УДК 321
DOI: 10.21209/2227-9245-2021-27-4-55-72

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: КРИТИЧЕСКОЕ ИССЛЕДОВАНИЕ СОДЕРЖАНИЯ УНИВЕРСИТЕТСКОЙ ПОЛИТИКИ

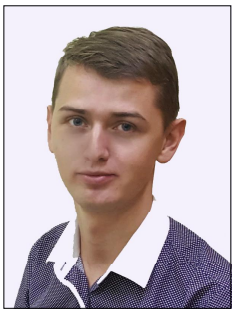
INFORMATION SECURITY POLICY: A CRITICAL STUDY OF THE CONTENT OF UNIVERSITY POLICY

Т. Е. Бейдина,
Забайкальский государственный университет, г. Чита
beydina@inbox.ru

T. Beydina,
Transbaikal State University, Chita

А. Н. Кухарский,
Забайкальский государственный университет, г. Чита
kukharskijjartjom@yandex.ru

A. Kukharsky,
Transbaikal State University, Chita



Дана оценка содержания информационной безопасности университетов. Обеспечение безопасности корпоративной информации стало чрезвычайно сложной задачей, особенно для наукоёмких организаций, таких как университеты, поскольку эффективное ведение их основной учебной и исследовательской деятельности всё больше зависит от доступности, целостности и точности компьютерных информационных ресурсов. Один из важных механизмов уменьшения количества нарушений безопасности и защиты корпоративной информации заключается в разработке и применении официальной политики информационной безопасности (ПИБ). Среди обилия публикаций о важности и роли ПИБ эмпирического материала, прямо касающегося структуры или содержания политик безопасности, немного. *Цель исследования* состоит в том, чтобы заполнить этот пробел в литературе путём критического осмысления структуры и содержания аутентичных политик информационной безопасности. В работе критически исследуется концептуализация информационной безопасности, встроенная в политику, из этого можно сделать два важных вывода: 1) разнообразие используемых разрозненных политик и стандартов вряд ли будет способствовать последовательному подходу к управлению безопасностью; 2) диапазон конкретных вопросов, явно охватываемых политикой университетов, низок и отражает в высшей степени техноцентричный взгляд на управление информационной безопасностью. Исследование представляет собой объективную, строгую и независимую оценку содержания аутентичных политик информационной безопасности и структурных схем документации по информационной безопасности в хорошо организованной организационной среде. Отмечено, что существуют четыре различных уровня информационной политики: 1) политика безопасности системы; 2) политика безопасности продукта; 3) политика безопасности сообщества и корпоративная политика информационной безопасности. Все виды политики предполагают личное использование информационных систем, раскрытие информации, физическую безопасность, нарушения и взломы, вирусы, контроль доступа к системе, мобильные вычисления, доступ в интернет, разработку программного обеспечения, шифрование и планирование на случай непредвиденных обстоятельств

Ключевые слова: *политики информационной безопасности; нарушения безопасности; содержание политики; секторы университета; информационная безопасность; университетская политика; информация; институциональное содержание; корпоративная политика; управление политикой; информационные ресурсы; технологический информационный прорыв; доступ в интернет*

The article is relevant, as it provides an assessment of the information security of universities. Ensuring the security of corporate information, which is increasingly stored, processed and disseminated using information and communication technologies (ICT). This is a particularly important problem for knowledge-intensive organizations such as universal ones; the effective conduct of their main educational activities and research activities increasingly depends on the availability, integrity and accuracy of computer information resources. One of the more important mechanisms to reduce the number of security breaches, and thus corporate information, is the

development and implementation of a formal information security policy (ISP). Although much has now been written about the importance and role of information security policies and approaches to formulating them, there is relatively little empirical material that is incorporated into the structure or content of security policies.

The purpose of the article is to fill this gap in the literature through this method of using the structure and methods of authentic information security policies. Having established the parameters and key features of university policies, the article critically examines the concept of information security embedded in the policy.

Two important conclusions can be drawn from this study: 1) the wide variety of disparate policies and standards used, whether there will be a consistent approach to security management; and 2) the range of specific issues explicitly covered by university policy, a surprisingly low and highly technocentric view of information security management. This article is one of the first to objectively, rigorously and independently assess the content of authentic information security policies and information security documentation frameworks in a well-organized organizational environment. The article notes that there are four different levels of information policy: "system security policy, product security policy, community security policy, and corporate information security policy." All policies involve: personal use of information systems, information disclosure, physical security, breaches and hacks, viruses, system access control, mobile computing, internet access, software development, encryption and contingency planning

Key words: *information security policies; security breaches; policy content; university sector; information security; university policy; information; institutional content; corporate policy; policy management; information resources; technological information breakthrough; Internet access*

Введение. Понятие информационной безопасности введено в научный оборот такими исследователями, как Портер, Миллар и Друкер, впервые признавшими, что «информационная революция произошла» и оказала значительное влияние на все аспекты жизни организации. Информация и информационные технологии могут улучшить работу организации, а также кардинально изменить организационные процессы, структуру, культуру и рабочие характеристики отдельных сотрудников. Учитывая растущее значение информации, её часто рассматривают как аналог корпоративной информации: если поток информации станет ограниченным или скомпрометированным, организация может «умереть». Но не только информация может вызвать ажиотаж в организации. Признана необходимость в управлении организационными знаниями. Появление наукоёмкой организации (НЕО) стало возможным в результате улучшений в мощности, скорости, гибкости и общей эффективности ИТ-инфраструктур.

Современное предприятие зависит от информации высокого качества, однако на практике информационные ресурсы бывают скомпрометированными из-за неприемлемо высокого уровня нарушений безопасности. Например, в Великобритании обнаружено, что количество инцидентов безопасности продолжает расти: 74 % предприятий сообщили о нарушениях в 2004 г. по сравнению с 44 % в 2000 г. [16]. Остин и Дарби (2003) отмечают, что в США нарушения безопасности ежегодно затрагивают 90 % предприятий и обходятся в 17 млрд долл. Они [28] предполагают, что защитные меры могут быть очень дорогими: «средняя компания может потратить 5…10 % своего ИТ-бюджета на безопасность».

Один из более важных механизмов защиты корпоративной информации и помощи в защите активов знаний организации заключается в формулировании и применении формальной политики информационной безопасности. Информационная безопасность определяет цели, намерения и приоритеты организации, выделяет роли, права и обязанности персонала в отношении достижения безопасности. Существуют работы, касающиеся исследований, которые непосредственно касаются объёма или содержания политик безопасности в целом, а также того, как они применяются в конкретных секторах организации, очень мало. На этом фоне *цель исследования* – заполнить этот пробел в литературе путём осмысления содержания и структуры фактических политик информационной безопасности. Исследование сосредоточено на университетах – наукоемких организациях, где качество и безопасность информационных активов должны быть приоритетными [34].

Политика информационной безопасности играет всё более важную роль в предот-

вращении, обнаружении и реагировании на нарушения. Она является важным механизмом информационной безопасности.

Задачи исследования:

– критически проанализировать общую структуру политик информационной безопасности, особенно с точки зрения количества используемых политик и их соотношения друг с другом, а также со связанными стандартами и процедурами более низкого уровня;

– рассмотреть конкретные проблемы, как показано в табл. 1, которые охватываются политиками информационной безопасности.

