/4	1	2 600
Система Dallas Lock 8.0	11	8 300
Итого:		327 150

Для того чтобы оценить целесообразность внедряемых средств защиты, необходимо рассчитать размеры ущерба, которые может понести кредитно-финансовая организация с учетом вероятности реализации угроз безопасности.

Воспользуемся данными из таблицы 3. Вероятность реализации угрозы представим в соответствующих показателях и дадим оценку стоимости ресурса. Далее сам риск R (актив, № угрозы) рассчитаем по формуле [9]:

$$R = P_В * P_у * W \quad (1)$$

Где: $P_В$ – вероятность реализации угрозы; $P_у$ – вероятность уязвимости актива; W – стоимость ценного актива. Вероятностные значения угроз и ущерба были получены экспертным путем и с использованием статистических данных.

Результаты представлены в таблице 4.

Как видно в таблице 4, величина ущерба, который может понести организация ввиду реализации потенциальных угроз ИБ, в два раза выше, чем стоимость рекомендованных технических средств защиты информации. Отсюда можно сделать вывод, что их внедрение экономически целесообразно.

При использовании новых технических средств защиты информации предполагается, что уровень риска для выбранных угроз ИБ снизится с отметки «высокого» до «приемлемого». Составим таблицу, где для каждого ценного актива и потенциальных угроз ИБ указаны уровень риска до внедрения новых средств защиты информации (ЗИ) и уровень после. Процесс изменения уровня риска также можно отобразить на гистограммах.

Благодаря предложенным для внедрения техническим средствам защиты информации была достигнута цель по снижению «высоких» рисков информационной безопасности, за счет снижения вероятности возникновения соответствующих угроз ИБ. Кроме того, на объекте был повышен уровень компетентности и осведомлённости сотрудников организации в вопросах обеспечения защиты информационных ресурсов. Таким образом за счёт проведенных мероприятий в целом был повышен уровень информационной безопасности организации.

3. Построение экономико-математической модели выбора оптимального набора средств защиты для объекта КФС

Ранее была произведена оценка экономической эффективности предлагаемых ко внедрению технических средств защиты информации. Данный расчет не предполагал условие ограниченного бюджета организации для реализации предложенных средств. Но как правило организация имеет ограниченный бюджет на подобные цели. При этом преследуется цель внедрить новый программно-аппаратный комплекс (ПАК) таким образом,

DOI:10.21681/2311-3456-2020-03-87-96

Таблица 4

Таблица оценки целесообразности внедрения рекомендуемых мер защиты

Ценный актив	№ угрозы ИБ	$P_у$	$P_в$	W (руб.)	R (руб.)
A – Конфиденциальная информация, а также сведения, составляющие коммерческую тайну или являющиеся персональными данными	04	50%	60%	750 000	225 000
	08	65%	75%	250 000	121 875
G – Сеть	04	55%	60%	350 000	115 500
	08	70%	75%	290 000	152 250
Итого:					614 625

Таблица 5

Таблица данных для построения гистограммы, отражающей процесс изменения уровня риска

Ценный актив	№ угрозы ИБ	Уровень риска до внедрения новых средств ЗИ	Уровень риска после внедрения новых средств ЗИ
A	04	24	15
A	08	32	17
G	04	24	14
G	08	32	18

