УДК 327
DOI: 10.21209/2227-9245-2022-28-1-75-87

МОДЕЛЬ ЭФФЕКТИВНОЙ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОНТЕКСТЕ ПРАКТИКИ УПРАВЛЕНИЯ

MODEL OF EFFECTIVE INFORMATION SECURITY POLICY IN THE CONTEXT OF MANAGEMENT PRACTICE



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

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

А. В. Новикова,
Забайкальский государственный университет, г. Чита
novikova2010@mail.ru

T. Beydina,
Transbaikal State University, Chita

A. Kukharsky,
Transbaikal State University, Chita

A. Novikova,
Transbaikal State University, Chita

Статья посвящена политике управления информационной безопасностью. Тема исследования является актуальной. В работе содержится оценка эффективности модели управления информационной безопасностью. Обзор литературы по управлению информационной безопасностью выявил четыре основных недостатка, которые снижают пользу рекомендательных характеристик для государственных и муниципальных органов власти, внедряющих методы управления информационной политикой. *Объект исследования* – практики управления информационной безопасностью. *Предмет исследования* – разработка эффективной модели управления политикой информационной безопасности для органов власти. *Цель работы* – исследование ориентировано на выявление методов управления политикой информационной безопасности для государственных и муниципальных органов власти. Обзор зарубежной литературы показывает, что целесообразно охарактеризовать эффективную модель управления информационной политикой для органов власти. Однако существует ряд недостатков, которые снижают полезность и эффективность модели информационной политики для органов власти при реализации политики безопасности. В литературе отсутствует целостное представление о модели информационной политики; не существует единообразия в терминологии и семантике; используются различные уровни детализации при описании действий по управлению политикой; затруднено использование руководства по управлению информационной политикой из других областей практики, таких как управление рисками, обучение информационным практикам и осведомленность в области безопасности. Авторы структурируют статью следующим образом. Во-первых, рассматривают существующие жизненные циклы управления политикой информационной безопасности. Во-вторых, объясняют методологию исследования, используемую для обзора и анализа литературы. В-третьих, предлагают модель управленческих практик, связанных с политикой информационной безопасности. В-четвертых, объясняют как предлагаемая модель устраняет выявленные недостатки. Из исследования можно сделать два вывода: 1) модель практики управления политикой информационной безопасности предполагает принудительное применение власти, направленное на руководство рисками; 2) модель ориентирована на выделение трех этапов институализации – разработку, внедрение и оценку управления

Ключевые слова: *политика информационной безопасности, политика управления безопасностью, информационная безопасность, методы защиты информации, государственное и муниципальное управление, модели эффективной политики, практики управления, информация, управленческая деятельность, жизненный цикл политики*

The article is devoted to the study of policy in the field of information security management and is relevant, since it contains an assessment of the effectiveness of the information security management model. However, our review of the information security management literature has identified four major weaknesses that reduce the usefulness of recommendation characteristics for state and municipal governments implementing information policy management practices. *The aim of this article* is to provide a comprehensive overview of information security policy management and to develop a model based on the generalization of practice. Our review of foreign literature shows that it is advisable to characterize an effective model of information policy management for government bodies. However, there is a number of shortcomings that reduce the usefulness and effectiveness of the information policy model for authorities in the implementation of security policy. In the literature, in our opinion: there is no holistic view of the information policy model (deficiency 1); there is no uniformity in terminology and semantics (flaw 2); different levels of detail are used when describing policy management actions (flaw 3); and it is difficult to use information policy management guidance from other practice areas such as risk management, information practice training and security awareness (Gap 4). The authors structure the article as follows. Firstly, it examines the existing lifecycles of information security policy management. Secondly, the authors explain the research methodology used to review and analyze the literature. Thirdly, the authors propose a model of management practices related to information security policy. Fourthly, the authors explain how the proposed model eliminates the identified shortcomings. Two conclusions can be drawn from the study: 1) the model of information security policy management involves the enforcement of power aimed at managing risks; 2) the model is focused on identifying 3 stages of institutionalization – the development, implementation and assessment of management activities

Key words: *information security policy, security management policy, information security, information protection methods, state and municipal management, effective policy models, management practices, information, management activities, policy life cycle*

Введение. Растет признание роли управления в защите информации органов власти от ряда рисков безопасности, таких как утечка государственной тайны и интеллектуальной собственности, нарушение работы критически важных систем как со стороны внутренних, так и со стороны внешних факторов управления [1; 2; 3]. Политика – это управление, с помощью которого руководство контролирует выполнение стратегических и тактических установок по вопросам структуры и безопасности информационных технологий [1; 4]. Очевидно, что зарубежные исследователи управленческие, информационные практики неразрывно связывают с политикой безопасности [5; 6].

Актуальность проблемы ориентирована на управление политикой на основе других областей практики, таких как риск, предлагаемая модель фокусируется исключительно на практике управления политикой. Упущение практик других областей управления безопасностью не означает, что предлагаемая модель игнорирует эти практики и их важность в процессе управления политикой безопасности, а скорее направлена на упрощение руководства по управлению политикой. Хотя модель не рассматривает проведение оценки рисков в качестве практики управления политикой, она признает важность оценки рисков на этапе разработки, а также на этапе оценки процесса управления политикой. Кроме того, модель ориентирована на необходимость проведения программы для связи и обеспечения соблюдения политики безопасности. Однако разработка и реализация программы не является частью процесса управления политикой, что ориентирует на практическую значимость статьи.

Объект исследования – практики управления информационной безопасностью.

Предмет исследования – разработка эффективной модели управления политикой информационной безопасности для органов власти.

Цель работы – исследование ориентировано на выявление методов управления политикой информационной безопасности для государственных и муниципальных органов власти.

На основании заявленной цели сформулированы следующие *задачи:*

– раскрыть содержание модели управления политикой информационной безопасности;

– определить связь модели с осуществлением власти в органах управления;

– проанализировать структуру модели информационной безопасности.

