УДК 330.47

В.Н. Юрьев, С.А. Эрман

ТЕОРЕТИКО-ВЕРОЯТНОСТНАЯ МОДЕЛЬ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

V.N. Iur'ev, S.A. Erman

PROBABILITY-THEORETICAL MODEL OF RISK EVALUATION OF ENTERPRISE INFORMATION SECURITY

Рассматривается один из этапов создания теоретико-вероятностной модели количественной оценки рисков информационной безопасности предприятия при проведении ее аудита.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ; АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ; РИСКИ; ТЕОРИЯ ВЕРОЯТНОСТИ; МАТЕМАТИЧЕСКАЯ МОДЕЛЬ.

In the article one of the stage of development probability-theoretical model of risk quantity evaluation in audit of enterprise information security is considered.

INFORMATION SECURITY; INFORMATION SECURITY AUDIT; RISKS; THEORY OF PROBABILITY; MATH MODEL.

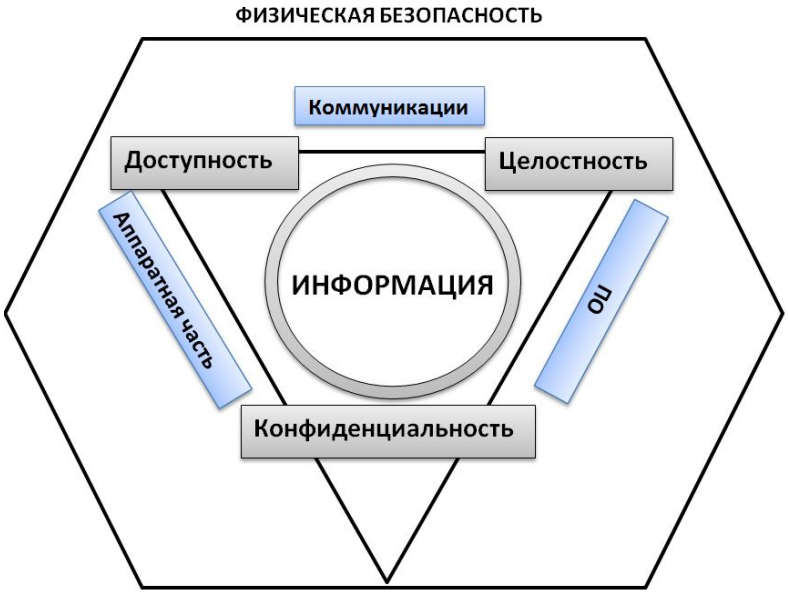
Введение. При проведении аудита информационной безопасности (ИБ) предприятия одним из важных мероприятий является анализ угроз и уязвимостей ИБ. Угроза ИБ – совокупность условий и факторов, создающих опасность нарушения информационной безопасности. Уязвимость ИБ – недостаток или слабое место в информационной системе предприятия, программно-аппаратных комплексах и прочих средствах, которые могут быть использованы для реализации угрозы ИБ. Независимо от выбранной аудиторами методики, использующей количественные (CORAS, CRAMM) или качественные (OCTAVE) оценки риска ИБ, представления об уязвимостях и угрозах должны быть четко систематизированы и структурированы. Если для методик, основная задача которых определить соответствие информационных систем предприятия любому международному стандарту ИБ, данный этап аудита имеет среднюю важность, то для методик, использующих количественную и качественную оценку риска ИБ, а также для построения собственной теоретико-вероятностной модели оценки рисков ИБ для конкретного предприятия этот этап играет ключевую роль. Он проводится после идентификации и описания бизнес-процессов, информационных активов и их ценности, а также формирования их реестра, определения соответствия требований бизнеса, законодательства текущему состоянию активов и информационных систем предприятия. Информационный актив – это материальный или нематериальный объект, который является информацией или содержит информацию, служит для обработки, хранения или передачи информации, имеет ценность для организации [1]. Инцидент информационной безопасности (information security incident) – это появление одного или нескольких нежелательных или неожиданных событий информационной безопасности, с которыми связана значительная вероятность компрометации бизнес-процессов организации [2]. Риск – это вероятность возможной

нежелательной потери чего-либо при плохом стечении обстоятельств. Под риском будем понимать произведение вероятности на убыток. Таким образом, риск информационной безопасности определяется как произведение финансовых потерь (ущерба), связанных с инцидентами безопасности, и вероятности того, что они будут реализованы [3].