Таблица 1 / Table 1

Таксономия вопросов политики информационной безопасности (по Фулфорду и Доэрти [17]) / Taxonomy of Information Security Policy Issues (by Fulford and Doherty)

Проблема / Problem	**Описание / Description**
Личное использование информационных систем / Personal use of information systems	Политика информационной безопасности должна чётко определять права и обязанности отдельных сотрудников при использовании ими информационных систем организации / The information security policy should clearly define the rights and responsibilities of individual employees when they use the organization's information systems
Раскрытие информации / Disclosure information	Информационные системы предоставляют сотрудникам прямой доступ к значительным объемам информации, большая часть которой может быть конфиденциальной. Поэтому в политике безопасности должны быть указаны любые ограничения в отношении раскрытия или использования такой информации / Information systems increasingly provide employees with direct access to a significant amount of information, much of which may be confidential. Therefore, the security policy should specify any restrictions on the disclosure or use of such information
Физическая охрана инфраструктуры и информации / Physical protection of infrastructure and information	Из-за высокой стоимости аппаратное и программное обеспечение является потенциальной целью для воров. Поэтому важно, чтобы в политике были сформулированы стратегии защиты инфраструктуры и информационных ресурсов / Because of their high cost, hardware and software are potential targets for thieves. It is therefore important that policies formulate strategies to protect infrastructure and information resources
Нарушения и уничтожение безопасности / Security breaches and destruction	Поскольку нарушения безопасности по-прежнему являются обычным и потенциально опасным явлением, в документе политики должны быть указаны шаги, которые необходимо предпринять для восстановления после нарушения или уничтожения, а также требования к регистрации инцидентов безопасности / Since security breaches are still common and potentially dangerous, the policy document should specify the steps that need to be taken to recover from the breach or humiliation, as well as the requirements for recording such security incidents
Предотвращение вирусов и червей / Preventing viruses and worms	В ответ на быстрое распространение вирусов, червей и троянов политика организации должна быть чёткой в отношении применения программного обеспечения для проверки на вирусы, использования вложений и обмена информацией / In response to the rapid spread of viruses, worms, and Trojans, the organization's policies should be clear about the use of virus-scanning software, the use of attachments, and the exchange of information
Доступ пользователя к управлению / User access to management	Политика информационной безопасности должна содержать чёткое руководство по распределению средств контроля доступа и управлению ими в соответствии с бизнес-требованиями / The information security policy should provide clear guidance on the allocation and management of access controls in accordance with business requirements
Мобильные вычисления / Mobile Computing	Использование ноутбуков, карманных и портативных компьютеров вдали от традиционной рабочей среды делает их владельцев очень уязвимыми, поскольку их сложнее защитить с помощью обычных мер безопасности. Таким образом, политика должна подчёркивать позицию и методы организации в отношении безопасных мобильных вычислений / Using laptops, handhelds, and laptop computers away from a traditional work environment makes them very vulnerable, as they are more difficult to protect with conventional security measures. Thus, the policy should emphasize the organization's position and practices regarding secure mobile computing
Доступ в интернет / Internet access	Поскольку корпоративное использование интернета продолжает быстро расти, важно, чтобы политика прямо касалась проблемы доступа, особенно в отношении таких вопросов, как просмотр порнографии и личный просмотр / As corporate Internet use continues to grow rapidly, it is important that policies explicitly address the issue of Internet access, especially with regard to issues such as pornography viewing and personal browsing

Окончание табл. 1

Проблема / Problem	**Описание / Description**
Программное обеспечение и развитие / Software and Development	Многие проблемы безопасности могут быть напрямую связаны с ошибками и упущениями при разработке информационных систем, политика должна содержать руководящие принципы для обеспечения того, чтобы эффективные меры безопасности были встроены во все новые системы / Since many security issues can be directly related to errors and omissions in the development of information systems, the policy should contain guidelines to ensure that effective security measures are built into all new systems
Обслуживание / шифрование / Maintenance / Encryption:	Рост электронной коммерции и мобильных вычислений значительно увеличил объём информации, которая передаётся через общедоступные и потенциально менее безопасные сети. Следовательно, политика должна учитывать требования организации к шифрованию / защите такой информации / The growth of e-commerce and mobile computing has significantly increased the amount of information that is transmitted over public and potentially less secure networks. Therefore, the policy should take into account the organization's requirements for encrypting / protecting such information
Непрерывность и планирование / Continuity and planning	Очень важно, чтобы у всех организаций был план действий в чрезвычайных ситуациях, в котором указывалось бы, как справиться и восстановиться после серьёзного нарушения безопасности, такого как стихийное бедствие. Политика безопасности должна определять, как такие планы действий на случай непредвиденных обстоятельств должны быть написаны, протестированы, поддержаны и реализованы / It is very important that all organizations have an emergency plan that outlines how to deal with and recover from a major security breach, such as a natural disaster. The security policy should define how such contingency plans should be written, tested, maintained, and ultimately implemented

При решении названных задач мы стремились рассмотреть следующие две темы: отражают ли документы политики чисто техническую концептуализацию управления информационной безопасностью [13] и насколько они адаптированы с учётом наукоемкого контекста.

Объект исследования – информационная безопасность наукоёмких организаций, в частности университетов. *Предмет исследования* – содержание политики информационной безопасности университетов.

Методология и методика исследования. Применены системный, институциональный, информационный подходы. Для оценки университетской политики информационной безопасности использовались библиографический, компаративистский методы, а также индукции и дедукции. Структурно-функциональный ориентирован на необходимость эффективного управления информационной безопасностью университетов и целесообразность технологического и информационного прорыва. Информационный – позволил зафиксировать следование стандартам в университетской политике безопасности.

Степень изученности темы. В литературе растёт консенсус в отношении того, что политика информационной безопасности становится важным бизнес-документом, который имеет уникальные возможности для активной защиты доступности, конфиденциальности и целостности корпоративных информационных ресурсов [3; 8]. Утверждалось, что документ должен «изложить подход организации к управлению информационной безопасностью». С этой целью политика информационной безопасности должна определить индивидуальные обязанности, разрешённое и несанкционированное использование систем, предоставить сотрудникам места для сообщения об обнаруженных или предполагаемых угрозах системе, определить штрафы за нарушения и предоставить механизм для обновления политики [51].

Наиболее важной задачей политики информационной безопасности является чёткое определение конкретных прав и обязанностей отдельных пользователей и их успешная передача каждому сотруднику. [24]. Политика должна служить отправной точкой для сотрудников в отношении всех вопросов информационной безопасности [40].

Несмотря на значительный объём литературы и консенсус в отношении, важности политики, гораздо меньше внимания уделено содержанию.

Baskerville & Siponen [3] исследуют, должна ли быть единая политика или её следует подразделить на несколько отдельных уровней или типов. Другие учёные также размышляли об идеальном структурном устройстве ПИБ. Сипонен [42] предлагает модель двух категорий: «компьютерно-ориентированная и организационная политика». Стерн [45] отдаёт предпочтение трёхуровневой модели: институциональная политика, институциональный интернет-провайдер и технический интернет-провайдер. Линдуп [31] предлагает четыре различных уровня: политика безопасности системы; политика безопасности продукта; политика безопасности сообщества и корпоративная политика информационной безопасности. Линдуп [31] отмечает, что на практике организации, как правило, имеют единую корпоративную политику информационной безопасности. Другие учёные сосредоточили внимание на различии между политиками высокого уровня и практиками более низкого уровня, которые можно использовать в поддержку политики [35]. В последние годы в литературе гораздо меньше внимания уделяется наиболее эффективной конфигурации документации по информационной безопасности, но нет решения или консенсуса по этому вопросу. Ситуация значительно усложнилась из-за появления новых форм документации по безопасности: политика использования интернета и электронной почты [1]; политика в области авторского права [32]. Следовательно, существует острая необходимость в целенаправленных эмпирических исследованиях для изучения структурных механизмов в отношении фактических политик информационной безопасности, поскольку они применяются в организационном контексте.