Технология исследования. Выполнен обзор и анализ литературы, предложенные

Околи и Шабрамом (2010). Процесс обзора был сосредоточен сначала на четырнадцати статьях, связанных с жизненными циклами безопасности. Каждая статья рассмотрена: абзацы сведены к темам, а предложения, связанные с разработкой политики, – подчеркнуты. Затем идеи и концепции записывались на полях. Резюме позволяет исследователям вспомнить важные темы, связанные с жизненным циклом политики (зарождение, развитие, умирание, оценка). Процесс кодирования был использован для синтеза статей, он включал открытое, осевое и селективное кодирование, как описано в Neuman (2006).

Второй обзор начался с более пристального внимания к подчеркнутым выдержкам и резюме, полученным в результате первого обзора. Появились темы, связанные с управлением политикой. Исследователи рассмотрели выявленные проблемы, уделяя больше внимания темам, которые часто обсуждаются в статьях. Темы разделены на подтемы, а несколько родственных понятий объединены в более общую тему. Проведено сравнение между темами, которые появляются в разных местах. Проведен обзор 92 публикаций, которые непосредственно не затрагивают процедуру разработки политики безопасности. Процесс проверки основан на результатах жизненного цикла политики безопасности. Новых проблем не выявлено. Обзор позволил получить подробную информацию об этапах жизненного цикла политики безопасности. В отдельных жизненных циклах упоминается о важности вовлечения заинтересованных сторон в процесс разработки политики безопасности. Однако не определено, кто является заинтересованными сторонами и не установлена их роль и обязанности в процессе разработки политики.

Методология исследования. Для разработки политики безопасности использован подход жизненного цикла.

Методы исследования. Использовался сравнительный и библиографический метод. Применялись как общенаучные, так и социологические методы исследования.

Степень изученности темы. Ряд исследований посвящен разработке и реализации политики информационной безопасности [7; 8; 9; 10; 11; 12]. Большинство из них представляют развитие политики безопасности как многоступенчатые жизненные циклы. Использование подхода жизненного цикла позволяет эффективно управлять процессом разработки политики безопасности и предусматривает выполнение всех важных действий для реализации задачи [5; 13]. Ølnes [14] подчеркивает важность названного методологического подхода для разработки, осуществления и поддержания политики безопасности. Патрик [13] утверждает, что использование подхода жизненного цикла политики безопасности обеспечит комплексный процесс разработки, охватывающий все необходимые мероприятия для эффективной политики безопасности.

Результаты исследования. В ходе исследования в существующих моделях разработки политики выявлены четыре недостатка, что отражено в табл. 1:

1) отсутствие целостного представления о жизненном цикле политики. Это можно четко определить в некоторых существующих моделях разработки политики. Например, Баюк (1997) представляет процесс, который фокусируется на разработке программных документов и не включает практик, связанных с реализацией и поддержанием политики. Процесс Баюка (1997) состоит из нескольких этапов: он начинается с определения активов; формирование команды для разработки политики; составление проекта политики, который рассматривается и утверждается к публикации. Исследователи (Патрик (2002) предполагают, что политика безопасности выходит за рамки разработки документа. Подобно Баюку (1997), модель разработки политики Элнеса (1994) не является целостной, так как она конкретно не касается механизма разработки, передачи, применения и оценки политической информации. В работе Аль-Маяхи и Саада (2014) основное внимание уделяется разработке политики информационной безопасности, а не руководству по процессу ее разработки;

2) существующие модели разработки политики не имеют последовательности в терминологии и семантике. В то время как [15; 16; 17; 13; 12] представили более целостный взгляд на процесс разработки политики, существует несколько пересекающихся концепций, таких как соблюдение, мониторинг и правоприменение. Эти три концепции проявляются в подходе как три отдельных вида деятельности, в то время как они представляют собой усилия руководства по обеспечению

соблюдения политики сотрудниками. Ссылаясь на одну концепцию в трех различных терминах, исследователи оценивали разные виды деятельности, что может вызвать путаницу среди специалистов безопасности, приступающих к процессу разработки политики;

3) при описании деятельности по управлению политикой существующие модели разработки политики используют различные уровни детализации. Каждая из моделей отличается уровнем детализации и акцентом на аспектах разработки политики. Например, Hare [15] систематически представляет процесс разработки политики безопасности, однако отсутствуют подробные сведения о том, как эта политика будет опубликована (какую форму она примет, например, онлайн), как она будет передаваться и применяться. Кроме того, Hare [15] не обсуждал вопрос о соответствии пользователей политике и важности осведомленности пользователей и обучения в области коммуникации и обеспечения соблюдения политики безопасности в организациях. Проблема содержания также прослеживается в предлагаемых этапах разработки политики [18; 19; 9; 17; 12; 20; 21]. Авторы дают скудные сведения о многих важных мероприятиях в процессе разработки политики безопасности. Например, жизненный цикл, разработанный Уитменом [22], не содержит указаний по передаче и применению политики. Кроме того, Knapp et al. [9] предлагает модель разработки политики, которая представляет процесс в очень общем виде, не разработано детальное описание практики управления политикой;

4) трудно отделить воздействие по управлению политикой от руководства другими практическими областями, такими как управление рисками. Это связано с тем, что модели, предложенные Ølnes [14], Rees et al. [10], Knapp et al. [23] и Patrick [13], включают такие практики, как оценка рисков, разработка программы повышения осведомленности о безопасности, выбор технических средств контроля в рамках этапов разработки политики. Мы признаем важность оценки рисков в процессе разработки политики, а также необходимость повышения осведомленности о безопасности и подготовке кадров для информирования и обеспечения политики, при этом утверждаем, что оценка рисков и разработка программы повышения осведомленности и обучения по вопросам безопасности не являются частью жизненного цикла политики безопасности. Жизненные циклы разработки политики, предложенные Олнесом (1994), Рисом и др. (2003), выходят за рамки разработки политики безопасности и ориентированы на разработку программы безопасности в организации. Они касаются политики безопасности, оценки рисков, технического контроля и реагирования на инциденты. Политика безопасности – это часть общей программы безопасности, на которой фокусируется модель.