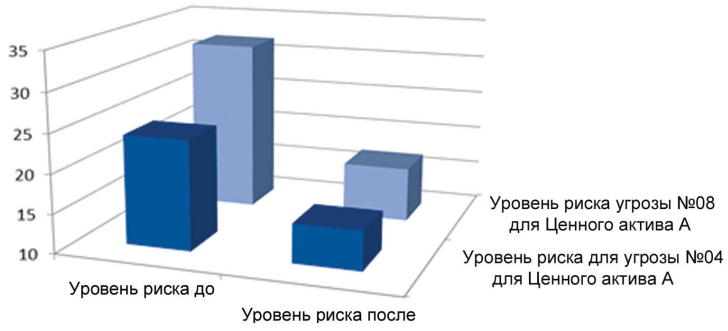

Рис.1. Изменение уровня риска для Ценного актива А

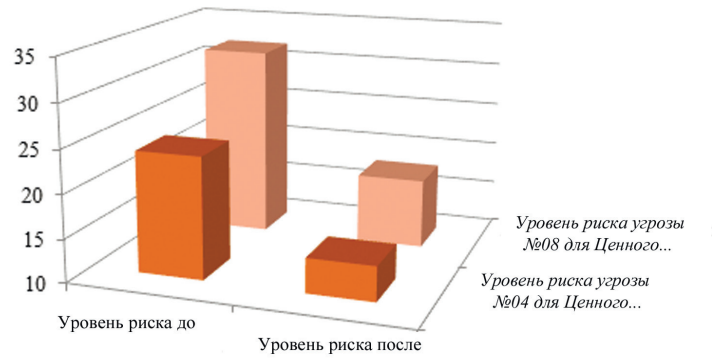

Рис. 2. Изменение уровня риска для Ценного актива G

чтобы уложиться в установленный срок (время на реализацию ограничено), с учетом ограничений на объем выделяемых инвестиций для покупки и установки ПАК при заданных размерах прибыли от каждого из рассматриваемых вариантов ПАК и затрат на их реализацию. Существует некое множество вариантов, представляющих собой различные комбинации программного обеспечения (ПО) и технических средств, которые будут входить в состав ПАК. Для дальнейшего упрощения комбинации технических средств и ПО будем называть проектами. «Проект» можно назвать инвестиционным, так как внедрение нового ПАК – это инвестиции в будущую безопасность организации. Для решения поставленной задачи предлагается составить и решить задачу оптимизации [4].

Прежде всего следует определить подзадачи, которые предстоит решить:

1. Сформировать экономико-математическую модель отбора оптимального набора проектов с оценкой NPV.
2. Выбрать и описать метод решения задачи.
3. Сформировать алгоритм реализации применяемого метода и апробировать метод на примере для выбора ПАК на объекте кредитно-финансовой сферы.

Модель поиска оптимального набора инвестиционных проектов в общем виде имеет следующий вид:

$$\sum_i^n NPV_i U_i \rightarrow max \quad (2)$$

$$\sum_i^n Z_i U_i \leq Z_0, \quad (3)$$

$$U_i = \begin{cases} 0 \\ 1 \end{cases}, i = 1,2,\ldots n, \quad (4)$$

где:

NPV_i – значение чистой текущей стоимости по каждому проекту i;

U_i – (булева) переменная, которая указывает на факт включения проекта в оптимальный план или на факт исключения;

Z_i – затраты, необходимые для реализации i-го проекта:

Z_0 – ограничение по объему возможных инвестиций;

n – количество проектов.

Иными словами, нам нужно найти такой оптимальный набор проектов, удовлетворяющий ограничениям по затратам на их реализацию и позволяющий получить максимальную прибыль. Максимальная прибыль в рамках поставленной задачи обеспечения информационной безопасности организации предполагает прибыль от осуществления непрерывной деятельности и отсутствие возможных финансовых потерь, связанных с реализацией возможных угроз ИБ.

В качестве исходных данных для задачи такого типа принимаются значения прибыли и затрат для каждого проекта. Введем следующие обозначения:

- *CO (Cash Outflow)* – исходящий денежный поток с отрицательным знаком, в рамках нашей поставленной задачи — это затраты;
- *CI (Cash Inflow)* – входящий денежный поток, имеющий положительный знак — это прибыль;
- *CF (Cash Flow)* – денежный поток, который рассчитывается по формуле:

$$CF = CI - CO \quad (5)$$

Также, как правило, имеется конкретное значение ставки дисконтирования *r* (это процентная ставка, используемая для пересчёта будущих потоков доходов в единую величину текущей стоимости).