Академическое обсуждение конкретных вопросов, рассмотренных ПИБ, представлено в литературе скудно. Международный стандарт 17799 1[1][26] даёт полезное указание на типы проблем, которые следует решать, но эти вопросы были предметом довольно ограниченного научного исследования. Одной из очень немногих попыток восполнить этот пробел было эмпирическое исследование использования политик информационной безопасности в крупных британских организациях, основанное на структуре потенциальных вопросов политики. Исследование основано на восприятии ИТ-менеджерами содержания их собственных политик, а не на объективном обзоре фактического содержания политик, чтобы обеспечить единообразие подхода и терминологии. Исследование *Fulford & Doherty* [18] фокусируется на опыте крупных организаций в целом вместо того, чтобы сосредоточиться конкретно на практике организаций. Однако таксономия *Fulford & Doherty* действительно является очень полезной отправной точкой для анализа политик информационной безопасности в нашем исследовании.

Помимо вопросов содержания и структуры политики информационной безопасности, существуют вопросы её эффективности. Подавляющее большинство организаций заявляют, что сформулировали и внедрили формальную политику информационной безопасности. Неизменно высокий уровень нарушений безопасности может ориентировать на то, что политика информационной безопасности не всегда предусматривает поставку товаров. Исследование *Doherty & Fulfor*d [15] показало, что с точки зрения количества обнаруженных нарушений безопасности не было значительной разницы между организациями, принявшими политику информационной безопасности, по сравнению с теми, у кого этого не было. Одно из возможных объяснений очевидной неэффективности политик информационной безопасности состоит в том, что они принимают очень определение информационной безопасности, которое сосредоточено только на вопросах конфиденциальности, целостности и доступности [10].

Такая техноцентричная концептуализация информационной безопасности не учитывает все важные аспекты деятельности людей и организации [13]. Поддержка этой гипотезы обеспечивается технически ориентированной концептуализацией информационной безопасности, встроенной в наиболее часто применяемый стандарт политики: он явно фокусируется на таких вопросах, как доступность, конфиденциальность и целостность данных, но игнорирует больше социально-организационных вопросов, таких как

[1] Международный стандарт ISO 17799, который мы использовали при разработке исследования, переименован в ISO / IEC 27002, но содержание его не изменилось [6].

доверие, этичность и порядочность сотрудников [12].

Ранее признано, что сбор данных от организаций, касающихся управления информационной безопасностью, может быть затруднён из-за деликатности и конфиденциальности предмета. Как указывают Котулич и Кларк, исследования информационной безопасности – «один из самых навязчивых видов исследования организации», что приводит к недоверию организаций внешним исследователям. *Kotulic & Clark* [30] предостерегают от использования почтовых опросов для сбора данных в исследованиях информационной безопасности. Исследование ИТ-безопасности, спонсируемое DTI [16], констатирует более низкий уровень ответов, поскольку потенциальные респонденты выразили обеспокоенность по поводу конфиденциальности и деликатности материалов. В нашем исследовании внимание к анализу политики позволило собрать необходимые данные непосредственно из документов политики, используемых в организациях, вместо того, чтобы полагаться на отдельных информаторов в каждой организации. Для целей исследования выбрали университеты, поскольку очень большая часть из них готова распространять свою документацию по политике информационной безопасности, размещая её на своих веб-сайтах. Процесс сбора данных повлёк за собой определение ряда университетов для исследования, ознакомление с их веб-сайтами, Университеты, включённые в исследование, отобраны из Всемирного рейтинга университетов 2007 г., подготовленного *Times Higher Education Supplement*. Этот рейтинг 200 лучших университетов мира сформировал основу выборки для исследования на пяти показателях, которые «отражают силу преподавания, исследований и международную репутацию» [53]. Согласно THES, меры, используемые для создания рейтинга, призваны быть максимально объективными и свободными от международных культурных предубеждений. Они включают экспертную оценку, количество цитирований на одного преподавателя, соотношение преподавателей и студентов, долю иностранных студентов и долю иностранных преподавателей. Использование рейтинга позволило выбрать влиятельные университеты из ряда стран.

Подход, позволивший использовать рейтинговый список 200 лучших университетов, заключается в том, чтобы сосредоточить внимание на университетах из англоязычных стран. Проведённый анализ веб-сайтов каждого университета позволил установить доступность политики информационной безопасности через их сайт. Всего в выборке использованы 122 англоязычных университета, чьи веб-сайты позволили определить, есть ли у них программный документ, доступный в режиме онлайн. Из 122 университетов 61 имеет политику, которую можно загрузить и оценить. Проверяемые документы поступают из университетов следующих стран: Соединённые Штаты Америки, Великобритания, Австралия, Канада, Новая Зеландия, Гонконг, Ирландия и Южная Африка (табл. 2).

Таблица 2 / Table 2

Разбивка по странам / Breakdown by country

Страна / Country	**Кол-во университетов в рейтинге 200 лучших / Number of universities in the Top 200 ranking**	**Количество политик, доступных онлайн / Number of policies available online**	**Процент / Percent**
США / USA	57	26	46
Англия / England	32	18	56
Австралия / Australia	12	8	67
Канада / Canada	11	6	55
Гонконг / Hong Kong	4	1	25
Новая Зеландия / New Zealand	3	1	33
Ирландия / Irish	2	1	50
Южная Африка / South Africa	1	0	0
ИТОГО / TOTAL	122	61	50

Контент-анализ нашего исследования гарантировал последовательность и точность процесса сбора данных по каждой политике информационной безопасности. Исследование включало четыре составляющие:

1) сведения об университете: имя, страна, позиция в мировом рейтинге вузов, вебсайт адрес;

2) структура политики: сведения о том, какие типы политик доступны на сайте кроме политики информационной безопасности. Какие политики включают политику допустимого использования, политику электронной торговли, политику электронной почты и политику конфиденциальности. Записан ряд дополнительных процедур или инструкций;

3) подробности администрирования политики: конкретные сведения о дате создания политики информационной безопасности, дате последнего обновления, лице / отделе, ответственном за создание политики, и лице / отделе, ответственном за управление политикой и её обслуживание;

4) страховое взаимодействие. На основе областей политики в таксономии *Fulford & Doherty* [18] включены следующие области политики: личное использование информационных систем, раскрытие информации, физическая безопасность, нарушения и взломы, вирусы, контроль доступа к системе, мобильные вычисления, доступ в интернет, разработка программного обеспечения, шифрование и планирование на случай непредвиденных обстоятельств [см. табл. 1]. Если в политике указывалось явное взаимодействие области, то записывались следующие дополнительные сведения об этой области: лицо / лица, ответственные за область действия политики; действующие запреты, относящиеся к этой области; разрешения, предоставленные в отношении этой области; и наложенные штрафы в случае нарушения политики. Дополнительные поля доступны в проформе для записи любых других относящихся к делу подробностей о каждой области политики. Мы стремились идентифицировать любые явные ссылки на цели безопасности или безопасность знаний. Данные собирали путём изучения и перевода распечаток каждой политики по очереди. Содержание анализа затем сводили в таблицы для проведения сравнения.

Вступительный анализ в каждой политике явился полезным средством раскрытия широких взглядов университета в отношении информационной безопасности. Некоторые из них сосредоточились на защите оборудования, компьютерных залов и других аспектах физической безопасности. Другие больше беспокоились о защите конфиденциальности и целостности своих административных информационных систем и административных данных. Третьи подчёркивали важность информации для исследований, и поэтому, их внимание концентрировалось на защите такой информации и обеспечении того, чтобы их правила управления безопасностью помогали исследованиям процветать и быть защищёнными от атак.