Таблица 1 / Table 1

Сводная информация о недостатках, выявленных в существующих моделях разработки политики / Summary of weaknesses identified in existing policy development models

Разработчики / Developers	**Недостатки / Disadvantages**			
	1-й	2-й	3-й	4-й
Rees et al. (2003)		X		X
Patrick (2002)		X		X
Knapp et al. (2009)			X	X
Karyda et al. (2005)			X	
Kadam (2007)	X		X	
Hare (2002)			X	X
Bayuk (1997)	X	X		
Wood (1995)			X	X
Ølnes (1994)	X			X
Whitman et al. (1999)			X	
Saltzman and Gadkari (2004)	X		X	
Whitman and Mattord (2008)			X	
Lowery (2002)			X	X
Al-Mayahi and Sa'ad (2014)			X	X

Таким образом, обзор литературы свидетельствует о четырех критических недостатках, которые влияют на организации, стремящиеся реализовать политику информационной безопасности, а также поддерживает утверждение Knapp et al. [9] о необходимости эмпирических исследований в этой области, поскольку большинство существующих моделей разработки политики являются концептуальными и не подкрепляются эмпирическими данными.

Процесс проверки основывался на выделении нами методов управления политикой безопасности. Мы определяем практику управления политикой как деятельность стратегического уровня, осуществляемую для управления политикой безопасности в органах власти. Управление политикой безопасности включает разработку, внедрение и оценку политики безопасности. Процесс кодирования, в конечном итоге, привел к выявлению методов управления политикой безопасности. Каждая практика имеет несколько видов деятельности. Эти практики сгруппированы в три этапа.

Общее понимание возникло в результате систематического обзора и процесса проверки и привело к разработке модели практики управления политикой информационной безопасности. В табл. 2 представлена модель, состоящая из трех основных этапов:

1 – развития;

2 – осуществления технического обслуживания;

3 – оценки.

Каждый этап состоит из нескольких практик, каждая из которых включает ряд видов деятельности.

Таблица 2 / Table 2

Модель практики управления политикой информационной безопасности / Information Security Policy Management Practice Model

Этапы жизненного цикла / Life cycle stages	**Практика / Practice**	**Мероприятия / Events**
Формирование и развитие / Formation and development	Создание группы разработки политики информационной безопасности / Creation of an information security policy development group	Определение ключевых заинтересованных сторон / Identification of key stakeholders
		Определение ролей и обязанностей / Defining roles and responsibilities
	Определение потребностей организации в области безопасности / Identification of the organization's security needs	Определение требований безопасности / Defining security requirements
		Оценка текущей политики и процедур организации / Evaluation of the organization's current policies and procedures
	Составление документа политики безопасности / Drafting a security policy document	Выбор компонентов политики / Selecting policy components
		Проект политики безопасности / Draft security policy
		Обзор проекта программного документа / Overview of the draft policy document
Внедрение и обслуживание / Implementation and maintenance	Политика распространения / Distribution Policy	Выбор способов распространения политики / Choosing how to distribute the policy
		Выполнение фактического распределения / Performing the actual distribution
	Коммуникационная политика / Communication policy	Информирование о политике осуществляется различными способами, такими как брифинги, семинары и информационные кампании / Informing about the policy is carried out in various ways, such as briefings, seminars and information campaigns
	Принудительное применение политики / Policy enforcement	Проведение мероприятий по соблюдению политики (внедрение технологических механизмов и проведение программы) / Implementation of measures to comply with the policy (introduction of technological mechanisms and implementation of the program)
Умирание, оценка / Dying, evaluation	Периодически пересмотр политики информационной безопасности / Periodically review the information security policy	Сбор отзывов от заинтересованных сторон о политике безопасности / Collecting feedback from stakeholders about the security policy
		Изучение отчетов об инцидентах безопасности и новая оценка рисков / Review of security incident reports and a new risk assessment

Охарактеризуем стадии жизненного цикла политики обеспечения информационной безопасности. Стадия развития представляет собой все практики, связанные с разработкой политики информационной безопасности и создание группы разработчиков политики информационной безопасности.

Первая практика, которую специалисты по информационной безопасности в организациях должны предпринять в процессе разработки политики информационной безопасности, заключается в создании команды разработчиков. В этой практике существует два основных направления деятельности:

1) определение ключевых заинтересованных сторон, которые должны участвовать в разработке политики;

2) выявление ролей и обязанностей специалистов.

Участие заинтересованных сторон в процессе разработки политики безопасности является фактором ее успеха на этапах разработки, реализации и оценки. Таким образом, создается команда представителей заинтересованных сторон со всей организации и на всех уровнях: технический персонал, лица, принимающие решения, менеджеры, юридический отдел; отдел кадров; пользователи, сотрудники функциональных структур, затронутых новой политикой [5; 14; 24]. Сфера охвата разработанной политики является важным фактором определения участников процесса развития [13]. Например, политика безопасности, разработанная для отдела организации, должна включать в процесс разработки меньше людей, чем политика, ориентированная на власть.

При определении ролей и обязанностей важно четко определить задачи членов команды разработчиков, чтобы избежать задержек в процессе реализации межличностных проблем и политических убеждений, которые могут возникнуть [11; 20; 25]. Мейнард [25] утверждает, что, хотя многие авторы подчеркивают важность вовлечения различных заинтересованных сторон в процесс развития, роль этих сторон остается неясной. Он указывает, что авторы просто упоминают имя заинтересованной стороны, которая должна быть вовлечена в процесс разработки, не уточняя, что эта группа людей должна делать в данном процессе. Поэтому Мейнард [25] рассматривает роль каждого участника процесса разработки политики безопасности.