Тогда значение NPV можно вычислить по следующей формуле:

$$NPV = \sum_{t=1}^{n} \frac{CF_t}{(1+r)^t} - IC \quad (6)$$

где:

t - количество временных периодов;

IC (Invested Capital) - начальная инвестиция в размере IC = - CF_0.

Все необходимые теоретические определения и формулы приведены, можно переходить к численному виду модели.

Исходная формулировка поставленной задачи уже была приведена. Напомним, что под проектом мы понимаем совокупность технических средств и ПО, которые будут содержаться в ПАК, внедряемом на объекте КФС [2].

Введем числовые данные. Выше была упомянута ставка дисконтирования, пусть в нашей задаче она будет равна 0,1. Ограничения по объемам инвестиций – 350 тыс. руб. По решению руководства объекта КФС внедрить новые средства защиты необходимо в течении 7 месяцев. Пусть существует 3 потенциальных проекта для повышения уровня информационной безопасности. Их состав и стоимость приведены в таблице 6, а данные об условной прибыли и затратах (предполагаем, что они складываются только из стоимости проекта, не включая иные издержки), соответствующих каждому проекту (таблица 6).

Используя все вышеприведенные формулы, проведем ряд несложных расчетов, необходимых для нахождения значения NPV для каждого проекта. На таблице 8 представлены расчеты для первого проекта, для остальных проектов все рассчитывается аналогично.

К таблице 8 следует дать некоторые пояснения:

При t=1 (в первый месяц) естественно мы не получим никакой прибыли, поэтому в этой строке ее значения равны 0. В строках далее значение прибыли за каждый месяц будет рассчитываться как сумма значений прибыли за предыдущий год и прибыли, полученной на втором году.

Столбцы, отражающие затраты на проект, имеют ненулевые значения только при t=1 - мы инвестируем в проект один раз при его запуске, далее затраты отсутствуют.

Таблица 6

Данные о проектах, потенциальных для внедрения на объекте КФС

№ проекта	Средства защиты, входящие в состав ПАК			Стоимость проекта (руб.)
	Название	Стоимость продукта (лицензии) (руб.)	Количество	
1	СКЗИ КриптоПро JCP	30 000	7	233 250
	Электронный ключ JaCarta PKI	1 550	15	
2	Приемно-контрольный охранно-пожарный прибор Астра-712/4	2 600	1	113 250
	Система Dallas Lock 8.0	8 300	11	
	Dr.Web Security Space	1 290	15	
3	СКЗИ Крипто-КОМ 3.4	150 000	1	150 000
4	Электронный ключ Рутокен ЭЦП 2.0	1 600	15	38 300
	McAfee AntiVirus Plus	1 300	11	

Таблица 7

Данные о прибыли и затратах для каждого потенциального проекта для внедрения на объекте КФС

№ проекта	Исходные данные	
	Прибыль (P_i), руб./мес.	Затраты на реализацию проекта (q_i), руб.
1	80 000	233 250
2	60 000	113 250
3	110 000	150 000
4	50 000	38 300

Таблица 8

Таблица предварительных расчетов для проекта №1

t	Прибыль	Затраты	CF	(1+r)^(1-t)	CF*disc	NPV
1	0	233 250	-233 250	1	-233 250	-233 250
2	80 000	0	80 000	0,91	72 800	-160 450
3	160 000	0	160 000	0,83	132 800	-27 650
4	240 000	0	240 000	0,75	180 000	152 350
5	320 000	0	320 000	0,68	217 600	369 950
6	400 000	0	400 000	0,62	248 000	617 950
7	480 000	0	480 000	0,56	268 800	886 750

4. CF (денежный поток) рассчитан по формуле (4).
5. Столбец disc содержит значения дисконтного множителя, рассчитанного как единица, деленная на знаменатель из формулы (5).
6. Значения в столбце NPV рассчитаны по формуле (6).

Проведя аналогичные расчеты для всех 4-х проектов, найдем итоговое значение NPV и CF. Результаты приведены в таблице 9.