Как указывалось ранее, литература по формулированию политики информационной безопасности предполагает, что организации обычно применяют один из трёх основных подходов к структуре и формату своей документации по политике безопасности. Первый из них заключается в создании единой всеобъемлющей политики информационной безопасности, содержащей подробный охват каждой из областей риска и каждой проблемы управления безопасностью, относящейся к рассматриваемой организации [30]. Второй – в создании серии взаимосвязанных политик с перекрёстными ссылками: например, отдельных систем, продуктов, сообществ и корпоративных информационных политик [3]. Третий – в формулировании политики информационной безопасности, дополненной рядом соответствующих руководств или процедур, обычно каждый руководящий или процедурный документ сосредоточен на одном конкретном аспекте управления безопасностью [12; 39].

Результаты обзора университетской документации по информационной безопасности показали, что большинство университетов предпочитают иной подход (табл. 3). Как правило, университеты имеют политику информационной безопасности, сопровождаемую рядом связанных политик, дополняемую рядом конкретных руководств и/или документов, связанных с практикой. Наиболее типичная комбинация – политика информационной безопасности, сопровождаемая политикой допустимого использования и политикой электронной почты. Политика допустимого использования, как правило, охватывает вопросы разрешений и запретов на использование университетских вычислительных

средств отдельными членами университета. Политика электронной почты сосредоточена на вопросах разрешений, запретов в отношении отправки массовых электронных писем большому количеству университетского сообщества и писем, не связанных с работой; вопросах, ориентированных на мониторинг электронной почты со стороны университетского руководства; вопросах удаления и хранения электронной почты. Дополнительные руководящие принципы и/или процедуры имели тенденцию решать проблемы с сильной технической ориентацией, например, разрешения и запреты на подключение портативных компьютеров к сетям организации; стандарты систем и сетевой безопасности; использование беспроводных технологий и утилизация оборудования и программного обеспечения; вопросы, связанные с мониторингом электронной почты со стороны университетского руководства, а также с удалением и хранением электронной почты.

Таблица 3 / Table 3

Политики и руководящие принципы/процедуры / Policies and guidelines/procedures

Тип политики / Type of policy	**Общие показатели / General indicators**	**Страны / Countries**							
		США / USA	Англия / England	Австралия / Australia	Канада / Canada	Гонконг / Hong Kong	Новая Зеландия / New Zealand	Ирландия / Irish	Южная Африка / South Africa
Политика информационной безопасности / Information Security Policy	61	26	18	8	6	1	1	1	1
Политика допустимого использования / Acceptable Use Policy	52	20	17	8	4	1	1	1	1
Политика электронной почты Email Policy	35	13	12	6	1	1	1	1	1
Политика авторских прав / Copyright Policy	17	7	6	3	1	0	0	0	0
Политика конфиденциальности / Privacy Policy	16	11	2	2	0	1	0	0	0
Политика защиты данных / Data Protection Policy	11	9	0	1	1	0	0	0	0
Политика публикации в интернете / Online Publishing Policy	7	2	3	3	0	0	0	0	1
Веб и доменные имена / Web and domain names	6	1	3	1	0	1	0	0	0
Политика закупок / Procurement Policy	6	5	4	0	0	0	1	1	0
Политика электронной коммерции / E-commerce Policy	3	3	0	0	0	0	0	0	0
Политика инфраструктуры / Infrastructure Policy	3	0	2	0	0	1	0	0	0
Свобода информации / Freedom of information	1	1	0	0	0	0	0	0	0
Другие инструкции /процедуры / Other instructions /procedures	33	17	11	2	1	1	0	0	1

Помимо наличия политики допустимого использования и политики электронной почты замечено, что университеты в США с большей вероятностью имеют политику конфиденциальности, чем университеты других стран в нашей выборке. Например, только 2 из 18 выбранных университетов Великобритании имели политику конфиденциальности по сравнению с 21 из 26 университетов США. Эти политики, как правило, охватывают вопросы, касающиеся прав на защиту конфиденциальности как данных, так и электрон-

ных сообщений, которые пользователи могут ожидать как члены университетского сообщества; а также действий, которые университет уполномочен предпринимать в отношении мониторинга и проверки данных.

Анализ конкретных вопросов управления безопасностью, рассматриваемых в документации по безопасности университетов, учитывал только основную политику информационной безопасности вуза, поэтому любые дополнительные политики/руководящие принципы/процедуры не рассматривались в явном виде. Каждая политика информационной безопасности подверглась тщательному пересмотру, чтобы определить охват ключевых областей риска/проблем управления безопасностью, отмеченных *Fulford & Doherty* [18]. В некоторых случаях политика могла отсылать читателя к дополнительной политике, и в этом случае это считалось явным охватом, поскольку ориентир исходил из основной политики информационной безопасности. Вопросы, рассматриваемые в отдельных политиках или процедурах, но не упомянутые явно в политике информационной безопасности, не рассматривались как явное.

Результаты этой части исследования показали, во-первых, что ни одна отдельная область политики не является общей для всех университетов в выборке. Наиболее широко освещаемые в порядке убывания проблемы касались следующих вопросов: нарушения и уничтожение; управление доступом пользователей; планирование на случай непредвиденных; и физическая безопасность (табл. 4). Правдоподобное объяснение высокого ранжирования нарушений и управления доступом пользователей состоит в том, что учреждения имеют ряд типов пользователей (исследовательский персонал, преподавательский состав, административный и канцелярский вспомогательный персонал, разрозненный состав студентов). Широкий диапазон типов пользователей влечёт потребность в множестве различных точек доступа к информационным системам и сетям организации: офисы персонала, компьютерные лаборатории, беспроводной доступ, исследовательские лаборатории, студенческие общежития и удалённый доступ. Большое разнообразие точек доступа может сделать информационные системы университета, а также данные и информацию, содержащиеся в них, уязвимыми для нарушений безопасности. Диапазон местоположений, в которых доступны вычислительные мощности в университетах, также может служить объяснением достаточно высокого рейтинга, показанного в исследовании физической безопасности (4-е место).

Таблица 4 / Table 4

Охват политик ИБ / Coverage of information security policies

Проблема безопасности / Security issue	**Охват интернет-провайдерами / Internet Service Provider Coverage**	**Охват, % / Coverage, %**
Нарушения и уничтожение / Violations and destruction	51	84
Управление доступом пользователей / Managing user access	44	72
Планирование на случай непредвиденных ситуаций / Contingency planning	31	51
Физическая защита / Physical protection	29	48
Раскрытие информации / Disclosure of information	22	36
Вирусы, черви и т. д. / Viruses, worms, etc.	21	34
Шифрование / Encryption	14	15
Мобильное обеспечение / Mobile Software	11	18
Разработка программного обеспечения / Software Development	10	16
Использование информации в личных целях / Use of information for personal purposes	8	13
Доступ в интернет / Internet access	5	8
Дополнительные вопросы / Additional questions		
Обязанности / Responsibilities	41	67
Правоприменение / Law enforcement	33	54

Окончание табл. 4

Проблема безопасности / Security issue	Охват интернет провайдерами / Internet Service Provider Coverage	Охват, % / Coverage, %
Осведомлённость и обучение / Awareness and training	23	38
Соблюдение законодательства / Compliance with the law	21	34
Классификация информации / Classification of information	13	21
BS (1) 7799 отсылка / BS (1) 7799 Reference	12	20