Угрозы ИБ очень разнообразны. Если обратиться к таким стандартам, как BS 7799-3 и ISO-27005, BSI IT Baseline Protection Manual (Базовое руководство защиты ИТ), то становится очевидно, что таких угроз тысячи, однако на практике используется ограниченное их количество в связи со спецификой обследуемого предприятия [4]. В соответствии с моделью ИБ (см. рисунок) для каждого информационного актива или группы активов определяется список угроз в отношении конфиденциальности, целостности и доступности [5]. За основу берется модель ИБ как основа системы менеджмента информационной безопасности (СМИБ) предприятия.

Доступность – это возможность за приемлемое время получить требуемую информационную услугу. Под целостностью подразумевается актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения [6]. Конфиденциальность – это защита от несанкционированного доступа к информации. Для каждой идентифицированной (актуальной) угрозы на актив определяется список уязвимостей, из-за которых реализация угроз становится возможной [7]. Учитываются влияния техногенного, человеческого фактора, факты отсутствия или слабости применяемых механизмов контроля (организационных и технических) [5]. На последующих этапах (например, при количественной оценки риска ИБ) учитываются уже реализованные на предприятии механизмы безопасности.

Постановка задачи. При проведении аудита ИБ с количественной оценкой рисков применяется такая методика, которая рассматривает ИБ предприятия исходя из взаимодействия таких объектов, как законодательная база РФ, бизнес-процессы, информационные активы, угрозы, уязвимости, информационные системы. Для такой методики важным этапом будет выбор и построение математической модели оценки рисков ИБ. Необходимо построить математическую модель, учитывающую эти параметры. Используя теорию вероятностей и теорию управления рисками, можно построить модель, отвечающую заданным критериям.



Модель информационной безопасности

Теоретико-вероятностная модель. Согласно приведенному выше определению для вычисления количественного показателя риска можно использовать формулу

$$R(A_n) = P_{\text{общ}}(A_n) L_{\text{общ}}(A_n), \quad (1)$$

где $R(A_n)$ – количественное выражение риска на актив A_n; $P_{\text{общ}}(A_n)$ – количественная оценка возможности наступления хотя бы одного события (из всех угроз на актив A_n); $L_{\text{общ}}(A_n)$ – общая стоимость потери актива A_n, выраженная в деньгах по всем угрозам вместе.

Так как основным объектом теоретико-вероятностной модели оценки рисков ИБ является информационный актив, рассмотрим на примере нескольких информационных активов конкретного предприятия использование методики аудита ИБ на основе такой модели [8].

Эти угрозы можно разбить на две группы событий. К первой группе $P_1(A_n)$ будут принадлежать совместные и независимые события, вероятность их осуществления вычисляется согласно формуле [9]

$$P\left(\sum_{k=1}^{n} A_k\right) = \sum_{k=1}^{n} P(A_k) - \sum_{k=1}^{n-1}\sum_{j=k}^{n} P(A_k A_j) + \sum_{k=1}^{n=2}\sum_{j=k+1}^{n-1}\sum_{i=j+1}^{n} P(A_k A_j A_i) - \ldots + (-1)^n P\left(\prod_{k=1}^{n} A_k\right). \quad (2)$$

Формула для определения вероятности осуществления событий из второй группы (совместных, зависимых событий) на актив A_n будет $P_2(A_n)$ [4]:

$$P\left(\prod_{k=1}^{n} A_k\right) = P(A_1)P(A_2 \mid A_1) \times \times P(A_3|A_1A_2) \ldots P\left(A_n|\prod_{k=1}^{n-1} A_k\right). \quad (3)$$