Таблица 9

Таблица NPV и CF для всех проектов

t	NPV (тыс. руб.)	CF (тыс. руб.)
1	886,75	233,25
2	1 126,15	113,25
3	1 978,5	150
4	929,2	38,3

Когда все подготовительные расчеты закончены, можно построить экономико-математическую модель в численном виде по формуле (7):

$$886,75*U_1 + 1\,126,15*U_2 + 1\,978,5*U_3 + 929,2*U_4 \rightarrow max \quad (7)$$

При ограничениях на объём доступных инвестиций:

$$233,25*U_1 + 113,25*U_2 + 150*U_3 + 38,3*U_4 \leq 350\ тыс.\ руб. \quad (8)$$

При необходимости можно включить в модель ограничения, отражающие влияние внешних и внутренних факторов.

3.1. Выбор и описание метода решения поставленной задачи

Теперь, получив модель задачи в явном виде, перейдем к обзору и анализу методов, которые могут быть использованы в процессе поиска оптимального решения задачи булевого программирования.

Воспользуемся «булевыми методами». К таким относятся [5]:

- метод Фора и Мальгранжа;
- метод Лемке и Шпильберга;
- метод случайного поиска;
- метод ветвей и границ.

Рассмотрим метод Фора и Мальгранжа. Процесс поиска оптимального решения состоит из двух этапов: поиска исходного плана и его улучшения. На первом этапе ищется произвольный план, удовлетворяющий ограничениям задачи, и находится первоначальное значение целевой функции. На втором этапе значение целевой функции, полученное ранее, пытаются улучшить таким образом, чтобы новое значение стало не меньше предыдущего. Если добиться улучшения плана не удается, то он является оптимальным, иначе процесс улучшения повторяется. Важно заметить, что порядок включения булевых переменных в план определяется путем ранжирования их по возрастанию в зависимости от их «вклада» в целевую функцию.

3.2. Алгоритм метода Фора и Мальгранжа

Прежде чем изложить алгоритм, введем необходимые обозначения:

c_i – коэффициент (значения NPV для *i*-ого проекта) в полученной математической модели:

$$\sum_{i=1}^{7} c_i * a_{ji} \rightarrow max \quad (9)$$

Где:

a_{ji} – значение (1 или 0) элемента расчетной матрицы, соответствующее i-ому проекту на j-ом шаге;

b_i – коэффициент (значения CF для *i*-ого проекта) в полученной математической модели в уравнении ограничения:

$$\sum_{i=1}^{7} b_i * a_{ji} \leq B \quad (10)$$

Где:

B– ограничение значений левой части в модели.

Далее представим сам *алгоритм метода Фора и Мальгранжа*:

Произвольно находим первоначальный план, придавая каждому a_{ji} значение «1» до тех пор, пока значение целевой функции будет удовлетворять ограничению B.

Отыскиваем в нем «младшую единицу»: это крайняя правая единица, после которой имеется хотя бы один ноль. Если таковая есть – переходим к шагу 3, иначе – 5.

В новом плане все значения a_{ji} до «младшей единицы» соответствуют предыдущим, но на месте ее самой ставится 0.

Значения a_{ji} в формируемом плане правее «младшей единицы» определяются путем последовательного перебора. Присваивается значение 1, если позволяют ограничения, 0 – в противном случае.

Далее для полученного набора планов рассчитывается значение целевой функции (величины NPV). Оптимальным вариантом признается тот, у которого величина NPV максимальна.

3.3. Расчет оптимального набора проектов для кредитно-финансовой организации с оценкой NPV при помощи метода Фора и Мальгранжа.

Далее проведем расчеты для выбора оптимального набора проектов, осуществленные методом Фора и Мальгранжа.

Перед тем, как приступить к расчету по алгоритму, ранжируем имеющиеся значения NPV и CF по проектам из таблицы 9 по возрастанию, сортировка производится по столбцу NPV. Транспонируем таблицу для удобства. Результат представлен ниже:

DOI:10.21681/2311-3456-2020-03-87-96

Таблица 10

Ранжированная по значениям NPV таблица итоговых значений

t	3	2	4	1
NPV (тыс. руб.)	1 978,5	1 126,15	929,2	886,75
CF (тыс. руб.)	150	113,25	38,3	233,25

Заполним таблицу для дальнейших расчетов.

