УДК 658.1:004.056 + 339.137 Вестник УрФО № 1(31) / 2019, с. 37–47

Астахова Л. В., Лушникова С. С.

DOI: 10.14529/secur190106

КУЛЬТУРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЗАРУБЕЖНЫХ И РОССИЙСКИХ ИССЛЕДОВАНИЙ

В данной статье предпринят анализ литературы, посвященной тематике культуры информационной безопасности (КИБ) и культуры кибербезопасности (ККБ), опубликованной в период с 2010 года по 2017 годы. Выделены основные аспекты содержания публикаций, выявлены методики исследований данной темы, произведено сравнение общемирового и российского опыта в данной области. На основе полученных результатов уточнено понятие культуры информационной безопасности и предложена документационная модель ее развития на предприятии.

Ключевые слова: *информационная безопасность, кибербезопасность, защита информации, культура информационной безопасности, киберкультура, осведомленность, кадровая безопасность, организационная культура, культура безопасности.*

Astakhova L. V., Lushnikova S. S.

CULTURE OF INFORMATION SECURITY ENTERPRISE: COMPARATIVE ANALYSIS OF FOREIGN AND RUSSIAN RESEARCH

This article analyzes the literature on the subject of the culture of information security (KIB) and the culture of cybersecurity (KKB), published between 2010 and 2017. The main aspects of the contents of publications are singled out, the methods of research of this topic are revealed, the global and Russian experience in this field is compared. On the basis of the results obtained, the notion of a culture of information security was clarified and a documentary model of its development at the enterprise was proposed.

Keywords: *information security, cybersecurity, information security, information security culture, cyberculture, awareness, personnel security, organizational culture, safety culture.*

Статья выполнена при поддержке Правительства РФ (Постановление №211 от 16.03.2013 г.), соглашение № 02. A03.21.0011

Согласно статистическим исследованиям, устойчивой тенденцией является тот факт, что более двух третей угроз, имеющих злонамеренный характер, исходит от персонала предприятия [1]. Несмотря на то, что защита информационного капитала крайне важна

для обеспечения стабильной экономики [2], а недоразвитость культуры может привести к серьезному ущербу не только в экономической отрасли, но и пошатнуть безопасность целой нации [3], область культуры информационной безопасности и культуры кибербезопасности, которая закладывает морально-этическую основу отношения человека к защите информации, до сих пор слабо изучена. В данной статье произведен сравнительный наукометрический анализ количества и содержания публикаций, посвященных КИБ и ККБ в зарубежных и российских источниках, появившихся во второе десятилетие XXI века. Цели сравнительного анализа - выявить зарубежные тенденции исследований этой сферы; определить уровень зрелости развития КИБ; определить необходимый вектор развития КИБ для России.

В качестве источников материала для анализа мы взяли: международную реферативную базу данных Scopus; российский информационно-аналитический портал eLibrary; стандарты семейства ГОСТ-Р ИСО МЭК 27000 по управлению информационной безопасностью, банковские стандарты ЦБ РФ в области информационной безопасности; интернет-блоги наиболее известных экспертов в области информационной безопасности (Алексея Лукацкого – «Бизнес без опасности» и Андрея Прозорова – «Жизнь 80 на 20»).

При исследовании базы Scopus были рассмотрены статьи, найденные по запросу «Cybersecurity culture» OR «Information security culture» за временной промежуток с 2010 по 2017 годы. Общее количество найденных публикаций на заданную тему – 85. Во внимание были приняты заглавия, аннотации статей и ключевые слова.

Анализ выявленных в Scopus публикаций был призван ответить на следующие вопросы: 1. Какую часть в процентном соотношении занимают российские публикации в рамках общего количества статей на заданную тему? 2. Какие аспекты данной тематики исследуются за рубежом и в России? 3. Какие методы доминируют в исследованиях культуры информационной безопасности?

Данные Scopus (рис.1) демонстрируют следующую статистику распределения публикаций по странам. Наибольшее число публикаций имеют Южная Африка, (24 статьи), Австралия (12 статей), Малайзия, США и Великобритания поровну (8 статей). В России же на заданную тематику опубликовано всего 2 статьи, что составляет 2,35% от общего числа публикаций, и в 12 раз меньше, чем число трудов ученых из Южной Африки.