Теоретико-вероятностная модель предполагает учитывать риск несоответствия законодательству z, требованиям бизнеса, договоров, т. е. количественному выражению вероятности его осуществления – P_z. Данная угроза влияет сразу на все направления угроз ИБ (целостность, доступность, конфиденциальность), поэтому вероятность ее осуществления необходимо учитывать при подсчете $P(A_n)$ на каждый актив. Данная вероятность определяется на основе экспертных оценок и статистических данных. Поэтому в методике предлагается вынести расчет этой вероятности на отдельный (более ранний) этап, чтобы затем использовать полученные показатели при количественной оценке риска ИБ. Таким образом, $P_{\text{общ}}(A_n) = P_1(A_n) + P_2(A_n) + P_z$, но так как данные группы событий являются совместными и независимыми, получаем [9]:

$$P_{\text{общ}}(A_n) = P_1(A_n) + P_2(A_n) + P_z - P_1(A_n)P_2(A_n) - P_1(A_n)P_z - P_2(A_n)P_z + P_1(A_n)P_2(A_n)P_z. \quad (4)$$

Необходимо отметить, что

$$L_{\text{общ}}(A_n) = C(A_n) + \ldots F(A_n),$$

где $C(A_n)$ – количественное выражение ущерба в деньгах от реализации угрозы на актив A_n; $F(A_n)$ – затраты на восстановление актива (в случае реализации угроз по доступности и целостности, а в случае реализации угрозы по конфиденциальности – затраты на принятие мер). Следовательно,

$$R(A_n) = (P_1(A_n) + P_2(A_n) + P_z - P_1(A_n) \times \times P_2(A_n) - P_1(A_n)P_z - P_2(A_n)P_z + P_1(A_n)P_2(A_n)P_z)(C(A_n) + \ldots F(A_n)). \quad (5)$$

Пример. На предприятии, занимающемся производством нескольких видов продукции, присутствует множество бизнес-процессов, самые важные из которых – работа с поставщиками, работа с клиентами, участие в тендерах, финансовое управление, бухгалтерский учет. Для обеспечения этих бизнес-процессов на предприятии налажена работа IT-сервисов, от которых зависит эффективность перечисленных процессов (доступ к корпоративному порталу, где находится база поставщиков и информация о тендерах, CRM-система предприятия, доступ к бухгалтерской базе данных, печать документов из различных систем, доступ в Интернет и т. д.). Информационными активами в данном случае будут корпоративный портал (со всеми базами данных к нему привязанными), CRM-система, бухгалтерская база данных. Рассмотрим эти активы: корпоративный портал (размещен на внутренних инфраструктурных серверах компании, имеет

Таблица 1

Некоторые угрозы уязвимостей по активу A_1

Доступность		Целостность		Конфиденциальность	
Уязвимость	Угроза	Уязвимость	Угроза	Уязвимость	Угроза
Физически незащищенная СКС	Отказ корпоративной сети	Сложный пользовательский интерфейс ПО	Ошибка оператора	Отсутствие политики регулярной смены паролей	Несанкционированный доступ
Нестабильный интернет-канал	Отказ доступа Интернет	Нет разграничения прав доступа	(Не)преднамеренная модификация данных	Отсутствие политики сложных паролей	Несанкционированный доступ
Несвоевременная оплата услуг связи	Отказ доступа Интернет	Отсутствие политик чистых рабочих столов	(Не)преднамеренная модификация данных	Отсутствие аудита попыток доступа	Несанкционированный доступ
Отсутствие ИБП и систем аварийного электропитания	Отказ телекоммуникационного и серверного оборудования, потеря данных	Отсутствие системы регулярного резервного копирования	Потеря достоверной информации, актуальных данных	Отсутствие сертификатов безопасности	Несанкционированный доступ
Отсутствие системы регулярного резервного копирования	Потеря данных			Отсутствие двухфакторной аутентификации	Несанкционированный доступ

Web-доступ через Интернет) – A_1, бухгалтерская база данных (размещена на внутренних инфраструктурных серверах компании, доступ только из корпоративной сети) – A_2, CRM-система A_3 (облачное решение, имеет интеграцию с системой 1С, размещенной в центре обработки данных провайдера услуг связи – ЦОД).