Таблица 11

Основа расчетной таблицы

Номер шага	Значения искомых переменных				Значения	
	U3	U2	U4	U1	Функции	Левой части ограничения
1	1	1	1	0	4033,85	301,55

В столбцах «Значения искомых переменных» проекты *i (Ui)* расположены согласно полученной нумерации, в них отмечаем, включается ли проект в план или нет. Первоначальный план, согласно алгоритму метода, найден случайным образом: поочередно проекты включались в план так, чтобы «Значение Левой части» не превышало ограничение (по бюджету – 350 тыс. руб.). Находим крайнюю правую единицу и далее по всем правилам просчитываем значения функции и ограничений. И так продолжаем до тех пор, пока крайних правых единиц у нас попросту не останется:

Далее в столбце «Значение Функции» находим максимальное значение NPV, которое мы можем получить, если включим в план проекты № 1 и 2. Этот план является оптимальным, т.к. удовлетворяет ограничениям поставленной задачи.

4. Оценка срока окупаемости проектов

Выбрав проекты для реализации и имея необходимые предварительные расчеты, дополнительно можно вычислить, в какой момент времени проекты начнут окупаться, т.е. когда доход от их реализации превысит соответствующие издержки. Нам понадобятся рассчитанные значения NPV для каждого момента времени (7 месяцев) для проекта №1, их мы возьмем из таблицы 12 и по такому же принципу рассчитаем значения NPV для проекта №2.

Итоговая таблица представлена ниже.

Таблица 13

Итоговая таблица NPV для проектов №1 и 2

t	NPV для проекта №1	NPV для проекта №2
1	-233 250	-53 250
2	-160 450	55 950
3	-27 650	205 350
4	152 350	385 350
5	369 950	589 350
6	617 950	812 550
7	886 750	1 126 150

Момент, когда проект становится окупаемым, – это период, когда значение NPV меняет знак с минуса на плюс. Для наглядности изобразим это на графике Рис.3.

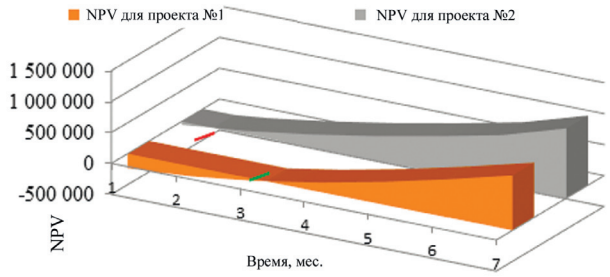

Рис 3. График оценки окупаемости проектов №1 и 2

Таблица 12

Итоговая таблица для расчета

Номер шага	Значения искомых переменных				Значения	
	U3	U2	U4	U1	Функции	Левой части ограничения
1	1	1	1	0	4033,85	301,55
2	1	1	0	0	3104,65	263,25
3	1	0	1	0	2907,70	188,3
4	1	0	0	0	1978,50	150
5	0	1	1	0	2055,35	151,55
6	0	1	0	1	2012,90	346,5

Анализируя график, можно сделать вывод о том, что проект №1 начнет окупаться между 3 и 4 месяцами, а проект №2 – между 1 и 2 месяцем после его реализации.

Таким образом, путем применения одного из методов булевого программирования, а именно метода Фора и Мальгранжа, была решена поставленная задача. По результатам расчетов был найден оптимальный набор проектов, удовлетворяющий ограничениям по затратам на их реализацию и позволяющий получить максимальную прибыль.

Построенная экономико-математическая модель отбора оптимального набора проектов, безусловно, не является полной и совершенной. Для более корректных расчетов рекомендуется дополнить модель, включив в нее факторы, отражающие информацию о текущей конкретной задаче.