Области, получившие наименьшее освещение в политике информационной безопасности университетов, изученные в ходе исследования: разработка и сопровождение программного обеспечения (9-е место) из 11 областей политики; использование информационных систем в личных целях (10-е место), доступ в интернет (11-е место). Низкий рейтинг таких областей, как личное использование информационных систем и доступ в интернет, можно объяснить тем, что они охвачены отдельными процедурами и/или руководящими принципами: «приемлемое использование», а также политика электронного письма – в ряде университетов выборки. Однако мы утверждаем, что если такие вопросы адекватно освещены в другом месте, на них всё равно следует ссылаться в политике информационной безопасности, чтобы она сохраняла своё положение в качестве центральной точки отсчёта для всех проблем безопасности. Разработка программного обеспечения рассматривается только в некоторых университетских политиках информационной безопасности в образце и не рассматривается в значительной степени в связанных политиках и/или процедурах. Это, возможно, связано с тем, что разработка систем считается специализированной деятельностью, которая обычно не имеет отношения к более широкой организации. Однако это может быть опасной стратегией, поскольку университеты, как правило, предоставляют членам своего сообщества определённую свободу для создания собственного программного обеспечения. Например, если исследовательские группы разрабатывают собственные простые приложения для баз данных, чтобы хранить и анализировать исследовательские данные, по-прежнему важно, чтобы такие приложения были надлежащим образом защищены. Личное использование также может иметь относительно низкий рейтинг, поскольку университеты обычно обладают высоким уровнем гибкости, особенно в ролях, связанных с исследованиями в отношении рабочего времени и методов работы, а границы между личным использованием и деятельностью, связанной с работой, иногда могут быть размыты. Следовательно, строгое регулирование личного использования ИТ в университетском контексте затруднительно, особенно в ролях, ориентированных на исследования в отношении рабочего времени и методов работы, а границы между личным использованием и рабочей деятельности размыты.

В дополнение к областям политики, определённым Фулфорд и Доэрти [18]: из нашего анализа отдельных политик безопасности университетов в выборке очевидно, что ряд других областей явно не охвачен. Наиболее распространённый дополнительный вопрос – обязанности сотрудников в отношении информационной безопасности, и это является положительным открытием, поскольку поддерживает точку зрения Гастона [18], что хорошо составленная политика должна «распределять обязанности различных отделов и отдельных лиц в достижении целей политики».

Однако нет смысла чётко разграничивать обязанности, если сотрудникам не разъясняется, как они будут нести ответственность за увольнение, поэтому обнадеживает тот факт, что многие университеты теперь четко формулируют, как их политика будет применяться (табл. 4).

Ещё одна важная область, которой уделяется большое внимание во многих, но далеко не всех политиках, это обучение информационной безопасности и осведомлённость о политике безопасности. Это справедливо для всех различных стран в выборке, за исключением США, где были свидетельства того, что меньше внимания уделялось обучению и осведомленности о безопасности, а больше внимания отводили вопросам конфиден-

циальности, мониторинга, интеллектуальной свободы. Растущий акцент на обучении и осведомлённости о безопасности является обнадеживающим открытием, поскольку, если пользователи не будут знать о содержании своей политики, она, скорее всего, станет недействующим документом [42], что менее обнадеживает, так это то, что политики информационной безопасности, как правило, охватывают лишь небольшую часть областей, определённых в структуре, предложенной *Fulford & Doherty* [18], и то, что охват все ещё имеет тенденцию ограничиваться, даже когда вся документация по информационной безопасности для каждого учреждения проверяется целиком (т. е. дополнительные политики, а также дополнительные процедуры и/или руководящие принципы).

Что касается основных целей управления информационной безопасностью [12], отражённых в политиках информационной безопасности, то, как видно из данных, представленных в табл. 5, существует высокая степень согласованности, очень сильная техническая ориентация; заявленные цели сосредоточены на вопросах необходимости строгого контроля доступа и первостепенной важности обеспечения максимальной конфиденциальности и целостности их информационных активов. Гораздо менее явное внимание уделялось социально-организационным аспектам информационной безопасности, таким как необходимость развития человеческих ресурсов и методов управления или необходимость создания и поддержания этической среды. Аналогичная тенденция обнаружена при изучении андерлаинга, принципов [10], которые отражены в содержании нашего образца политик. Особое внимание уделялось доступности информации, конфиденциальности и честности, но очень мало свидетельств явного беспокойства о доверии, этичности или организационной целостности. Один повторяющийся принцип, имевший более социально-организационную направленность, – это обязанность, поскольку почти во всех рассмотренных политиках чётко определены конкретные обязанности различных сотрудников или групп сотрудников в отношении поддержания информационной безопасности.

Таблица 5 / Table 5

Заявленные цели политик информационной безопасности / Declared Objectives of Information Security Policies

Цели политик информационной безопасности (на основе Dhillon & Torkzadeh, 2006) / Information Security Policy Objectives (based on Dhillon & Torkzadeh, 2006)	**Количество политик / Number of policies**
Улучшение практики развития менеджмента / Improving management development practices	14
Обеспечение адекватных методов управления человеческими ресурсами / Ensuring adequate human resource management practices	0
Создание и поддержание этической среды / Creating and maintaining an ethical environment	0
Максимизация контроля доступа / Maximizing access control	44
Содействие индивидуальной трудовой этике / Maximizing access control	9
Максимизация целостности данных / Maximizing data Integrity	36
Повышение целостности бизнес-процессов / Improving business process integrity	31
Повышение конфиденциальности / Improving privacy	28
Максимизация организационной целостности / Maximizing organizational integrity	0

Доказательства явной адаптации политики информационной безопасности с учётом статуса университетов нашей выборки оказались крайне сложными. Лишь четыре из рассмотренных политик (7 %) содержали какое-либо явное признание того, что информационной безопасности следует уделять особенно высокий приоритет из-за статуса наукоёмкой принимающей организации. Существующие ссылки обычно ограничивались краткими заявлениями во введении к политике, например: «информация является жизненно важным активом для любой организации, особенно в такой организации, основанной на знаниях, как университет». Не было абсолютно никаких свидетельств, что какой-либо университет явно приспосабливал конкретные вопросы политики с учётом наукоёмкого контекста, в котором их политика будет применяться.

Нами проведено сравнение областей политики университета с областями, охваты-

ваемыми крупными коммерческими организациями, исследованными *Fulford & Doherty* [18] (табл. 6). Есть существенные различия как в рейтинге распространённости конкретных политических проблем, так и в общих уровнях охвата. Очевидно, что политика предыдущего исследования, как правило, охватывала более широкий круг вопросов, чем те, которые рассматривались в рамках нашей выборки университетской политики. Вероятность того, что конкретная проблема будет рассмотрена в исходной выборке, составляла 0,74, в нашей выборке университетской политики она составляла лишь 0,36.

Таблица 6 / Table 6

Контент политики для университетов по сравнению с контентом политики для крупных организаций, % / Policy content for universities versus policy content for large organizations, %

Область политики / Policy area	**Содержание политики в университетах / Content of policy in universities**	**Содержание политики в целом по организациям [Фулфорд и Доэрти, 2003] / The content of policy in general for organizations [Fulford and Doherty, 2003]**
Нарушения и уничтожение / Violations and destruction	84 (1)	85 (4)
Управление доступом пользователей / Managing user access	72 (2)	91 (1)
Планирование на случай непредвиденных нарушений / Planning for unexpected violations	51 (3)	56 (8)
Физическая охрана / Physical security	48 (4)	83 (5)
Раскрытие информации / Disclosure of information	36 (5)	82 (6)
Вирусы, черви и т.д. / Viruses,worms, etc	34 (6)	87 (3)
Шифрование / Encryption	23 (7)	35 (10)
Мобильные вычисления / Mobile Computing	18 (8)	61 (7)
Разработка программного обеспечения / Software Development	16 (9)	53 (9)
Использование информации в личных целях / Use of information for personal purposes	13 (10)	87 (3)
Доступ в интернет / Access to the Internet	8 (11)	90 (2)
Примечание: цифры в скобках относятся к относительному рангу каждой области политики / Note: The numbers in parentheses refer to the relative rank of each policy area		

Между двумя выборками наиболее заметные различия в охвате доступа в интернет (11-е место) в университете тех, кто учится, в исследовании других организаций и личном использовании ИБ (10-е место) в вузе, учебе и совместной выборке в исследованиях других организаций. Эти различия можно объяснить замечаниями, сделанными ранее в этом разделе относительно гибкости использования ИТ и методов работы в организациях, а также диапазоном типов пользователей в таких учреждениях. Поскольку рабочая среда в университетах, как правило, отличается высокой степенью гибкости и границы между работой и личным использованием могут иногда стираться, университетам может быть трудно регулировать эти области. В качестве альтернативы может оказаться, что университеты предпочтут сосредоточить внимание на вопросах личного использования и доступа в интернет, сделав их предметом отдельной политики (например, политики допустимого использования).