После создания группы разработки политики организация должна определить свои потребности в области безопасности [10; 11; 20]. Требуется понимание текущей ситуации организации, а также достаточное осознание целей и задач организации в области безопасности [14; 26; 27]. Для этого следует тщательно исследовать проблемы, стоящие перед организацией [22]. Определение потребностей организации в безопасности состоит из двух видов деятельности: определение требований безопасности и оценка текущей политики и процедур организации.

Важно четко определить требования безопасности, так как власть и организации имеют разные потребности в безопасности [16; 14; 25]. Баскервиль и Сипонен [28] утверждают, что при разработке политики безопасности важно хорошо понимать цели безопасности власти. Поэтому власть должна определить свои требования к безопасности, включая уровень безопасности, который она стремится достичь. Требования безопасности должны устранять риски безопасности, выявленные путем оценки рисков.

Результат оценки риска является вкладом в определение требований безопасности, поэтому ряд авторов включают оценку риска как практику в жизненные циклы политики безопасности [7; 29; 10]. Однако, хотя результат оценки риска является необходимым условием для определения требований безопасности, оценка риска должна быть частью управления рисками безопасности, а не частью разработки политики.

Оценка текущей политики и процессов организации, во-первых, помогает команде разработчиков безопасности выявить текущее состояние существующей политики и процессов [30; 28; 10; 22], что, в свою очередь, позволяет власти выделить пробелы и определить возможность существующей политики информационной безопасности организации справиться с рисками. Во-вторых, оценка существующей политики и процессов обеспечит соответствие новой политики существующим политическим стандартам [11]. Это повысит шансы на успешную реализацию информационной политики в организации [31]. В-третьих, процесс оценки поможет собрать ключевые материалы, такие как документы по политике и процедурам, которые

будут использоваться группой разработчиков в качестве ключевых справочных материалов [13; 12].

Обязательное составление документа политики безопасности является последней практикой на этапе разработки политики информационной безопасности. В документе должны быть обоснованы обязательства и направления руководства, изложен подход власти к управлению информационной безопасностью [32]. Мейнард и Руйгавер (2003) доказывают важность документирования процесса разработки политики информационной безопасности для обоснования процесса разработки и для помощи в оценке существующей политики.

Составление документа о политике безопасности включает ряд этапов: выбор элементов политики, составление проекта политики и представление его соответствующим заинтересованным сторонам для рассмотрения и утверждения [15; 13; 22].

Группа разработки устанавливает элементы политики для удовлетворения потребностей организации в области безопасности [17; 10; 25]. Они могут касаться контроля доступа, использования интернета, мобильных устройств, портативных устройств хранения данных и т. д. Например, пункты контроля доступа должны включать авторизованный доступ к системам, способы контроля доступа (пароли и/или биометрические данные) и последствия несанкционированного доступа [20; 24].

Проект политики безопасности служит элементом модели обобщения практики управления политикой информационной безопасности. Группа разработки назначает одного из своих членов для написания политики [33]. Остальные члены группы дают указания относительно содержания политики.

Höne и Eloff (2002) исследуют факторы, которые делают политику безопасности эффективным средством контроля при защите организационных информационных активов. Они называют характеристики, которые следует учитывать при написании политики безопасности. Эти показатели связаны с объемом и стилем изложения текста документа политики безопасности. Документ должен быть коротким, написан ясным, кратким и простым для понимания языком. Ряд авторов [27; 22; 25] подчеркивают важность использования регламентированного языка при написании рассматриваемого документа.

Первый проект политики представляется соответствующим заинтересованным сторонам для рассмотрения о качестве, удобстве использования и принятии политики [8; 34; 22]. Замечания по проекту должны быть отправлены автору. Написание и пересмотр политики – это интерактивный процесс [10]. Другими словами, проект может пройти через множество изменений, пока не будет отработан окончательный вариант, который должен быть направлен высшему руководству для утверждения. Затем он будет опубликован и готов к реализации [22], что предполагает этап внедрения и технического обслуживания.

Внедрение и техническое обслуживание является вторым этапом процесса управления политикой безопасности. Это непрерывный процесс, состоящий из нескольких практик. Далее приводятся методы и способы управления информационной безопасностью на этом этапе с точки зрения политики распространения.

Практика распространения политики заключается в обеспечении того, чтобы все заинтересованные стороны в организации, включая пользователей, имели доступ к нормативно-правовому документу [35]. Результативное распространение политики среди заинтересованных лиц требует значительных усилий со стороны организации [22]. Распределение политики включает выбор и использование методов распространения.

Существуют различные способы распространения политики в организации [29; 34; 11; 22]: одни организации предпочитают распространять печатный текст, в котором печатная копия документа доставляется сотрудникам, другие публикуют политику в электронном виде во внутренней и внешней сети [22]. Независимо от того, какие методы распространения выбирает организация, политика должна быть легко доступной [11]. Выбор методов распространения зависит от условий коммуникационной политики.

Информирование сотрудников о политике является важной практикой до ее применения [4; 9; 11; 12], оказывая помощь власти в управлении изменениями, вызванными внедрением новой политики [5]. Информирование о политике преследует цель ознакомить пользователей с политикой, информи-

ровать о пользе ее реализации, оповещение и о последствиях несоблюдения [9; 5].

Донести политику до общественности можно с помощью программ обучения, подготовки и повышения квалификации в области безопасности. Сипонен и др. (2014) подчеркивают важность программы в обучении сотрудников организации, их роль в поддержании политики. Уитмен [22] выделяет роль программы повышения квалификации в сохранении актуальности политики в сознании сотрудников.

В современной практике имеет место принудительное применение политики, что связано с необходимостью использования силы [15; 17]. Обеспечение соблюдения политики не сводится к простому выявлению и наказанию нарушителей. Правоприменение – это управленческая деятельность, которая учитывает само несанкционированное действие, а также тяжесть преступления и намерения пользователя [36].

