ISSN 2524-0986

iScience™

АКТУАЛЬНЫЕ НАУЧНЫЕ ИССЛЕДОВАНИЯ В СОВРЕМЕННОМ МИРЕ

ЖУРНАЛ

Выпуск 5(49)
Часть 7

Переяслав-Хмельницкий
2019

АКТУАЛЬНЫЕ НАУЧНЫЕ ИССЛЕДОВАНИЯ В СОВРЕМЕННОМ МИРЕ

ВЫПУСК 5(49)
Часть 7

Май 2019 г.

ЖУРНАЛ

Выходит – 12 раз в год (ежемесячно)
Издается с июня 2015 года

Включен в наукометрические базы:

РИНЦ http://elibrary.ru/title_about.asp?id=58411
Google Scholar

https://scholar.google.com.ua/citations?user=JP57y1kAAAAJ&hl=uk
Бібліометрика української науки
http://nbuviap.gov.ua/bpnu/index.php?page_sites=journals **Index Copernicus**
http://journals.indexcopernicus.com/++++,p24785301,3.html

Переяслав-Хмельницкий

«Актуальные научные исследования в современном мире»
Выпуск 5(49) ч. 7 ISSN 2524-0986

УДК 001.891(100) «20»
ББК 72.4
А43

Актуальные научные исследования в современном мире // Журнал - Переяслав-Хмельницкий, 2019. - Вып. 5(49), ч. 7 – 128 с.

Языки издания: українська, русский, english, polski, беларуская, казақша, o'zbek, limba română, кыргыз тили, Հայերեն

Сборник предназначен для научных работников и преподавателей высших учебных заведений. Может использоваться в учебном процессе, в том числе в процессе обучения аспирантов, подготовки магистров и бакалавров в целях углубленного рассмотрения соответствующих проблем. Все статьи сборника прошли рецензирование, сохраняют авторскую редакцию, всю ответственность за содержание несут авторы.

УДК 001.891(100) «20»
ББК 72.4
А43

СОДЕРЖАНИЕ

СЕКЦИЯ: СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Бабаев Владимир Яндашевич (Ташкент, Узбекистан)

ПРЕИМУЩЕСТВО FACEBOOK В ОТНОШЕНИИ УПРАВЛЕНИЯ

ЦЕНТРАМИ ОБРАБОТКИ ДАННЫХ…….. 5

Безсмертний Олександр Петрович,

Голян Наталія Вікторівна (Харків, Україна)

ВПЛИВ ЗАБРУДНЕННЯ ПОВІТРЯ НА ОТОЧУЮЧЕ СЕРЕДОВИЩЕ

ТА МОЖЛИВІСТЬ ЙОГО МОНІТОРИНГУ ЗА ДОПОМОГОЮ

ВЕБ-СИСТЕМИ…… 9

Дранишников Леонід Васильович (Кам'янське, Україна)

ОЦІНКА РИЗИКУ ЗА ДОПОМОГОЮ НЕЧІТКОЇ ЛОГІКИ…… 14

Қамалов Мирас Қадырғазыұлы, Оқас Айгерім Елжасқызы

(Алматы, Казахстан)

АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІҢ ӘЗЕКТІ ПРОБЛЕМАЛАРЫ НЕГІЗІНДЕ

АҚПАРАТТЫ ӘҢДЕУДІҢ ҚОРҒАЛҒАН ЖҢЙЕСІНІҢ МАҢЫЗДЫЛЫҒЫ…. 22

Кульмамиров Серик Алгожаевич,

Карюкин Владислав Игоревич (Алматы, Казахстан)

РИСКИ ЗАЩИТЫ РЕСУРСОВ ИНФОРМАЦИОННОЙ СИСТЕМЫ

ТИПОВОГО ПРЕДПРИЯТИЯ…… 26

Кирєєва Ірина Олександрівна,

Афанасьєва Ірина Віталіївна (Харків, Україна)

ПОШУК ПОСЛІДОВНИХ ШАБЛОНІВ…….. 36

Кульмамиров Серик Алгожаевич,

Алимжанова Лаура Муратбековна,

Исламгожаев Урумгали, Алимжанова Жанна Муратбековна,

Карюкин Владислав Игоревич (Алматы, Казахстан)