Различия в используемых методологиях исследования могут также объяснить некоторую разницу в охвате университетской документации по информационной безопасности и документации других организаций. В этом исследовании, ориентированном на университет, использовался метод объективного стороннего анализа политической документации. В отличие от этого исследование в

других организациях проводилось с использованием анкетных опросов, зависящих от информатора в каждой организации, чтобы обеспечить надежную и правдивую информацию об охвате управления безопасностью их организации. Возможно, эти респонденты считали охват своей организации более обширным, чем на самом деле. Однако проверить это проблематично, поскольку коммерческие организации, в отличие от университетов, не склонны обнародовать свои конфиденциальные данные.

Заключение. Сосредоточив внимание на содержании документации по безопасности, ориентированной на сотрудников, исследование помогает преодолеть одно из наиболее распространённых критических замечаний в отношении исследований в области информационной безопасности за то, что они излишне технические по своей направленности. Цель работы состоит в том, чтобы чётко сформулировать вклад исследования, прежде чем определять его значение для менеджера и исследователя.

Результативность исследования заключается в предоставлении независимого и объективного обзора охвата политиками информационной безопасности, в констатации того, что охват политиками информационной безопасности с точки зрения количества явно решаемых проблем обычно довольно скромен, особенно если сравнивать с предписаниями из литературы и международными стандартами. Обнаружено, что документы по политике информационной безопасности эффективно играют свою роль в координации пакета документации по безопасности организации, поскольку они не содержат адекватных ссылок на дополнительные политики и стандарты. Если эти результаты указывают на более широкую тенденцию, это может объяснить растущее беспокойство, которое многие комментаторы выражают по поводу эффективности политик информационной безопасности. Исследование представляет эмпирические данные о продолжающихся дебатах по поводу «идеальных структурных мер в отношении документации по безопасности». Хотя исследование выявило разнообразие практик, наиболее распространённой схемой является широкая политика информационной безопасности высокого уровня при поддержке.

Важным вкладом исследования стала оценка основных целей и принципов управления информационной безопасностью, что отражено в политике информационной безопасности. Возможно, наш образец политик все ещё отражает высоко техноцентричный взгляд на управление информационной безопасностью, учитывая техническую направленность большинства стандартов безопасности, это подчёркивает необходимость как для учёных, так и для практиков изучать способы, с помощью которых социально-организационные аспекты информационной безопасности могут быть лучше отражены в политических документах. Теоретический вклад исследования заключается в том, что мы сосредоточили внимание на университетах, которые сталкиваются со сложной проблемой безопасности компьютерных активов. С одной стороны, информацию и знания следует рассматривать как высоко конкурентный ресурс, конфиденциальность которого должна быть строго защищена, а с другой – если эти активы свободно делятся между коллегами, их ценность вряд ли будет использована. Исследование не даёт никаких свидетельств ни по используемому языку, ни по охвату вопросов, чтобы предположить, что университеты адаптировали свою политику для отражения статуса наукоёмких организаций; с другой стороны – если эти активы не будут свободно делиться между коллегами, то их ценность вряд ли будет увеличена.

Университетам необходимо критически пересмотреть свою политику, чтобы гарантировать, что охват является всеобъемлющим и специально разработанным с учётом критической роли информации о работе академика. Более того, в среде, где количество различных соответствующих документов быстро растёт, политика информационной безопасности должна вернуть себе первенство, в котором она выступает в качестве отправной точки для всех других процедур и политик. Изучение имеет важные последствия для исследователя не только с точки зрения его нового понимания объёма и охвата, но и в отношении формулирования политики информационной безопасности. Баскервиль и Сипонен ранее подчёркивали значительный пробел в литературе в отношении подходов к формулированию политики информационной безопасности. Одна из основных причин того, что эта конкретная литература

недостаточно развита, может быть связана с отсутствием ясности в отношении структуры и охвата документации по безопасности. Заключительный вклад исследования может сводиться к предоставлению чётких эмпирических данных в отношении содержания политик информационной безопасности, которые могут быть использованы для помощи и информирования при создании новых подходов к формулированию будущих политик информационной безопасности.

Работа представляет собой объективную и независимую оценку содержания аутентичных политик информационной безопасности и структурных схем документации по ней в организационной среде. При этом подчёркиваются некоторые вызывающие беспокойство недостатки с точки зрения чёткого охвата вопросов политики и способности организаций эффективно сопоставлять и интегрировать свои портфели документации по информационной безопасности. Исследование принятия сложных политик в динамичном организационном контексте является амбициозным мероприятием и поэтому имеет ряд присущих ему ограничений. В частности, принятие формата опроса ограничивает круг вопросов и конструкций, которые могут быть изучены, и не даёт исследователю возможности выяснить, почему были приняты конкретные решения в отношении структуры и охвата политики.

Список литературы

1. Arnesen D. W. & Weis, W. L. Developing an effective company policy for employee internet and email use // *Journal of organizational culture, communications and Conflict*, 2007, 11. P. 53–67.

2. Austin R. D. & Darby, C. A. The Myth of Secure Computing. *Harvard Business Review*, 2003, 81. P. 120–126.

3. Baskerville R. & Siponen, M. An information security meta-policy for emergent organizations // *Information Management and Computer Security*, 2002,15, P. 337–346.

4. Besnard D. & Arief, B. Computer security impaired by legitimate users // *Computers & Security*, 2004, 23. P. 253–264.

5. Brynjolfsson E. & Hitt L. Paradox Lost? Firm-Level Evidence on the Returns to Information Systems // *Management Science,* 1996, 42. P. 541–558.

6. Calder A Van Bom, J. *Implementing Information Security Based on ISO 27001/ISO 17799.* Van Haren Publishing, 2006.

7. Churchill Gilbert A. Jr *Marketing Research, Methodological Foundations*. The Dryden Press, 1997.

8. David J. Policy enforcement in the workplace // *Computers and Security,* 2002, 21. P. 506–513.

9. Desouza K. C. & Vanapalli G.K. Securing knowledge in organizations: lessons from the defence and intelligence sectors // *International Journal of Information Management,* 2005, 25. P. 85–98.

10. Dhillon G. *Managing Information Systems Security*, Macmillan Press, London, 1997.

11. Dhillon G. & Backhouse J. Information System Security Management in the New Millennium // *Communications of the ACM*, 2000, 43. P. 125–128.

12. Dhillon G. Realizing Benefits of an information security program // *Business Process Management Journal,* 2004, 10, P. 21–22.

13. Dhillon G. & Torkzadeh G. Value-Focused Assessment of Information System Security in Organizations // *Information Systems Journal,* 2006, 16, p. 293–314.

14. Doherty N. F., King M. & Al-Mushayt O. The impact of inadequacies in the treatment of organizational issues on information systems development projects, *Information and Management,* 2003, 41, p. 49–62.