В литературе подчеркивается значимость принудительного применения политики [30; 23; 10; 22]. Институт SANS сообщает, что для снижения рисков информационной безопасности «политика должна строго соблюдаться, а несоблюдение должно наказываться» [11]. Для обеспечения эффективной реализации политики безопасности необходимо обеспечить правоприменение и соблюдение требований [37].

Для обеспечения соблюдения политики необходимо выполнить ряд мероприятий. Во-первых, реализация технологических механизмов, таких как администрирование пользователей (добавление, удаление и изменение пользователей систем и приложений), оценка и применение патчей безопасности к системам и приложениям, мониторинг систем и приложений на предмет событий безопасности и администрирование антивирусных приложений [37; 10]. Во-вторых, принудительное исполнение может быть осуществлено путем проведения программы по изменению поведения сотрудников в отношении соблюдения политики безопасности [6; 4]. Sommestad et al., Li et al., Vance et al. утверждают, что организации должны перейти от навязывания политики через внедрение стимулов и санкций к созданию общего видения политики безопасности. Этот аргумент поддерживает утверждение ряда авторов [38; 39; 40; 41; 42] о том, что создание культуры безопасности приведет к лучшему соблюдению политики безопасности.

В литературе существует обоснование того, что политика должна периодически пересматриваться [23; 5; 10]. Организационная среда, как внутренняя, так и внешняя, постоянно меняется. Это приводит к изменению информационных рисков, с которыми сталкивается организация. Чтобы политика информационной безопасности оставалась актуальной, эффективной, ее необходимо модернизировать. Для выполнения практики обзора желательно выполнить два основных вида деятельности:

1) сбор отзывов от соответствующих заинтересованных сторон о политике безопасности.

Обратная связь может быть получена от соответствующих заинтересованных сторон (специалистов, пользователей и т. д.) с помощью интервью, опросов и других средств сбора данных [33]. Обратная связь необходима для определения эффективности политики, контроля над ее соблюдением и определения актуальности политики. Это позволит установить, нуждаются ли власти в изменении политики, и поможет избежать риска наличия устаревшей и нерелевантной политики безопасности [33; 13];

2) изучение отчетов об инцидентах безопасности и новой оценке рисков.

Очевидна важность сбора данных об инцидентах безопасности для разработки политики. Количество и тип инцидентов могут быть значимыми для определения утраты эффективности политики [43; 8; 11]. Это позволяет выявить области, которые в существующей политике необходимо обновить или удалить.

Ряд исследователей предполагают, что обзор и пересмотр политики должны проводиться ежегодно [35]. Другие считают, что это должно происходить лишь когда вносятся изменения в информационные системы организации [26; 4; 21]. Инциденты безопасности также могут спровоцировать этот процесс [44; 45].

Управление политикой информационной безопасности – это интерактивный процесс, что подчеркивает обратную связь текущей политики (необходимости изменения и обновления политики) со стадией разработки и практикой управления политикой. Создание модели эффективной политики ин-

формационной безопасности органов власти предполагает учет практики управления в зарубежных странах, значительно продвинувшихся в решении информационных проблем. Существующая практика обобщения предполагает учет следующих элементов модели: ее структурные элементы, целевая ориентация с учетам жизненного цикла, власть, недостатки и преимущества практики управления информационными процессами. Для устранения недостатков, выявленных в литературе (см. табл. 1), обоснованная нами модель практики управления политикой безопасности предлагает следующие рекомендации:

1) обеспечить целостное представление о процессе управления политикой. Патрик [45] утверждает, что организации должны иметь более широкие сведения о процессе разработки политики, чем простые задачи написания и реализации, что узкий взгляд на процесс приводит к «разработке политики, которая плохо продумана, неполна, избыточна, не полностью поддерживается пользователями или руководством, является излишней или неуместной» (p297). Поэтому для обеспечения более целостного представления о процессе управления политикой проведен всесторонний и систематический обзор литературы, ориентированной на политику безопасности. Методы качественного анализа, включая кодирование и обсуждение, использованы для построения целостного представления о процессе;

2) усовершенствовать терминологический аппарат. Предлагаемая модель практики управления политикой безопасности решает проблему несогласованности терминологии и семантики, представляя собой явное занижение терминологии, используемой для обозначения деятельности по управлению политикой. В этой модели проводится четкое различие между «сообщением» и «распространением» политики безопасности, которые используются в литературе. Предлагаемая модель относится к выбору методов распространения политики и фактической доставке программных документов сотрудникам как «распространение политики». В то время как обеспечение ознакомления сотрудников с политикой называется «передачей политики». Другим примером непоследовательности в терминологии и семантике является использование терминов «принуждение» и «соблюдение» для обозначения усилий, которые руководство должно предпринять для обеспечения развития политики. Модель определяет практику управления, обеспечивающую соблюдение пользователями политики, как «принудительного применения политики». Соблюдение, с другой стороны, является желаемым результатом правоприменительной практики;

3) описанная модель фокусируется на практиках управления политикой безопасности. Модель состоит из трех этапов институционализации. Каждый этап предполагает несколько управленческих практик, и каждая практика состоит из действий, которые должны быть предприняты для выполнения этой практики. Эта организация модели обеспечивает глубокое обсуждение методов управления политикой безопасности, что позволяет организациям достаточно ориентироваться в управлении политикой безопасности.

Выводы.

1. В данной работе обсуждается разработка модели практики управления политикой безопасности. Обзор и анализ зарубежной литературы позволил получить более полное и четкое представление о процессе разработки политики безопасности. На основе этого обзора мы разработали модель практики управления политикой информационной безопасности. Модель состоит из трех стадий институционализации: разработки; внедрения и сопровождения; оценки. Каждый этап состоит из нескольких практик, содержащих элементы управленческой деятельности.