ПРЕИМУЩЕСТВА РОБОТОТЕХНИЧЕСКИХ КОМПЛЕКСОВ

КОНСТРУКТОРА LEGO MINDSTORMS NXT 2.0

В ПОДГОТОВКЕ ОБУЧАЮЩИХСЯ СПЕЦИАЛЬНОСТЕЙ ИКТ…… 41

Бурибаев Бакыт Бурибаевич, Кульмамиров Серик Алгожаевич,

Зулпыхаров Нуркен Тастанбекович (Алматы, Казахстан)

ПОИСК УЯЗВИМОСТИ В ТЕКСТЕ C++ СТАТИСТИЧЕСКИМ

АНАЛИЗОМ..... 53

Байганова Алтынзер Мынтургановна, Жолтаева Акпейл

(Ақтөбе, Қазақстан)

БІЛІМДІ БАҒАЛАУДА SOCRATIVE БАҒДАРЛАМАСЫ..... 63

СЕКЦИЯ: ЭКОНОМИЧЕСКИЕ НАУКИ

Воробьева Светлана Михайловна, Мурзина Милана Олеговна

(Караганда, Республика Казахстан)

СОВРЕМЕННОЕ СОСТОЯНИЕ РЫНКА ПЕРЕСТРАХОВАНИЯ

В РЕСПУБЛИКЕ КАЗАХСТАН…….. 69

«Актуальные научные исследования в современном мире»
Выпуск 5(49) ч. 7 ISSN 2524-0986

Кубік Валентина Дмитрівна (Одеса, Україна)

ПОНЯТТЯ СПРАВЕДЛИВОЇ ОЦІНКИ У ВІДПОВІДНОСТІ

ДО МІЖНАРОДНИХ СТАНДАРТІВ: ПРОБЛЕМИ ЗАСТОСУВАННЯ

В УКРАЇНІ…….. 74

Резяпова Ляйсан Фавазитовна,

Мурзагалина Гульназ Миннуловна (Стерлитамак, Россия)

ПОНЯТИЕ СЕБЕСТОИМОСТИ ПРОДУКЦИИ В ПРОИЗВОДСТВЕ

И ПУТИ ЕЕ СНИЖЕНИЯ…… 80

Спицына Дарья Викторовна (Томск, РФ)

АНАЛИЗ И ОЦЕНКА РИСКОВ ПРЕДПРИЯТИЯ АО «НПО «ВИРИОН»…. 83

Кузнецова Ирина Гарриевна,

Арюткина Анна Николаевна (Самара, Россия)

АНАЛИЗ СИСТЕМЫ СОЦИАЛЬНОГО ПАРТНЕРСТВА
В САМАРСКОЙ ОБЛАСТИ..... 89

Женсхан Дарима, Бакыт Муталипкызы (Астана, Казахстан)

ЗАРУБЕЖНЫЙ ОПЫТ ГОСУДАРСТВЕННО-ЧАСТНОГО
ПАРТНЕРСТВА И ПЕРСПЕКТИВЫ ЕГО ПРИМЕНЕНИЯ
В РЕСПУБЛИКЕ КАЗАХСТАН..... 94

Мурзагалина Гульназ Миннуловна,

Юрьев Дмитрий Андреевич (Стерлитамак, Россия)

УЧЕТНАЯ ПОЛИТИКА ОРГАНИЗАЦИИ И ЕЕ ВЛИЯНИЕ НА
ФОРМИРОВАНИЕ ФИНАНСОВЫХ РЕЗУЛЬТАТОВ ПРЕДПРИЯТИЯ..... 99

Мурзагалина Гульназ Миннуловна,

Юрьев Дмитрий Андреевич (Стерлитамак, Россия)

РОЛЬ УЧЕТНОЙ ПОЛИТИКИ ПРИ ФОРМИРОВАНИИ
БУХГАЛТЕРСКОЙ ФИНАНСОВОЙ ОТЧЕТНОСТИ..... 103

Соломина Елена Сергеевна,

Петрова Людмила Петровна (Томск, Россия)

ДРОБЛЕНИЕ БИЗНЕСА КАК УГРОЗА ЭКОНОМИЧЕСКОЙ
БЕЗОПАСНОСТИ ГОСУДАРСТВА..... 108

Толстова Алиса Захаровна,

Михайленко Яна Юрьевна (Краснодар, Россия)