Рассмотрим актив A_1. Этот актив зависим от таких IT-сервисов, как корпоративная сеть, Интернет, печать, электронная почта, внутренний Web-сервер. Следовательно, на него будут распространяться все угрозы технического, административного и техногенного характера, влияющие на работу указанных сервисов. Некоторые угрозы и уязвимости по активу A_1 представлены в табл. 1 [5].

Эксперты оценивают текущее состояние (наличие уязвимостей, их количество и предпринятые меры) информационных систем и систем безопасности в соответствии со стандартами ИБ и на основе имеющихся всемирных статистических и данных по данному предприятию, определяют вероятности возникновения различных групп угроз на данный актив. Некоторые результаты экспертных оценок вероятностей угроз на актив A_1 (корпоративный портал) приведены в табл. 2 [5].

Угрозы по доступности и целостности можно посчитать по формуле (2)

$$P_1(A_1) = 0{,}1 + 0{,}2 + 0{,}05 + 0{,}05 + 0{,}1 + 0{,}05 + 0{,}07 + 0{,}2 - 0{,}1(0{,}2 + 0{,}05 + 0{,}05 + 0{,}1 + 0{,}05 + 0{,}07 + 0{,}2) - 0{,}2(0{,}1 + 0{,}05 + 0{,}05 + 0{,}1 + 0{,}05 + 0{,}07 + 0{,}2) - 0{,}05(0{,}1 + 0{,}2 + 0{,}05 + 0{,}1 + 0{,}05 + 0{,}07 + 0{,}2)\ 0{,}05 \cdot (0{,}1 + 0{,}2 + 0{,}05 + 0{,}1 + 0{,}05 + 0{,}07 + 0{,}2) - 0{,}1 \cdot (0{,}1 + 0{,}2 + 0{,}05 + 0{,}05 + 0{,}05 + 0{,}07 + 0{,}2) - 0{,}05(0{,}1 + 0{,}2 + 0{,}05 + 0{,}05 + 0{,}1 + 0{,}07 + 0{,}2) - 0{,}07 \cdot (0{,}1 + 0{,}2 + 0{,}05 + 0{,}05 + 0{,}1 + 0{,}05 + 0{,}2) - 0{,}2 \cdot (0{,}1 + 0{,}2 + 0{,}05 + 0{,}05 + 0{,}1 + 0{,}05 + 0{,}07) + 0{,}1 \cdot 0{,}2 \cdot 0{,}05 \times 0{,}05 \cdot 0{,}1 \cdot 0{,}05 \cdot 0{,}07 \cdot 0{,}2 = 0{,}82 - 0{,}1 \times (0{,}72) - 0{,}2 \cdot (0{,}62) - 0{,}05 \cdot (0{,}77) - 0{,}05 \cdot (0{,}77) - 0{,}1 \cdot (0{,}72) - 0{,}05 \cdot (0{,}77) - 0{,}07 \cdot (0{,}75) - 0{,}2 \cdot (0{,}62) + 2 \cdot 10^{-8} = 0{,}82 - 0{,}072 - 0{,}124 - 0{,}0385 - 0{,}0385 - 0{,}072 - 0{,}0385 - 0{,}0525 - 0{,}124 + 0 = 0{,}26.$$

Таблица 2

Результаты экспертных оценок вероятностей угроз на актив A_1

Угроза	Количество обнаруженных уязвимостей	Количество предпринятых мер	Вероятность угрозы (экспертная оценка)
Угроза доступности информации			
Отказ локальной сети	3	1	0,1
Отказ доступа Интернет	3	5	0,1
Отказ телеком и серверного оборудования	3	3	0,05
Потеря информации	7	10	0,05
Угрозы целостности информации			
Ошибки операторов	3	0	0,1
Непреднамеренная модификация данных (ошибка системы)	2	2	0,05
Преднамеренная модификация данных	5	1	0,07
Потеря актуальных копий БД	5	1	0,2
Угрозы конфиденциальности			
Несанкционированный доступ (кражи паролей, учетных записей)	10	3	0,15
Несанкционированный доступ к системе печати	3	0	0,1
Утечка информации (внутренний источник, человеческий фактор)	5	2	0,1