2. Модель практики управления политикой безопасности имеет несколько результатов для исследователей. Эта модель обеспечит всестороннее руководство по методам управления политикой безопасности, которые могут быть реализованы для управления политикой безопасности власти. Эта модель также позволит практикующим специалистам сопоставить свою деятельность по управлению политикой безопасности с этой моделью и обеспечить лучшее понимание управленческого процесса. Модель позволит исследователям сопоставить существующую исследовательскую деятельность по управлению политикой с предложенным эталоном (т. е. этапами институционализации, а также практиками внутри каждого этапа), чтобы определить области для будущих исследований.

3. Разработанная нами модель обеспечивает прочную основу для дальнейшей работы. Следующим шагом является эмпирическое уточнение и проверка модели с использованием, в свою очередь, набора экспертных интервью, тематических исследований и, наконец, набора фокус-групп. Экспертные интервью будут проведены для получения комментариев по предложенной модели с целью ее уточнения. Тематические исследования позволят оценить внедрение практик управления безопасностью в соответствии с данной моделью, фокус-группы позволят провести окончательную проверку модели на практике.

Список литературы

1. Ahmad A., Bosua R., Scheepers R. Protecting Organizational Competitive Advantage: A Knowledge Leakage Perspective // Computers & Security. 2014. № 42. P. 27–39.

2. Ahmad A., Maynard S. B., Shanks G. A. Case Analysis of Information Systems and Security Incident Responses // International Journal of Information Management, 2015. P. 717–723.

3. Al-Mayahi I. H., Sa'ad P. M. Information Security Policy Development // Journal of Advanced Management Science. 2014. № 2:2. June. P. 135–139.

4. Alshaikh M., Ahmad A., Maynard S.B., Chang S. Towards a Taxonomy of Information Security Management Practices in Organisations // 25th Australasian Conference on Information Systems. Auckland. New Zealand. 2014. P. 40–42.

5. Anderson Consulting. Policy Framework for Interperting Risk in Ecommerce Security // Center for Education and Research in Information Assurance and Security, Purdue University. 2000. 320 p.

6. Bañares-Alcántara R. Perspectives on the Potential Roles of Engineers in the Formulation, Implementation and Enforcement of Policies // Computers & Chemical Engineering. 2010. № 34:3. P. 267–276.

7. Baskerville R., Siponen M. An Information Security Meta-Policy for Emergent Organizations // Logistics Information Management. 2002. № 15:5/6. P. 337–346.

8. Bayuk J. Security Through Process Management // Morristown, NJ, Price Waterhouse. 1997. 385 p.

9. Bin Muhaya F. An Approach for the Development of National Information Security Policies, 2010.

10. CengageBrain. Whitman M. E., Townsend A. M. and Aalberts R. J. Considerations for an Effective Telecommunications-Use Policy // Communications of the ACM № 42:6. 1999. P. 101–108.

11. Doherty N.F., Fulford H. Aligning the Information Security Policy with the Strategic Information Systems Plan // Computers & Security. 2006. № 25:1. P. 55–63.

12. Gaunt N. Installing an Appropriate Information Security Policy // International Journal of Medical Informatics. 1998. № 49:1. P. 131–134.

13. Hare C. Policy Development // Information Security Management Handbook Fourth Edition. 2002. Vol. 3. CRC Press. P. 353–383.

14. Hassan N. H., Ismail Z. A Conceptual Model for Investigating Factors Influencing Information Security Culture in Healthcare Environment // Procedia – Social and Behavioral Sciences. 2012. № 65:0. P. 1007–1012.

15. Höne K., Eloff J.H.P. Information Security Policy – What Do International InformationSecurity Standards Say? // Computers & Security. 2002. №1:5. P. 402–409.

16. ISO/IEC27002. Australian/New Zealand Standard: Information Technology – Security Techniques-Code of Practice for Information Security Management. 2006.

17. Kadam A.W. Information Security Policy Development and Implementation // Information Systems Security. 2007. № 16:5. P. 246–256.

18. Karyda M., Kiountouzis E., Kokolakis S. Information Systems Security Policies: A Contextual Perspective // Computers & Security. 2005. № 24:3. P. 246–260.

19. Klaic A., Hadjina N. Methods and Tools for the Development of Information Security Policy – a Comparative Literature Review. MIPRO, 2011 // Proceedings of the 34th International Convention. 2011. P. 1532–1537.

20. Knapp K. J., Ferrante C. J. Policy Awareness, Enforcement and Maintenance: Critical to Information Security Effectiveness in Organizations // Journal of Management Policy and Practice. 2012. № 13:5. P. 66–80.

21. Knapp K. J., Franklin Morris Jr R., Marshall T. E., Byrd T. A. Information Security Policy:An Organizational-Level Process Model // Computers & Security. 2009. № 28:7. P. 493–508.

22. Li H., Sarathy R., Zhang J., Luo X. Exploring the Effects of Organizational Justice, Personal Ethics and Sanction on Internet Use Policy Compliance // Information Systems Journal. 2014. № 24:6. P. 479–502.

23. Lim Ahmad A., Chang S., Maynard S. Embedding Information Security Culture Emerging Concerns and Challenges // PACIS 2010 Proceedings. Paper 43. 2010. P. 463–474.

24. Lindup K. R. A New Model for Information Security Policies // Computers & Security. 1995. № 14:8. P. 691–695.

25. Lowery J. Developing Effective Security Policies. Dell power solutions. 2002. P. 147–217.

26. Maynard S., Ruighaver A. Development and Evaluation of Information System Security Policies // Information Systems: The Challenges of Theory and Practice. 2003. P. 366–393.

27. Ølnes J. Development of Security Policies // Computers & Security. 1994. № 13:8. P. 628–636.

28. Oost D., Chew E.K. Investigating the Concept of Information Security Culture //Strategic and Practical Approaches for Information Security Governance: Technologies and Applied Solutions. IGI Global. 2012. P. 1–12.

29. Palmer M. E., Robinson C., Patilla J. C., Moser E. P. Information Security Policy Framework: Best Practices for Security Policy in the E-Commerce Age // Information Systems Security. 2001. № 10:2. P. 1–15.