ПРОБЛЕМЫ РАЗВИТИЯ ПОТРЕБИТЕЛЬСКОГО КРЕДИТОВАНИЯ
В РОССИИ..... 114

Мурзагалина Гульназ Миннуловна,

Юрьев Дмитрий Андреевич (Стерлитамак, Россия)

ПОНЯТИЕ, НАЗНАЧЕНИЕ И СОСТАВЛЕНИЕ УЧЕТНОЙ
ПОЛИТИКИ ПРЕДПРИЯТИЯ..... 118

Баладыга Элеонора Григорьевна,

Сергеева Виктория Евгеньевна (Краснодар, Россия)

РАЗВИТИЕ ПРЕДПРИЯТИЙ РЕКЛАМНОГО БИЗНЕСА

В РОССИИ: ПРОБЛЕМЫ И ПУТИ РЕШЕНИЯ…….. 122

ИНФОРМАЦИЯ О СЛЕДУЮЩЕЙ КОНФЕРЕНЦИИ..... 127

УДК 519.24:004.023:004.041

Кульмамиров Серик Алгожаевич
к.т.н., академик МАИН,
Карюкин Владислав Игоревич
Казахский национальный
университет имени аль-Фараби
(Алматы, Казахстан)

РИСКИ ЗАЩИТЫ РЕСУРСОВ ИНФОРМАЦИОННОЙ СИСТЕМЫ ТИПОВОГО ПРЕДПРИЯТИЯ

Аннотация. *В статье приводятся результаты исследований по выявлению и управлению рисков при защите информационных ресурсов (ИР) информационной системы (ИС) типового предприятия. Эти риски основаны на оценках вероятности реализации неблагоприятных событий (НС), предсказания величины ущерба от нарушений безопасности ИР и вероятности реализации угроз в системе информационной безопасности (СИБ).*

Ключевые слова: *оценка, риск, защита информации, информационные ресурсы, информационная система, ущерб, модель, система безопасности, неблагоприятное событие.*

Kulmamirov Serik Algozhaevich, Karyukin Vladislav Igorevich
Al-Farabi Kazakh National University
(Almaty, Kazakhstan)

RISKS OF PROTECTION OF INFORMATION RESOURCES TYPICAL ENTERPRISE SYSTEMS

Abstract. *The article presents the results of studies on the identification and management of risks in the protection of information resources (IR) of an information system (IS) of a typical enterprise. These risks are based on estimates of the likelihood of adverse events occurring, the prediction of the magnitude of the damage caused by the security breaches of the information security and the likelihood of threats in the information security system (ISS).*

Keywords: *assessment, risk, information protection, information resources, information system, damage, model, security system, unfavorable event.*

Основанный на рисках подход к оценке потенциального ущерба от защиты информационных ресурсов от атак нарушителей и выбору мер для минимизации риска получил название управления рисками. Под управлением рисками подразумевается полный комплекс из ряда выполняемых последовательно процессов, что соответствует существующим международным стандартам и практике управления рисками [1]:

- идентификация рисков;

- анализ рисков;
- принятие рисков;
- мониторинг и пересмотр.

В методиках управления рисками их выявление осуществляется различными путями:

- командные «мозговые штурмы»;
- составление схем последовательности процессов и деревьев событий;
- анализ архитектуры системы; - операционное моделирование; - анализ сценариев [2-3].

Одна из современных методик управления рисками основана на так называемых «экспертных оценках» [4]. Основанием анализа рисков являются данные, собранные в процессе выявления рисков, а результаты работы системного аналитика используются лицами, принимающими решения [5].

В историческом плане модели анализа и оценки рисков прошли 3 стадии развития [3]:

1) в первых моделях использовались эвристические оценки всех возможных угроз;
2) во вторых моделях (риск в области ИТ) рассматриваются случаи, когда оценка рисков исходит из стоимостной оценки ИР;
3) третье поколение моделей рассматривает управление рисками как принятие решений в условиях неопределенности, а количественные показатели риска – как критерии принятия альтернативных решений в процессе какой-либо деятельности. Неопределенность, учитываемая в моделях третьего поколения, объясняется недостаточными субъективными знаниями о предмете, в отличие от вероятности, которая является объективной мерой возможности реализации событий [3, 6].

Указанные подходы оценивания рисков имеют непосредственное приложение к решению задач обеспечения безопасности ИР, а количественные показатели рисков становятся количественными показателями безопасности ИР в информационной системе.