А для угрозы по конфиденциальности (при краже пароля вероятность несанкционированного доступа сильно возрастает, данная величина также определяется экспертной оценкой; в данном случае такая вероятность будет равна 0,7, а с учетом человеческого фактора – 0,75) условная вероятность вычисляется по формуле (3):

$$P_2(A_1 \mid B) = 0{,}15 + 0{,}7 + 0{,}75 - 0{,}15(0{,}7 + 0{,}75) - 0{,}7\,(0{,}15 + 0{,}75) - 0{,}75 \cdot (0{,}15 + 0{,}7) - 0{,}15 \cdot 0{,}7 \cdot 0{,}75 = 1{,}6 - 0{,}2175 - 0{,}63 - 0{,}6375 + 0{,}08 = 0{,}465.$$

Это означает, что в случае угрозы по конфиденциальности существует вероятность 0,15, при которой общая вероятность будет 0,465. Тогда, по формуле зависимых событий:

$$P_2(A_1 B) = 0{,}15 \cdot 0{,}465 = 0{,}07.$$

Следовательно, вероятность угрозы по конфиденциальности можно рассчитать по формуле (2) и получить результат:

$$P_2(A_1) = 0{,}15 + 0{,}1 + 0{,}1 + 0{,}07 - 0{,}15(0{,}1 + 0{,}1 + 0{,}07) - 0{,}1 \cdot (0{,}15 + 0{,}1 + 0{,}07) - 0{,}1(0{,}15 + 0{,}1 + 0{,}07) - 0{,}07(0{,}15 + 0{,}1 + 0{,}1) + 0{,}15 \cdot 0{,}1 \cdot 0{,}1 \cdot 0{,}07 = 0{,}42 - 0{,}04 - 0{,}03 - 0{,}03 - 0{,}03 = 0{,}29.$$

Для подсчета общей вероятности угроз для актива A_1 применим формулу (4). Напомним, что P_z – показатель вероятности угрозы по несоответствию законодательству и условиям ведения бизнеса. Он также определяется экспертными оценками на основе данных проведенного аудита (табл. 3).

Для данного предприятия в ходе аудита обнаружено 10 уязвимостей: лицензионное ПО рабочих станций (ОС), лицензионное ПО (ОС) серверных платформ, специализированное лицензионное ПО (СУБД, офисные пакеты приложений), криптозащиты

Таблица 3

Экспертные оценки вероятности по показателю P_z

Количество уязвимостей	Количество выполненных мер	Вероятность угрозы применения санкций (экспертная оценка)
10	21–30	0,01
10	11–20	0,25
10	Менее 10	0,5
10	Не выполняются	0,9

телекоммуникационного оборудования в соответствии со стандартами ФСТЭК и т. д. и 15 выполненных мер. По экспертным оценкам, вероятность угрозы (P_z) составляет 0,25. Таким образом, по формуле (3)

$$P_{\text{общ}}A_1 = 0{,}26 + 0{,}29 + 0{,}25 - 0{,}26(0{,}29 + 0{,}25) - 0{,}29(0{,}26 + 0{,}25) - 0{,}25(0{,}26 + 0{,}29) + 0{,}25 \cdot 0{,}26 \cdot 0{,}29 = 0{,}8 - 0{,}26 \times 0{,}54 - 0{,}29 \cdot 0{,}51 - 0{,}25 \cdot 0{,}55 + 0{,}02 = 0{,}8 - 0{,}14 - 0{,}15 - 0{,}14 + 0{,}02 = 0{,}39.$$

Равенство $P_{\text{общ}}A_1 = 0{,}39$ означает, что с вероятностью 0,39 с активом A_1 произойдет хотя бы одно неблагоприятное событие из списка всех актуальных угроз. Руководство компании оценило денежное выражение возможных потерь при реализации угроз по доступности и целостности в размере 500 000 р., а при реализации угрозы конфиденциальности – 1 млн р., эксперты оценили стоимость работ восстановления по угрозам в размере 300 000 р. и 100 000 р. соответственно. Величина вероятного ущерба по формуле $L_{\text{общ}}(A_n) = C(A_n) + \ldots F(A_n)$ (5) составит:

$$L_{\text{общ}}(A_1) = C(A_1) + F(A_1) = 1\,500\,000 + 400\,000 = 1\,900\,000 \text{ р.},$$