30. Park S., Ruighaver A.B., Maynard S.B., Ahmad A. Towards Understanding Deterrence: Information Security Managers' Perspective // Proceedings of the International Conference on IT Convergence and Security. Suwon, Korea. 2012.

31. Patrick D. H. The Security Policy Life Cycle // Information Security Management Handbook, Fourth Edition, vol. 4. Auerbach Publications. 2002. P. 297–311.

32. Peltier T. R. Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management // CRC Press. 2013.

33. Puhakainen P., Siponen M. Improving Employees' Compliance through Information Systems Security Training: An Action Research Study // Mis Quarterly. 2010. № 34:4. P. 757–778.

34. Ramachandran S., Rao C., Goles T., Dhillon G. Variations in Information Security Cultures across Professions: A Qualitative Study // Communications of the Association for Information Systems. 2012. № 33:11. P. 163–204.

35. Rees J., Bandyopadhyay S., Spafford E. H. PFIRS: A Policy Framework for Information Security // Communications of the ACM. 2003. № 46:7. P. 101–106.

36. Ruighaver Maynard S. B., Chang S. Organisational Security Culture: Extending the End- User Perspective // Computers & Security. 2007. № 26:1. P. 56–62.

37. SANS Institute. Security Policy Roadmap – Process for Creating Security Policies. 2001. P. 48–96.

38. Siponen M., Adam Mahmood, M. Pahnila S. Employees' Adherence to Information Security Policies: An Exploratory Field Study // Information & Management. 2014. № 51:2. P. 217–224.

39. Siponen M., Pahnila S., Mahmood A. Employees' Adherence to Information Security Policies: An Empirical Study // New Approaches for Security, Privacy and Trust in Complex Environments. 2007. P. 133–144.

40. Stahl B. C., Doherty N. F., Shaw M. Information Security Policies in the Uk Healthcare Sector: A Critical Evaluation // Information Systems Journal. 2012. № 22:1. P. 77–94.

41. Webb J., Ahmad A., Maynard S.B., Shanks G. A. Situation Awareness Model for Information Security Risk Management // Computers & Security. 2014. № 44. P. 1–15.

42. Whitman M. E. Security Policy: From Design to Maintenance. Information Security: Policy, Processes, and Practices // D. W. Straub, S. E. Goodman R. Baskerville (eds.). Advances in Management Information Systems. London, England Armonk, New York : M.E. Sharpe, 2008. P. 123–151.

43. Whitman M. E., Mattord H. J. Management of Information Security. 2010.

44. Whitman M. E., Townsend A. M., Aalberts R .J. Information Systems Security and the Need for Policy. 2001.

45. Wood C. C. Information Security Policies Made Easy // A Comprehensive Set of Information Security Policies. Houston: InformationShield. Version 10.0. 2005.

46. Wood C.C. Writing Infosec Policies // Computers & Security. 1995. № 14:8. P. 667–674.

47. Wood C.C., Lineman D. Information Security Policies Made Easy Version 11 // InformationShield, Inc. 2009. 478 p.

References

1. Ahmad A., Bosua R., Scheepers R. *Computers & Security* (Computers & Security), 2014, no. 42, pp. 27–39.

2. Ahmad A., Maynard S. B., Shanks G. A. *International Journal of Information Management* (International Journal of Information Management), 2015, pp. 717–723.

3. Al-Mayahi I. H., Sa'ad P. M. *Journal of Advanced Management Science* (Journal of Advanced Management Science), 2014, no. 2:2. June, pp. 135–139.

4. Alshaikh M., Ahmad A., Maynard S.B., Chang S. *25th Australasian Conference on Information Systems* (25th Australasian Conference on Information Systems). Auckland. New Zealand, 2014, pp. 40–42.

5. Anderson Consulting. *Center for Education and Research in Information Assurance and Security, Purdue University* (Center for Education and Research in Information Assurance and Security, Purdue University), 2000, 320 p.

6. Bañares-Alcántara R. *Computers & Chemical Engineering* (Computers & Chemical Engineering), 2010, no. 34:3, pp. 267–276.

7. Baskerville R., Siponen M. *Logistics Information Management* (Logistics Information Management), 2002, no. 15:5/6, pp. 337–346.

8. Bayuk J. *Morristown, NJ, Price Waterhouse* (Morristown, NJ, Price Waterhouse), 1997, 385 p.

9. Bin Muhaya F. *An Approach for the Development of National Information Security Policies* (An Approach for the Development of National Information Security Policies), 2010.

10. CengageBrain. Whitman M. E., Townsend A. M. and Aalberts R. J. *Communications of the ACM* (Communications of the ACM), 1999, no. 42:6, pp. 101–108.

11. Doherty N.F., Fulford H. *Communications of the ACM* (Computers & Security), 2006, no. 25:1, pp. 55–63.

12. Gaunt N. *International Journal of Medical Informatics* (International Journal of Medical Informatics), 1998, no. 49:1, pp. 131–134.

13. Hare C. *Information Security Management Handbook Fourth Edition* (Information Security Management Handbook Fourth Edition), 2002, vol. 3, CRC Press, pp. 353–383.

14. Hassan N. H., Ismail Z. *Procedia – Social and Behavioral Sciences* (Procedia – Social and Behavioral Sciences), 2012, no. 65:0, pp. 1007–1012.

15. Höne K., Eloff J.H.P. *Computers & Security* (Computers & Security), 2002, no. 1:5, pp. 402–409.

16. *ISO/IEC27002. Australian/New Zealand Standard: Information Technology – Security Techniques-Code of Practice for Information Security Management* (ISO/IEC27002. Australian/New Zealand Standard: Information Technology – Security Techniques-Code of Practice for Information Security Management), 2006.

17. Kadam A.W. *Information Systems Security* (Information Systems Security), 2007, no. 16:5, pp. 246–256.

18. Karyda M., Kiountouzis E., Kokolakis S. Computers & Security, 2005, no. 24:3, pp. 246–260.

19. Klaic A., Hadjina N. *Proceedings of the 34th InternationalConvention* (Proceedings of the 34th International Convention), 2011, pp. 1532–1537.