15. Doherty N. F. & Fulford H. Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis // *Information Resources Management Journal,* 2005, 18, p. 21–38.

16. D. T. I. *Information security breaches survey*, Department of Trade & Industry, *2004.*

17. Drucker P. F. The Coming of the New Organization // *Harvard Business Review,* 1988, 66, p. 45–53.

18. Fulford H. & Doherty N. F. The application of information security policies in large UK-based organizations // *Information Management and Computer Security*, 2003, 11, p. 106–114.

19. Gaston S. J. *Information Security: Strategies for Successful Management*. Toronto: CICA, 1996. P. 18.

20. Garg A., Curtis J. & Halper H. Quantifying the financial impact of information security breaches // *Information Management and Computer Security,* 2003, 11, p. 74–83.

21. Hagen J.M., Albrechtsen E. & Hovden J. Implementation and effectiveness of organizational information security measures // *Information Management & Computer Security*, 2008, 16, p. 377–397.

22. Higgins H. N. Corporate system security: towards an integrated management approach // *Information Management and computer Security*, 1999, 7, p. 217–222.

23. Hinde S. Security surveys spring crop // *Computers and Security*, 2002, 21, p. 310–321.

24. Hone K. & Eloff J. H. P. Information security policy- what do international security standards say // *Computers & Security*, 2002, 21, p. 402–409.

25. Hone K. & Eloff J. H. P. What makes an effective information security policy // *Network Security,* 2002, 20, p. 14–16.

26. Hong K., Chi Y. Chao L. & Tang, J. An empirical study of information security policy on information security elevation on Taiwan // *Information Management and Computer Security, 2006, 14, p. 104–115.*

27. I.S.O Information technology – Security Techniques – Code of practice for information security management – ISO 17799. International Standards Organization, Geneva, 2005.

28. Johannessen J-A, Olsen B. Knowledge Management and sustainable competitive advantages: The impact of dynamic contextual training // *International Journal of Information Management*, 2003, 23, p. 277–289.

29. Karyda M. Kiountouzis E. & Kokolakis S. Information security policies: a contextual perspective // *Computers & Security*, 2005, 24, p. 246–260.

30. Kotulic A. J. & Clark J. G. Why there aren't more information security research studies // *Information and Management*, 2004, 41, p. 597–607.

31. Lindup K. R. A new model for information security policies // *Computers & Security*, 1995, 14, p. 691–695.

32. Loggie K. A., Barron A. E., Gulitz E., Hohlfield T. N., Kromrey J.D. & Venable M. An analysis of Copyright policies for distance learning materials at Major Research Universities // *Journal of Interactive Online Learning*, 2006, 5, p. 224–231.

33. Markus M.L. Technochange management: using IT to drive organizational change // *Journal of Information Technology,* 2004, 19, p. 4–20.

34. Mok K. H. Fostering entrepreneurship: Changing role of government and highe education governance in Hong Kong // *Research Policy,* 2005, 34, p. 537–554.

35. Moule B. & Giavara L. Policies, procedures and standards: an approach for implementation // *Information Management and Computer Security,* 1995, 3, p. 7–16.

36. Paula R., Ding X., Dourish P., Nies K., Pillet B., Redmiles D.F. Ren J., Rode J. A. & Filho R. S. In the eye of the beholder: a visualization-based approach to information security // *International Journal of Human-Computer Studies,* 2005, 63, p. 5–24.

37. Peppard J. The Conundrum of IT Management // *European Journal of Information Systems,* 2007, 16, p. 336–345.

38. Porter M.E. & Millar, V. How Information Gives you Competitive Advantage // *Harvard Business Review,* 1985, 63, p. 149–160.

39. Rees J., Bandyopadhyay S. & Spafford E. H. PFIRES: A Policy Framework for Information Security // *Communications of the ACM,* 2003, 46, p. 101–106.

40. Saleh M. S., Alrabiah A. & Saad H. B. Using ISO 17799; 2005 Information Security Management: a STOPE View with Six Sigma Approach // *International Journal of Network Management,* 2007, 17, p. 85–97.

41. Sheehan N. T. & Stabell C. B. Discovering new business models for knowledgeintensive organizations // *Strategy & Leadership,* 2007, 25, p. 22–29.

42. Siponen M Policies for construction of information systems' security guidelines // *Proceedings of 15th International Information Security Conference (IFIPTC11/SEC2000),* Beijing, China, 2000, August, p. 111–120.

43. Sircar S. & Choi J. A study of the impact of Information Technology on firm performance: a flexible production function approach // *Information Systems Journal*, DOI: 10.1111/j.1365-2575.2007.00274.x .

44. Solms B. & von Solms R. The ten deadly sins of information security management // *Computers & Security,* 2004, 23, 371–376.

45. Sterne D. F. On the buzzword '*security policy*' // *Proceedings of the IEEE Symposium on Research in Security and Privacy,* 1991, p. 19–230.

46. Straub D. W. & Welke R. J. Coping with systems risk: Security planning models for management decision making // *MIS Quarterly,* 1998, 22, p. 441–470.

47. Toit A. S. A. Competitive intelligence in the knowledge economy: what is in it for South African manufacturing enterprises // *International Journal of Information Management*, 2003, 23, p. 111–120.

48. Wadlow T. A. *The Process of Network Security*. Reading, MA: Addison-Wesley, 2000.

49. Ward J. & Peppard J. *Strategic Planning for Information Systems*, Wiley: Chester, 2002.

50. Wiant T. L. Information security policy's impact on reporting security incidents // *Computers & Security,* 2005, 24, p. 448–459.

51. Whitman. In defense of the realm: understanding threats to information security // *International Journal of Information Management,* 2004, 24, p. 3–4.

52. Zammuto R.F., Griffith T. L. Majchrzak A., Dougherty D.J. & Faraj S. Information Technology and the Changing Fabric of Organization // *Organization Science,* 2007, 18, p. 749–762.

53. THES (The Times Higher Education Supplement) // University World Rankings'.2007, November 5. Available at: http://www.timeshighereducation.co.uk/Magazines/THES/ graphics/WorldRankings2007.pdf (date access: 01.04.2021). Text: electronic.

References

1. Arnesen D. W. & Weis, W. L. *Journal of organizational culture, communications and Conflic (Journal of organizational culture, communications and Conflict)*, 2007, 11. P. 53–67.

2. Austin R.D. & Darby C. A. *Harvard Business Review* (Harvard Business Review), 2003, 81. P. 120–126.

3. Baskerville R. & Siponen M. *Information Management and Computer Security (Information Management and Computer Security*), 2002, 15, p. 337–346.

4. Besnard D. & Arief, B. *Computers & Security (Computers & Security)*, 2004, 23, p. 253–264.

5. Brynjolfsson E. & Hitt L. *Management Science (Management Science),* 1996, 42. P. 541–558.

6. Calder A Van Bom, J. *Implementing Information Security Based on ISO 27001/ISO 17799 (Implementing Information Security Based on ISO 27001/ISO 17799).* Van Haren Publishing, 2006.

7. Churchill, Gilbert A. Jr *Marketing Research, Methodological Foundations (Marketing Research, Methodological Foundations)*. The Dryden Press, 1997.

8. David J. *Computers and Security (Computers and Security),* 2002, 21. P. 506–513.

9. Desouza K. C. & Vanapalli G.K *International Journal of Information Management* (*International Journal of Information Management),* 2005, 25. P. 85–98.

10. Dhillon G. *Managing Information Systems Security (Managing Information Systems Security)*, Macmillan Press, London, 1997.