следовательно, риск (количественная величина), вычисленный по формуле (4),

$$R(A_1) = P_{\text{общ}}(A_1)\, L_{\text{общ}}(A_1) = 0{,}39 \cdot 1{,}9 \text{ млн р.} = 741 \text{ тыс. р.}$$

Проведя подобные вычисления для актива A_2 (бухгалтерская база данных) и для актива A_3 (CRM-система), мы получили следующие результаты.

Актив A_2 (бухгалтерская база):

$$P_1A_2 = 0{,}44; \quad P_2A_2 = 0{,}3; \quad P_z = 0{,}25;$$

$$L_{\text{общ}}A_2 = 2 \text{ млн р.} + 1 \text{ млн р.} = 3 \text{ млн р.};$$

$$P_{\text{общ}}A_2 = 0{,}44 + 0{,}3 + 0{,}25 - 0{,}44 \cdot 0{,}55 - 0{,}3 \cdot 0{,}63 - 0{,}25 \cdot 0{,}74 + 0{,}44 \cdot 0{,}3 \cdot 0{,}25 = 0{,}99 - 0{,}242 - 0{,}189 - 0{,}185 + 0{,}03 = 0{,}4.$$

$$RA_2 = 0{,}4 \cdot 3 \text{ млн р.} = 1200 \text{ тыс. р.}$$

Актив A_3 (CRM-система):

$$P_1A_3 = 0{,}11; \quad P_2A_3 = 0{,}18; \quad P_z = 0{,}25;$$

$$L_{\text{общ}}A_3 = 3 \text{ млн р.} + 2 \text{ млн р.} = 5 \text{ млн р.};$$

$$P_{\text{общ}}A_3 = 0{,}11 + 0{,}18 + 0{,}25 - 0{,}11 \cdot 0{,}48 - 0{,}18 \cdot 0{,}36 - 0{,}25 \cdot 0{,}29 + 0{,}11 \cdot 0{,}18 \cdot 0{,}25 = 0{,}54 - 0{,}05 - 0{,}07 - 0{,}07 + 0{,}01 = 0{,}36;$$

$$RA_3 = 0{,}36 \cdot 5 \text{ млн р.} = 1{,}8 \text{ млн р.}$$

Несмотря на защищенность актива A_3 относительно других активов, вероятный ущерб в случае реализации угрозы составит внушительную сумму (ввиду высокой стоимости самого актива).

Заключение. Полученные показатели можно использовать как для количественной оценки риска, так и для управления рисками и принятия решений по инвестиционным проектам в области информационной безопасности. Однако данный способ имеет и ряд недостатков. Во-первых, это точность экспертных оценок, во-вторых, при большем числе показателей (факторов) формула будет иметь слишком громоздкий вид и вычисления будут сильно затруднены без специально разработанного программного обеспечения, что не даст полной картины о рисках и финансовых потерях, связанных с нарушением ИБ. Несмотря на это, данный метод за счет математической модели позволяет гибко и взвешенно подходить к оценкам рисков ИБ при проведении аудита. В совокупности с другими количественными методами оценки риска, которые опираются на такие показатели, как ALE (оценка ожидаемых годовых потерь для одного конкретного актива от реализации одной угрозы), ROI (возврат инвестиций), NPV (чистая текущая стоимость), CVAR (условная стоимостная мера риска), TCO (совокупная стоимость владения), предложенная модель является важной ступенью этапа количественной оценки риска при проведении глубокого и детального аудита ИБ.

СПИСОК ЛИТЕРАТУРЫ

1. **Конеев И., Беляев А.** Информационная безопасность предприятия. BHV–Санкт-Петербург, 2003. 752 с.

2. **Бармен С.** Разработка правил информационной безопасности. М.: Изд. дом «Вильямс», 2002. 208 с.

3. **Бартон Т., Шенкир У., Уокер П.** Риск-менеджмент. Практика ведущих компаний: пер. с англ. М.: Изд. дом «Вильямс», 2008. 208 с.