Риск является одним из основополагающих понятий системного анализа. Следуя подходу Кумамото и Хенли [6], а также идеям, отраженным в работе [3], можно выбрать практическое направление формального определения параметров, характеризующее риски нарушения безопасности ИР:

1) необходимо классифицировать виды атак нарушения безопасности ИР;
2) необходимо накапливать данные наблюдений относительно каждого вида атак, которые характеризуют количество атак и стоимостную оценку ущерба от нарушений безопасности ИР.

Методическая оценка ущерба в ИС от реализации неблагоприятных событий (НС) зависит от оценки риска. Оценки риска рассчитываются в зависимости от вероятности реализации таких событий в среде ИС. Различают объективные и субъективные вероятности наступления НС.

Оценка объективных вероятностей наступления НС – одна из важных задач в выборе алгоритма расчета оценок риска. Использование этих объективных оценок для повышения эффективности оценок риска в информационной системе предприятия является ключевой задачей в методике расчета оценок потенциального ущерба от атак нарушителей.

Исследуем оценку объективной вероятности реализаций неблагоприятных событий в локальной сети типового предприятия. Для этого составим список существенных видов НС, возникающих в ИС предприятия, приводящих к снижению эффективности функционирования его локальной сети (ЛВС). Пусть этот список представляет собой множество видов НС $\{O_1, O_2, \ldots, O_m\}$. Выделим из этого множества некоторое существенное подмножество некоторых видов НС, приводящих к ощутимому нарушению безопасности ИР предприятия в среде ЛВС. Это подмножество обозначим через $O \{O_{i1}, O_{i2}, \ldots, O_{im}\}$. Например, O_{i1} – количество НС относительно нарушения запуска отдельных узлов ЛВС; O_{i2} – количество НС относительно неверного набора информации применительно к конкретному информационному процессу и обработке данных и т.д.

После построения подмножества O переходим к анализу свойств элементов подмножества на основе количественных показателей НС и соответственно величины ущерба, имевшей место в прошлом. Пусть $O \{O_{i1}, O_{i2}, \ldots, O_{im}\}$ – множество всех существенных НС, приводящих к снижению системной эффективности ЛВС. Математическое ожидание ущерба, вызываемого i-м НС за время T, можно представить в виде:

$$e(O_i, T) = M[e(O_i) f_i], i = \overline{1,m}, \quad (1)$$

Здесь $e(O_i)$ – случайная величина ущерба уже случившегося НС при единичном наступлении НС; f_i – случайная величина количества НС i-го вида за время T; m – общее количество всех видов уже свершившихся НС.

Если НС не имеют последствия в том смысле, что ущерб от каждого НС независим, то справедливо выражение:

$$e(O_i, T) = M[e(O_i)]M[f_i], i = \overline{1,m}, \quad (2)$$

Тогда ущерб для всего множества существенных НС будет определяться с помощью соотношения: m

$$E(O, \Box T) \Box \Box M[e(O_i)] \Box M[\, f_i]. \quad (3)$$

$i \Box 1$

Теперь составим алгоритм оценки вероятности реализаций неблагоприятных событий в ЛВС предприятия:

Шаг 1. Рассмотрим лишь один вид НС: зафиксируем конкретное значение i = 1. Далее, количественные показатели НС, например, за $\Box$ лет сведем в таблицу 1.

Таблица 1. Количественные показатели НС, произошедших в течение последних $\Box$ лет по месяцам

t	1	2	3	4	5	6	7	8	9	10	11	12
1	$f_{1(1)}$	$f_{2(1)}$	$f_{3(1)}$	$f_{4(1)}$	$f_{5(1)}$	$f_{6(1)}$	$f_{7(1)}$	$f_{18(1)}$	$f_{9(1)}$	$f_{10(1)}$	$f_{11(1)}$	$f_{12(1)}$
2	$f_{1(2)}$	$f_{2(2}$	$f_{3(2}$	$f_{4(2)}$	$f_{5(2)}$	$f_{6(2)}$	$f_{7(2)}$	$f_{18(2)}$	$f_{9(2)}$	$f_{10(2)}$	$f_{11(2)}$	$f_{12(2)}$
?	…	…	…	…	…	…	…	…	…	…	…	…
$\Box$	$f_{1(\Box)}$	$f_{2(\Box}$	$f_{3(\Box}$	$(\Box) f_4$	$f_{5(\Box)}$	$f_{6(\Box)}$	$f_{7(\Box)}$	$f_{8(\Box)}$	$f_{9(\Box)}$	$f_{10(\Box)}$	$f_{11(\Box)}$	$f_{12(\Box)}$