Выводы

Рассмотренные меры по внедрению на объекте КФС технических средств защиты информатизации, предназначены для снижения существующих «высоких» рисков в организации КФС до приемлемого уровня. В результате проведенного анализа были выбраны дополнительные технические средства для защиты информационных ресурсов организации, рассчитана стоимость их реализации, произведен расчет экономической эффективности рекомендуемых технических средств защиты. Проанализирован и рассчитан ущерб, который может понести организация КФС при реализации потенциальных угроз ИБ. По результатам анализа был сделан вывод о необходимости и целесообразности внедрения указанных технических средств защиты информации. Было проведено сравнение уровней риска до внедрения новых средств защиты и уровня после их внедрения. Таким образом, за счёт внедрения технических средств защиты в целом был повышен уровень информационной безопасности организации КФС.

Также была построена экономико-математическая модель выбора оптимального набора технических средств защиты для организации КФС. Для этого изначально была построена экономико-математическая модель отбора оптимального набора проектов с оценкой NPV, выбран и описан метод решения поставленной задачи – метод Фора и Мальгранжа, сформирован алгоритм реализации применяемого метода и проведена апробация метода на примере выбора ПАК. Дополнительно была проведена оценка срока окупаемости выбранных проектов и проиллюстрирована на графике.

Постановка и решение подобных задач могут применяться для оценки целесообразности инвестиций в потенциальные проекты с учетом ограничений бюджета, фиксированных затратах и возможной будущей прибыли организаций КФС не только в вопросах обеспечения информационной безопасности, но и в других сферах деятельности [8].

Литература

1. Атаманов А.Н. Динамическая итеративная оценка рисков информационной безопасности в автоматизированных системах: автореферат диссертации на соискание ученой степени кандидата технических наук по специальности 05.13.19. М., 2012. 23 с.
2. Быков А.Ю., Панфилов Ф.А., Шмырев Д.В. Задача выбора средств защиты в автоматизированных системах с учетом классов защищенности от несанкционированного доступа к информации // Вестник МГТУ им. Н.Э. Баумана. Сер. «Приборостроение». 2012. С.193 – 199.
3. Быков А. Ю., Алтухов Н. О., Сосенко А. С. Задача выбора средств защиты информации в автоматизированных системах на основе модели антагонистической игры // Инженерный вестник (электронный журнал). 2014. №4. с.5
4. Баранова Е.К. Методики анализа и оценки рисков информационной безопасности // Образовательные ресурсы и технологии. 2015. № 1 (9). С. 73-79
5. Джонс К.Д., Шема М., Джонсон Б.С., Инструментальные средства обеспечения безопасности / К.Д. Джонс, М. Шема, Б.С. Джонсон. ИНТУИТ, 2007. 1028 с.
6. Зобнин, А.В. Информационно-аналитическая работа в государственном и муниципальном управлении [Электронный ресурс]: учебное пособие / М.: Вузовский учебник, 2015. — 120 с.
7. Козьминых С.И. Организация защиты информации в российской полиции. Учебное пособие. М.: ЮНИТИ-ДАНА: Закон и право, 2017. 432 с.
8. Козьминых С.И. Обеспечение комплексной защиты объектов информатизации: учебное пособие для студентов вузов, обучающихся по направлению «Информационная безопасность» квалификация «магистр» М.: ЮНИТИ-ДАНА, 2019. 543 с.
9. Овчинников А.И., Журавлев А.М., Медведев Н.В., Быков А.Ю. Математическая модель оптимального выбора средств защиты от угроз безопасности вычислительной сети предприятия // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. 2007. № 3. С. 115- 121.
10. Тищенко Е.Н. Методика оценки рисков информационной безопасности экономических информационных систем электронной коммерции. Ростов-на-Дону, 2014. 42-53 с.
11. Чибиров М.О. Об одной проблеме, возникающей при использовании теории игр в области защиты информации. М.: Проблемы информационной безопасности в системе высшей школы, 2013. 56-58 с.