4. Стандарты в области управления рисками информационной безопасности. URL: http://xn

----7sbab7afcqes2bn.xn--p1ai/content/standarty-v-oblasti-upravleniya-riskami-informacionnoy-bezopasnosti

5. **Астахов А.** Искусство управления информационными рисками, МК Пресс, GlobalTrust, 2009. 312 с.

6. **Поскочинова О.Г.** Проблемы реализации системных решений в области управления рисками предприятия // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Экономические науки. 2013. № 6–1 (185). С. 279–286.

7. **Антохина В.А.** Управленческая ситуация и риски // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Экономические науки. 2013. № 6–1(185). С. 287–291.

8. **Зинкевич В., Шатов Д.** Информационные риски: анализ и количественная оценка // Бухгалтерия и банки. 2007. № 1. С. 50–54.

9. **Звягин Н.П.** Математика. Теория вероятностей: практикум : учеб. пособие. СПб.: Изд-во СПбГПУ, 2011, 2012. 120 с.

10. **Игнатьев В.А.** Информационная без опасность современного коммерческого предприятия: моногр. Старый Оскол: ТНТ, 2005. 448 с.

REFERENCES

1. **Koneev I., Beliaev A.** Informatsionnaia bezopasnost' predpriiatiia. BHV–Sankt-Peterburg, 2003. 752 s. (rus)

2. **Barmen S.** Razrabotka pravil informatsionnoi bezopasnosti. M.: Izd. dom «Vil'iams», 2002. 208 s. (rus)

3. **Barton T., Shenkir U., Uoker P.** Risk-menedzhment. Praktika vedushchikh kompanii: per. s angl. M.: Izd. dom «Vil'iams», 2008. 208 s. (rus)

4. Standarty v oblasti upravleniia riskami informatsionnoi bezopasnosti. URL: http://xn----7sbab7afcqes2bn.xn--p1ai/content/standarty-v-oblasti-upravleniya-riskami-informacionnoy-bezopasnosti (rus)

5. **Astakhov A.** Iskusstvo upravleniia informatsionnymi riskami, MK Press, GlobalTrust, 2009. 312 s. (rus)

6. **Poskochinova O.G.** Implementation problems of the enterprise risk management. *St. Petersburg State Polytechnical University Journal. Economics*, 2013, no. 6–1(185), pp. 279–286. (rus)

7. **Antokhina Iu.A.** A Management Situation and Risks. *St. Petersburg State Polytechnical University Journal. Economics*, 2013, no. 6–1(185), pp. 287–291. (rus)

8. **Zinkevich V., Shatov D.** Informatsionnye riski: analiz i kolichestvennaia otsenka. *Bukhgalteriia i Banki*. 2007. № 1. S. 50–54. (rus)

9. **Zviagin N.P.** Matematika. Teoriia veroiatnostei: praktikum : ucheb. posobie. SPb.: Izd-vo SPbGPU, 2011, 2012. 120 s. (rus)

10. **Ignat'ev V.A.** Informatsionnaia bez opasnost' sovremennogo kommercheskogo predpriiatiia: monogr. Staryi Oskol: TNT, 2005. 448 s. (rus)

ЮРЬЕВ Владимир Николаевич – профессор Санкт-Петербургского государственного политехнического университета, доктор экономических наук, профессор.
195251, ул. Политехническая, д. 29, Санкт-Петербург, Россия. E-mail: yurev@fem.spbstu.ru

IUR'EV Vladimir N. – St. Petersburg State Polytechnical University.
195251. Politechnicheskaya str. 29. St. Petersburg. Russia. E-mail: yurev@fem.spbstu.ru

ЭРМАН Станислав Александрович – аспирант Санкт-Петербургского государственного политехнического университета.
195251, ул. Политехническая, д. 29, Санкт-Петербург, Россия. E-mail: ehrmann1985@gmail.com

ERMAN Stanislav A. – St. Petersburg State Polytechnical University.
195251. Politechnicheskaya str. 29. St. Petersburg. Russia. E-mail: ehrmann1985@gmail.com