Шаг 2. Исходя из данных таблицы 1, с помощью нижеприведенной формулы (4) можно получить одну строку данных усредненных помесячных количественных значений НС по столбцам (таблица 2).

$$\overline{f_{t}} \; f_{ycp} \Box \Box \Box f_{t(i)} / \Box, \; t \Box 1,12. \quad (4)$$

$i \Box 1$

Таблица 2.Усредненная строка количественных показателей произошедших НС

t	1	2	3	4	5	6	7	8	9	10	11	12
f_{tycp}	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}

Рекомендуется построить аналогичные таблицы относительно других видов НС уже реализовавшихся суммарно в течение каждого месяца.

Шаг 3. Применительно к усредненным данным таблицы 2 можно построить математическую модель в форме пространства состояний (ПС) [10], по методике, изложенной в [7]. Опишем зависимости, указанные в методике [8].

$$x(t \Box 1) \Box a \Box x(t) \Box b \Box u(t) \Box w(t), \quad x(0) \Box x_0, \quad (5)$$

$$f^{ycp}(t+1) = x(t+1)+v(t+1), \quad t = \overline{0, N-1}. \qquad (6)$$

Здесь приняты обозначения:

- $x(t)$ – истинное количество НС, произошедших в течение месяца t;
- $u(t)$ – внешнее управляющее воздействие на выявленный вид НС в период t;
- $w(t)$ – белое гауссовское ненаблюдаемое воздействие в момент времени t с нулевым математическим ожиданием и дисперсией Q;
- $x(0)$ – количество НС в начальный момент $t = 0$ с математическим ожиданием x_0 и дисперсией $P(0)$;
- a_i, b_i – неизвестные коэффициенты в динамической модели (5);
- t – номер месяца в году;
- $N = 12$ – число месяцев в году;
- $f^{ycp}(t)$ – наблюдаемое случайное количество НС в течение месяца t (эти сведения должны быть фиксированы в журнале наблюдений предприятия);
- $v(t)$ – белая гауссовская последовательность ошибок наблюдений относительно количества НС в течение каждого месяца с нулевым математическим ожиданием и дисперсией R.

На шаге 3 требуется оценить все дисперсии, связанные с шумами измерительной системы $\hat{R}$, шумами относительно модели динамики $\hat{Q}$ и шумом величины начального состояния по формулам $\hat{P}(0)$, которые изложены в работах [7-8].

Шаг 4. Оценки коэффициентов модели (5) рассчитывают на основе МНК [7].

Шаг 5. Построенные модели (5) и (6) позволят получить наиболее достоверные оценки количества НС. Преимуществом такой оценки является ее реализации использованием аппарата фильтра Калмана в режиме реального времени. Для каждого месяца можно осуществлять оценку фильтрации [7-8] за последующий «t + 1» год. Полученные оценки фильтрации рекомендуется округлить до ближайшего целого.

Оценки фильтрации позволят рассчитать объективные вероятностные оценки реализаций НС.

Например, предложим следующую процедуру расчета вероятности для конкретного вида НС: пусть нас интересует вероятность появления НС в каждом месяце предыдущего □-го года. Для этого подсчитывается общее суммарное количество НС оценок фильтрации в течение всего □-года ($F^{(□)}$). Теперь фильтрационная оценка количества НС в течение каждого месяца ($f^{(□)}(t)$) делим на общую суммарную оценку фильтрационных оценок количества НС ($F^{(□)}$) в течение одного □-года:

$$p^{(□)}(t) □ f^{(□)}(t)/ F^{(□)}, \quad t □ \overline{1,12}, \tag{7}$$

где $p_t^{(□)} □ p^{(□)}(t)$ – объективная вероятность реализации конкретного вида НС в течение каждого месяца □-года и всех 12 месяцев (результаты сведены в таблицу 3).

Таблица 3. Объективные вероятности реализаций конкретного вида НС в течение □-го года

t	1	2	3	4	5	6	7	8	9	10	11	12
$p_t(□)$	$p_1(□)$	$p_2(□)$	$p_3(□)$	$p_4(□)$	$p_5(□)$	$p_6(□)$	$p_7(□)$	$p_8(□)$	$p_9(□)$	$p_{10}(□)$	$p_{11}(□)$	$p_{12}(□)$

Тогда для □-го года запишем зависимость:

$$□ \sum_{t□1}^{12} p^{(□)}(t) □ 1, \; □□ 4, 5, ?. \tag{8}$$

Такой алгоритм подробно исследован в работе [8].