20. Knapp K. J., Ferrante C. J. *Journal of Management Policy and Practice* (Journal of Management Policy and Practice), 2012, no. 13:5, pp. 66–80.

21. Knapp K. J., Franklin Morris Jr R., Marshall T. E., Byrd T. A. *Computers & Security* (Computers & Security), 2009, no. 28:7, pp. 493–508.

22. Li H., Sarathy R., Zhang J., Luo X. *Information Systems Journal* (Information Systems Journal), 2014, no. 24:6, pp. 479–502.

23. Lim Ahmad A., Chang S., Maynard S. *PACIS 2010 Proceedings* (PACIS 2010 Proceedings), 2010, paper 43, pp. 463–474.

24. Lindup K. R. *Computers & Security* (Computers & Security), 1995, no. 14:8, pp. 691–695.

25. Lowery J. *Developing Effective Security Policies. Dell power solutions* (Developing Effective Security Policies. Dell power solutions), 2002, pp. 147–217.

26. Maynard S., Ruighaver A. *Information Systems: The Challenges of Theory and Practice* (Information Systems: The Challenges of Theory and Practice), 2003, pp. 366–393.

27. Ølnes J. *Computers & Security* (Computers & Security), 1994, no. 13:8, pp. 628–636.

28. Oost D., Chew E. K. *Strategic and Practical Approaches for Information Security Governance: Technologies and Applied Solutions* (Strategic and Practical Approaches for Information Security Governance: Technologies and Applied Solutions). IGI Global, 2012, pp. 1–12.

29. Palmer M. E., Robinson C., Patilla J. C., Moser E. P. *Information Systems Security* (Information Systems Security), 2001, no. 10:2, pp. 1–15.

30. Park S., Ruighaver A.B., Maynard S.B., Ahmad A. *Proceedings of the International Conference on IT Convergence and Security* (Proceedings of the International Conference on IT Convergence and Security), Suwon, Korea. 2012.

31. Patrick D. H. *Information Security Management Handbook, Fourth Edition* (Information Security Management Handbook, Fourth Edition). Auerbach Publications, 2002, vol. 4, pp. 297–311.

32. Peltier T. R. *CRC Press* (CRC Press), 2013.

33. Puhakainen P., Siponen M. *Mis Quarterly* (Mis Quarterly), 2010, no. 34:4, pp. 757–778.

34. Ramachandran S., Rao C., Goles T., Dhillon G. *Communications of the Association for Information Systems* (Communications of the Association for Information Systems), 2012, no. 33:11, pp. 163–204.

35. Rees J., Bandyopadhyay S., Spafford E. H. *Communications of the Association for Information Systems* (Communications of the Association for Information Systems), 2003, no. 46:7, pp. 101–106.

36. Ruighaver Maynard S. B., Chang S. *Computers & Security* (Computers & Security), 2007, no. 26:1, pp. 56–62.

37. *SANS Institute. Security Policy Roadmap – Process for Creating Security Policies* (SANS Institute. Security Policy Roadmap – Process for Creating Security Policies), 2001, pp. 48–96.

38. Siponen M., Adam Mahmood, M. Pahnila S. *Information & Management* (Information & Management), 2014, no. 51:2, pp. 217–224.

39. Siponen M., Pahnila S., Mahmood A. *New Approaches for Security, Privacy and Trust in Complex Environments* (New Approaches for Security, Privacy and Trust in Complex Environments), 2007, pp. 133–144.

40. Stahl B. C., Doherty N. F., Shaw M. *Information Systems Journal* (Information Systems Journal), 2012, no. 22:1, pp. 77–94.

41. Webb J., Ahmad A., Maynard S.B., Shanks G. A. *Computers & Security* (Computers & Security), 2014, no. 44, pp. 1–15.

42. Whitman M. E. *Advances in Management Information Systems* (Advances in Management Information Systems). London, England Armonk, NY: M. E. Sharpe, 2008. P. 123–151.

43. Whitman M. E., Mattord H. J. *Management of Information Security* (Management of Information Security), 2010. 592 p.

44. Whitman M. E., Townsend A. M., Aalberts R. J. *Information Systems Security and the Need for Policy* (Information Systems Security and the Need for Policy), 2001.

45. Wood C. C. *A Comprehensive Set of Information Security Policies* (A Comprehensive Set of Information Security Policies). Houston: InformationShield. Version 10.0. 2005.

46. Wood C.C. *Computers & Security* (Computers & Security), 1995, no. 14:8, pp. 667–674.

47. Wood C.C., Lineman D. *InformationShield, Inc* (InformationShield, Inc), 2009, 478 p.

Информация об авторе

Бейдина Татьяна Евгеньевна, д-р полит. наук, профессор, профессор кафедры 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

Новикова Анна Владимировна, канд. полит. наук, доцент, доцент кафедры государственного, муниципального управления и политики, Забайкальский государственный университет, г. Чита, Россия. Область научных интересов: политические науки, государственное управление
anna_novikova2010@mail.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

Anna Novikova, candidate of political sciences, associate professor, assistant professor, State, Municipal Management and Politics department, Transbaikal State University Chita, Russia. Sphere of scientific interests: political science, public administration

Для цитирования

Бейдина Т. Е., Кухарский А.Н., Новикова А.В. Модель эффективной политики информационной безопасности в контексте практики управления // Вестник Забайкальского государственного университета. 2022. Т. 28, № 1. С. 75–87. DOI: 10.21209/2227-9245-2022-28-1-75-87.

Beydina T., Kukharsky A., Novikova A. Model of effective information security policy in the context of management practice // Transbaikal State University Journal, 2022, vol. 28, no. 1, pp. 75–87. DOI: 10.21209/2227-9245-2022-28-1-75-87.

Статья поступила в редакцию: 19.11.2021 г.
Статья принята к публикации: 11.01.2022 г.