11. Dhillon G. & Backhouse J. *Communications of the ACM (Communications of the ACM)*, 2000, 43. P. 125–128.

12. Dhillon G. *Business Process Management Journal (Business Process Management Journal),* 2004, 10, P. 21–22.

13. Dhillon G. & Torkzadeh G. *Information Systems Journal (Information Systems Journal),* 2006, 16, p. 293–314.

14. Doherty N. F., King M. & Al-Mushayt O. *Information and Management (Information and Management),* 2003, 41, p. 49–62.

15. Doherty N. F. & Fulford H. *Information Resources Management Journal (Information Resources Management Journal),* 2005, 18, p. 21–38.

16. D. T. I. *Information security breaches survey* (*Information security breaches survey)*, Department of Trade & Industry, *2004.*

17. Drucker P. F. *Harvard Business Review (Harvard Business Review),* 1988, 66, p. 45–53.

18. Fulford H. & Doherty N. F. *Information Management and Computer Security (Information Management and Computer Security)*, 2003, 11, p. 106–114.

19. Gaston S. J. *Information Security: Strategies for Successful Management* (*Information Security: Strategies for Successful Management)*. Toronto: CICA, 1996. P. 18.

20. Garg A., Curtis J. & Halper H. *Information Management and Computer Security (Information Management and Computer Security),* 2003, 11, p. 74–83.

21. Hagen J.M., Albrechtsen E. & Hovden J. *Information Management & Computer Security* (*Information Management & Computer Security)*, 2008, 16, p. 377–397.

22. Higgins H. N. *Information Management & Computer Security (Information Management and computer Security)*, 1999, 7, p. 217–222.

23. Hinde S. *Computers and Security Computers and Security*, 2002, 21, p. 310–321.

24. Hone K. & Eloff J. H. P. *Computers & Security (Computers & Security)*, 2002, 21, p. 402–409.

25. Hone K. & Eloff J. H. P. *Network Security (Network Security),* 2002, 20, p. 14–16.

26. Hong K., Chi Y. Chao L. & Tang, J. *Information Management & Computer Security (Information Management and Computer Security)*, 2006, 14, p. 104–115.

27. I.S.O *Information technology – Security Techniques –. Code of practice for information security management - ISO 17799* (*Information technology – Security Techniques –. Code of practice for information security management - ISO 17799)*. International Standards Organization, Geneva, 2005.

28. Johannessen J-A, Olsen B. *International Journal of Information Management (International Journal of Information Management)*, 2003, 23, p. 277–289.

29. Karyda M. Kiountouzis E. & Kokolakis S. *Computers & Security (Computers & Security)*, 2005, 24, p. 246–260.

30. Kotulic A. J. & Clark J. G. *Information and Management* (*Information and Management)*, 2004, 41, p. 597–607.

31. Lindup K. R. *Computers and Security (Computers & Security)*, 1995, 14, p. 691–695.

32. Loggie K. A., Barron A. E., Gulitz E., Hohlfield T. N., Kromrey J.D. & Venable M. *Journal of Interactive Online Learning (Journal of Interactive Online Learning)*, 2006, 5, p. 224–231.

33. Markus M. L. *Journal of Information Technology (Journal of Information Technology),* 2004, 19, p. 4–20.

34. Mok K. H. *Research Policy (Research Policy),* 2005, 34, p. 537–554.

35. Moule B. & Giavara L. *Information Management & Computer Security (Information Management and Computer Security),* 1995, 3, p. 7–16.

36. Paula R., Ding X., Dourish P., Nies K., Pillet B., Redmiles D.F. Ren J., Rode J. A. & Filho R. S. *International Journal of Human-Computer Studies (International Journal of Human-Computer Studies),* 2005, 63, p. 5–24.

37. Peppard J. *European Journal of Information Systems (European Journal of Information Systems),* 2007, 16, p. 336–345.

38. Porter M.E. & Millar, V. *Harvard Business Review (Harvard Business Review),* 1985, 63, p. 149–160.

39. Rees J., Bandyopadhyay S. & Spafford E. H. *Communications of the ACM (Communications of the ACM),* 2003, 46, p. 101–106.

40. Saleh M. S., Alrabiah A. & Saad H. B. *International Journal of Network Management (International Journal of Network Management),* 2007, 17, p. 85–97.

41. Sheehan N. T. & Stabell C. B. *Strategy & Leadership (Strategy & Leadership),* 2007, 25, p. 22–29.

42. Siponen M. *Proceedings of 15th International Information Security Conference (Proceedings of 15th International Information Security Conference),* Beijing, China, 2000, August, p. 111–120.

43. Sircar S. & Choi J. *Information Systems Journal (Information Systems Journal*), DOI: 10.1111/j.1365-2575.2007.00274.

44. Solms B. & von Solms R. *Computers and Security (Computers & Security),* 2004, 23, 371–376.

45. Sterne D. F. *Proceedings of the IEEE Symposium on Research in Security and Privacy (Proceedings of the IEEE Symposium on Research in Security and Privacy),* 1991, p. 19–230.

46. Straub D. W. & Welke R. J. *MIS Quarterly (MIS Quarterly)*, 1998, 22, p. 441–470.

47. Toit A. S. *International Journal of Information Management (International Journal of Information Management)*, 2003, 23, p. 111–120.

48. Wadlow T. A. *The Process of Network Security (The Process of Network Security)*. Reading, MA: Addison-Wesley, 2000.

49. Ward J. & Peppard J. *Strategic Planning for Information Systems (Strategic Planning for Information Systems).* Wiley: Chester, 2002.

50. Wiant T. L. *Computers and Security (Computers & Security),* 2005, 24, p. 448–459.

51. Whitman. *International Journal of Information Management (International Journal of Information Management),* 2004, 24, p. 3–4.

52. Zammuto R.F., Griffith T. L. Majchrzak A., Dougherty D.J. & Faraj S. *Organization Science Organization Science,* 2007, 18, p. 749–762.

53. *University World Rankings'* (University World Rankings'),2007, November 5. Available at: http://www.timeshighereducation.co.uk/Magazines/THES/ graphics/WorldRankings2007.pdf (date access: 1./04.2021). Text: electronic.

Благодарности

Работа выполнена в рамках внутреннего гранта
Забайкальского государственного унивнерситета № 321 -ГР

Информация об авторе

Бейдина Татьяна Евгеньевна, д-р полит. наук, профессор, зав. кафедрой государственного, муниципального управления и политики, Забайкальский государственный университет, г. Чита, Россия. Область научных интересов: политические науки, государственное управление
beydina@inbox.ru

Кухарский Артем Николаевич, канд. полит. наук, Забайкальский государственный университет, г. Чита, Россия. Область научных интересов: информационная безопасность
kukharskijjartjom@yandex.ru

Information about the author

Tatyana Beidina, doctor of political sciences, professor, head of State, Municipal Management and Politics department, Transbaikal State University, Chita, Russia. Sphere of scientific interests: political science, public administration

Artem Kukharsky, candidate of political sciences, Transbaikal State University, Chita, Russia. Sphere of scientific interests: political science, information security

Для цитирования

Бейдина Т. Е., Кухарский А. Н. Политика информационной безопасности: критическое исследование содержания университетской политики // Вестник Забайкальского государственного университета. 2021. Т. 27, № 4. С. 55–72. DOI: 10.21209/2227-9245-2021-27-4-55-72.

Beidina T., Kuharsky A. Information security policy: a critical study of the content of university policy // Transbaikal State University Journal, 2021, vol. 27, no. 4, pp. 55–72. DOI: 10.21209/2227-9245-2021-27-4-55-72.

Статья поступила в редакцию: 19.05.2021 г.
Статья принята к публикации: 27.05.2021 г.