Теперь исследуем объективную стоимостную оценку предсказания величины ущерба от нарушений безопасности ИР в информационной системе предприятия. Ход исследования также представим в виде пошаговой процедуры:

Шаг 1. Пусть $O = \{O_i, i = 1, m\}$ – множество видов НС, приводящих к нарушению безопасности ИР предприятия. Предположим, что в отделе ИБ предприятия имеется статистика относительно ежемесячной оценки ущерба. Эта статистика соответствует ежемесячному количеству нарушений ИБ конкретного i -го вида атаки. Значит значениям данных таблицы 1 будет соответствовать значения данных таблицы 4.

Таблица 4. Количественные ежемесячные показатели ущерба от нарушений ИБ в зависимости от i -го вида атаки

t	1	2	3	4	5	6	7	8	9	10	11	12
1	$S_1(1)$	$S_2(1)$	$S_3(1)$	$S_4(1)$	$S_5(1)$	$S_6(1)$	$S_7(1)$	$S_8(1)$	$S_9(1)$	$S_{10}(1)$	$S_{11}(1)$	$S_{12}(1)$
?	…	…	…	…	…	…	…	…	…	…	…	…
□	$S_1(□)$	$S_2(□)$	$S_3(□)$	$S_4(□)$	$S_5(□)$	$S_6(□)$	$S_7(□)$	$S_8(□)$	$S_9(□)$	$S_{10}(□)$	$S_{11}(□)$	$S_{12}(□)$

В таблице 4 выражения $\{S_t^{(i)}, t = 1,12, i = 1, □\}$ являются выходами, которыми характеризуются ежемесячное количество ущерба от НС в ИС типового предприятия в течение каждого i -ого года.

Шаг 2. Надо отметить, что ежемесячные показатели ущерба не всегда прямо пропорциональны количеству произошедших НС. На основе данных таблицы 4 можно построить линейную модель в форме пространства состояния. Эта форма будет соответствовать усредненным данным наблюдений по столбцам относительно данных таблицы 4.

Элементы строки усредненных данных вычисляются соотношением (9) и заносится в таблицу 5:

$$\overline{s_t(y)} = (\sum S_t(□))/□, \; t = 1,12. \quad (9)$$

Таблица 5. Усредненная строка ежемесячных количественных показателей ущерба, нанесенных ИР предприятия

t	1	2	3	4	5	6	7	8	9	10	11	12

$s_{t(y)}$	$s_{1(y)}$	$s_{2(y)}$	$s_{3(y)}$	$s_{4(y)}$	$s_{5(y)}$	$s_{6(y)}$	$s_{7(y)}$	$s8(y)$	$s_{9(y)}$	$s_{10(y)}$	$s_{11(y)}$	$s_{12(y)}$

Шаг 3. На основе строки данных $\{s_{t(y)},\ t = \overline{1,12}\}$ по известным алгоритмам ([7, 8]) построим линейную модель в форме пространства состояний:

$$s(t+1) = \hat{c}s(t) + \hat{d}w(t),\quad s(0) = s_0,\quad t = \overline{0,11}, \tag{10}$$

$$s^y(t+1) = s(t+1) + v(t+1),\quad t = \overline{0,11}.$$

Сначала на основе строки данных таблицы 5 рассчитываем оценки дисперсий шумов модели вида (10) и (11), а именно оценки дисперсий Q, R, $P(0)$.

Шаг 4. Теперь рассчитываем коэффициенты модели динамики (10) через алгоритмы, приведенные в [7-8].

Шаг 5. Допустим, что располагаем данными наблюдений количественных показателей ущерба, нанесенных ИР предприятия в $\square\square\square 1\square$ году (таблица 6) и на основе фильтра Калмана рассчитаем строку оценок фильтрации вида таблицы 7.