Рецензент: *Дворянкин Сергей Владимирович, доктор технических наук, профессор. Профессор кафедры «Информационная безопасность» Финансового университета при Правительстве Российской Федерации, г. Москва, Россия. E-mail: SVDvoryankin@fa.ru*

METHODOLOGICAL APPROACH TO ECONOMIC ASSESSMENT IMPLEMENTATION OF TECHNICAL MEANS OF INFORMATION PROTECTION IN CREDIT AND FINANCIAL INSTITUTION

Kozminykh S.I.[2]

Abstract. *In this article, measures on introduction on object of CFS of the technical means of protection of the Informatization intended for reduction of existing «high» risks in the organization of CFS to acceptable level are considered. In the result of the analysis was chosen as an additional technical means to protect information resources of the organization, calculated the cost of their implementation, the calculation of economic effectiveness of the recommended protection tools. Analyzed and calculated the damage that can be incurred by the organization of the CFS in the implementation of potential threats to is. According to the results of the analysis, the conclusion was made about the need and expediency of the introduction of these technical means of information protection. A comparison was made between the levels of risk before the introduction of new protection and the level after their introduction. In addition, an economic and mathematical model of choosing the optimal set of technical means of protection for the organization of CFS was constructed. This was originally built economic, mathematical models of the selection of the optimal set of NPV are selected, and the method of solving the task – method fora and Malgrange, formed the algorithm of implementation of the applied method and conducted testing of the method on the example for the select PAK. Additionally, the payback period of the selected projects was estimated and illustrated on the graph.*

The conclusions of the article say that the formulation and solution of such problems can be used to assess the feasibility of investments in potential projects, taking into account budget constraints, fixed costs and possible future profits of the CFS organizations not only in matters of information security, but also in other areas of activity.

Keywords: *technical means of protection of Informatization, information security, economic efficiency, damage to the CFS organization, risk levels, economic and mathematical model, and Faure and Malgrange method, evaluation of payback period.*

References:

1. Atamanov A. N. Dynamic iterative assessment of information security risks in automated systems: author's thesis for a Ph.D. degree in engineering degree in the specialty 05.13.19. Moscow, 2012. 23 p.
2. Bykov A. Yu., Panfilov F. A., Shmyrev D. V. The problem of choosing the means of protection in automated systems taking into account the classes of protection from unauthorized access to information. Vestnik MGTU. N. E. Bauman. Ser. «Instrument making». 2012. P. 193– 199.
3. Bykov A. Yu., Altukhov N. O., Sosenko A. S. The problem of choosing the means of information protection in automated systems based on the antagonistic game model. // Engineering Bulletin # 04, April 2014. 208 p.
4. Baranova E. K. Methods of analysis and assessment of information security risks / / Educational resources and technologies. No. 1 (9). 2015. Pp. 73-79
5. Jones K. D., Shema M., Johnson B. S., security Tools/K. D. Jones, M. Shema, B. S. Johnson.- INTUIT, 2007.-1028 PP.
6. Zobnin, A.V. Information and analytical work in state and municipal management [Electronic resource]: textbook / - M.: University textbook, 2015. - 120 p.
7. Kozminykh S. I. Organization of information protection in the Russian police. Textbook. - Moscow: UNITY-DANA: Law and law, 2017.- 432 p
8. Kozminykh S. I. providing complex protection of objects of Informatization: a textbook for University students studying in the direction of «Information security» qualification «master» M.: UNITY-DANA, 2019 -543 p.
9. Ovchinnikov A. I., Zhuravlev a.m., Medvedev N. V., Bykov A. Yu. Mathematical model of optimal choice of means of protection against security threats of the enterprise computer network.Vestnik MGTU im. N. E. Bauman. Ser. Instrument making. 2007. No. 3. Pp. 115 - 121.
10. Tishchenko E. N. Methodology of risk assessment of information security of economic information systems of e-Commerce. Rostov-on-don, 2014. Pp. 42-53
11. Chibirov M. O. On a problem arising when using game theory in the field of information security. M.: Problems of information security in the system of higher education, 2013. Pp. 56-58

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