Таблица 6. Ежемесячные количественные показатели ущерба от нарушений

ИБ предприятия в зависимости от i - го вида атаки в $\square\square\square 1\square$ году

t	1	2	3	4	5	6	7	8	9	10	11	12
$S_{t(\square)}$	$S_{1(\square)}$	$S_{2(\square)}$	$S_{3(\square)}$	$S_{4(\square)}$	$S_{5(\square)}$	$S_{6(\square)}$	$S_{7(\square)}$	$S_{8(\square)}$	$S_{9(\square)}$	$S_{10(\square)}$	$S_{11(\square)}$	$S_{12(\square)}$

Шаг 6. Используя возможности фильтра Калмана и данные таблицы 6,

получим последовательность оценок фильтрации $\{\hat{s}(t \mid t),\ t = \overline{1,12}\}$, относительно ежемесячных более достоверных количественных показателей нанесенного ущерба (таблица 7).

Таблица 7. Ежемесячные количественные показатели оценок фильтрации нанесенного ущерба в □□□1□ году

t	1	2	3	4	5	6	7	8	9	10	11	12
$s\hat{}(t \mid t)$	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8	s_9	$s10$	$s11$	$s12$

Шаг 7. Округлим следующие данные оценок фильтрации относительно количественных показателей:

- свершившихся НС в течение □□□1□ года по месяцам;
- количественные показатели ущерба, нанесенного на ресурсы предприятия в □□□1□ году (значения таблицы 7).

Шаг 8. Получим усредненный ущерб нанесенных от единичного случая

свершившегося НС $\overline{\square_{e(t),\ t\ \square 1,^{12}\square}}$. Для этого данные строки таблицы 7 разделим на соответствующие элементы строки данных количества реализации НС. Полученные расчетные данные сведем в таблицу 8.

Таблица 8. Усредненный нанесенный ущерб от единичного случая свершившегося НС

t	1	2	3	4	5	6	7	8	9	10	11	12
$e(t)$	e_1	e_2	e_3	e_4	e_5	e_6	e_7	e_8	e_9	$e10$	$e11$	$e12$

Шаг 9. Предсказывая количество НС (f_i^{pre}) i -го вида с помощью соответствующей модели и соответствующего усредненного ущерба по данным таблицы 7, можно получить оценку предсказания величины ущерба, которая будет нанесена предприятию в t месяце □□□2□ (текущего) года.

Работоспособность этого приведенного алгоритма проиллюстрирована на тестовом примере в работе [8].

Меры безопасности (контроли безопасности), применяемые в организации для ИР предприятия, можно распределить на 3 основных групп: технические, операционные и управленческие [4]. Группы в свою очередь можно разбивать на семейства. Такие эти меры безопасности в оценке ИР предприятия соблюдены требованиями стандарта NIST SP 800-30:2012. Guide for conducting Risk Assessments [9].

В группу управленческих контролей входят меры безопасности для ИС, которые сосредотачиваются на управлении рисками и безопасности ИС предприятия. Группа содержит пять семейств контролей [4, 9]. В группу

операционных контролей входят меры безопасности для ИС, которые, прежде всего, реализуются и выполняются специалистами службы ИБ предприятия. В группу входят 9 семейств контролей [4, 9]. В группу технических контролей входят меры безопасности для ИС, которые реализуются и выполняются через действия в аппаратных средствах, программном обеспечении или микропрограммных компонентах ИС предприятия. В группу входят четыре семейства контролей [4, 9].

Аналитики, которые буду проводить оценки, могут быть специалистами технической, финансовой, инженерной и управленческой специальности и профессии. Они со своими собственными индивидуальными восприятиями, отношениями и побуждениями в определении ущерба от количества реализованных НС являются работниками предприятия. Поэтому перед началом расчета величины риска и ИБ в ИС предприятия на основе экспертных оценок необходимо всем аналитикам ознакомиться со объективными оценками предсказания и фильтрации относительно ежемесячных количеств НС и ущерба от реализованных НС, которые позволят аналитикам наиболее реалистично предлагать свои экспертные оценки.

Результаты проведенных исследований показали, что процедура оценки риска на основе экспертных оценок должна быть организована по 6 этапам [4]:

1 этап. Характеристика чистемы.

2 этап. Идентификация угроз и уязвимостей.

3 этап. Оценка вероятности.

4 этап. Анализ последствия.

5 этап. Определение риска.

6 этап. Рекомендации по управлению рисками.

Например, пусть на предприятии, на котором оцениваются риски, существует три типа информационных систем: ИС-1, ИС-2, ИС-3. Аналитиками после ознакомления с результатами объективных оценок были обнаружены определенные уязвимости и угрозы, относящиеся к различным семействам контролей.

Требуется провести расчеты экспертных оценок для усвоения вышеописанной методики.

Полученные результаты исследований по оценке уровня безопасности 3 информационных систем предприятия показали следующую оценку. После ранжирования ИС предприятия по уровню риска в порядке убывания можно получить следующие расчетные данные (таблица 9).

Таблица 9. Ранги информационных систем

Информационная система	ИС-2	ИС-3	ИС-1
Уровень риска	0,453	0,446	0,410

Из таблицы 9 видно, что ИС-2 получает самый высокий уровень риска. Значит вероятность реализации угроз и ущерб для этой системы больше, чем

для остальных систем. Поэтому руководству предприятия, в первую очередь, необходимо обратить внимание на безопасность ИС-2.

Таким образом, проведенные исследования показали, что для достижения успеха в безопасности ИР в ИС предприятия, аналитик должен хорошо ориентироваться в 3 областях:

- технической или экономической теории;
- математическом моделировании, т.е. искусстве формализации постановки задачи, которое заключается в умении перевести задачу с языка проблемно-ориентированного на язык абстрактных математических схем моделей;
- соответствующем программном обеспечении ИС предприятия.

В результате сформулированы рекомендации о систематизированном изложении математических методов и моделей анализа мер безопасностей. Также было нацелено на изучение теоретических подходов и направлено на формирование практических навыков их разработки и применения к расчету рисков относительно исследуемых информационных рисков.

Рекомендации показали, что управление рисками базируется на данных, которые должны фиксироваться, накапливаться, анализироваться, храниться, обрабатываться для целей:

- оценивания потенциального ущерба от ошибок пользователей;
- фиксации атак нарушителей на ИР в ИС предприятия;
- выбора мер для его минимизации;
- расчета оценок предсказания и фильтрации всех возможных параметров и показателей, связанных с ИБ.

В итоге предложена процедура, позволяющая получать:

- оценки объективной вероятности в возможности наступления НС;
- оценки объективной стоимости ущерба от нарушений безопасности ИР в ИС предприятия;
- оценки предсказания и фильтрации величины ущерба.

Проведенные расчеты показателей безопасности ИР ИС предприятия использовали возможности линейной стохастической модели и возможностей фильтра Калмана для получения более достоверных значений оценок состояния безопасности исследуемого объекта, т.е. ИС предприятия. В процессе оценки рисков предложенной методикой учитываются взаимозависимости между мерами безопасности на типовом предприятии, что позволяет расставить приоритеты в реализации мер безопасности и разработать адекватную стратегию управления рисками.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ:

1. ISO/IEC 27005:2008. Information technology. Security techniques. Information security risk management. 2008.

2. Risk management: Implementation principles and inventories for risk management/risk assessment methods and tools ENISA (European Network and Information Security Agency). 2006.
3. Запечников С.В. Модель методической оценки возможного ущерба в ИС от реализации неблагоприятных событий// Безопасность ИТ. 2010. № 1. С. 21-27.
4. Chi-Chun Lo, Wan-Jia Chen. A hybrid information security risk assessment procedure considering interdependences between controls// Expert Systems with Applications. 2011. V.39. P.248-257.
5. Vose D. Risk analysis: a quantitative guide. 3-rd edition. John Wiley & Sons, 2008.
6. Kumamoto H., Henley E. Probabilistic risk assessment and management for engineers and scientists. 2-nd edition Institute of Electrical and Electronics Engineers. Inc.New York, 1996. - 620 p.
7. Заркумова-Райхель Р.Н., Абденов А.Ж. Прогнозирование количества инцидентов в системе ИБ предприятия при помощи динамической модели// Фундаментальные исследования. 2012. № 6 (2). С. 429-434.
8. Абденов А.Ж., Заркумова-Райхель Р.Н. Моделирование и прогнозирование количества инцидентов в системе ИБ при помощи динамической модели. Методические указания // Новосибирск: Изд-во НГТУ. 2012.
9. NIST SP 800-30:2012. Guide for conducting Risk Assessments//National Institute of Standards and Technology. – http://csrc.nist.gov/publications/PubsSPs.html. 2013.
10. Абденов А.Ж., Заркумова-Райхель Р.Н. Методика оценки рисков на основе экспертных оценок. Методические указания // Новосибирск: Изд-во НГТУ. 2013.