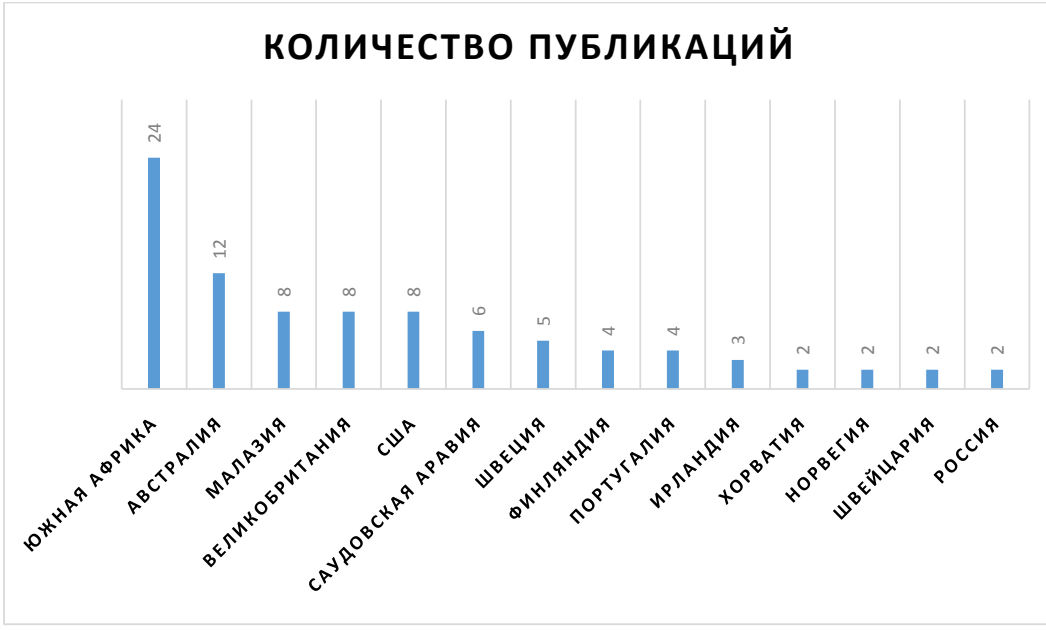

Рис. 1. Распределение количества публикаций по КИБ по странам (2010-2017 гг.)

Среди аспектов КИБ, изучаемых в публикациях (рис.2), самое большое число посвящено тематике взаимосвязи КИБ с культурой организационной и национальной (10,8%). Далее идут публикации о методах измерения и оценки КИБ в организации (9,6%). Также достаточно большое число статей посвящено исследованию существующей КИБ в какой-

либо конкретной организации или группе организаций, будь то библиотеки, учреждения здравоохранения, школы (8,4%). Достаточно распространены исследования, направленные на выявление факторов, способствующих успешному функционированию КИБ; на управление изменениями в КИБ, происходящими при каких-либо изменениях в режиме работы организации. Не последнее место занимает тематика определения и рамок КИБ, что свидетельствует о слабой развитости данной темы в целом в мире и отсутствии достаточного количества материала для теоретического фундамента знаний в этой области. время интенсивно исследуется в зарубежных странах. Тем не менее зарубежные ученые считают, что набор тем и методов исследований крайне ограничен и носит по большей части теоретический характер. Большинство теорий, по их мнению, адаптировано из психологии, экономики, управленческих и др. гуманитарных наук. Эти выводы позволили ученым заключить, что данная область научных знаний носит еще только зарождающийся характер [5]. Они предполагают, что в будущем эта отрасль должна использовать методы, незадействованные ранее, и подходы, которые в контексте КИБ еще не исследовались.

Рис. 2. Распределение количества публикаций по КИБ по аспектам изучения (2010-2017 гг.)

Методы изучения КИБ, к сожалению, проанализировать не удалось ввиду ограниченности доступа к материалу большей части исследований. Однако, согласно доступным материалам, в 40% всех публикаций превалируют эмпирические методы исследования посредством интервьюирования и аналитико-синтетические методы, обзора литературы. Эмпирический анализ использовался только в одной пятой из всего количества материала. Это свидетельствует о необходимости проведения дополнительных эмпирических исследований проблем КИБ [2].

По полученным в ходе анализа результатам можно судить, что область культуры информационной безопасности в настоящее

В базе данных Scopus было обнаружено 2 публикации по КИБ в России. Впервые на проблему КИБ с теоретических позиций обратила внимание Л. В. Астахова. Опираясь на функциональную концепцию культуры и сущность информационной безопасности, она определила концепт культуры безопасности информации как особый способ организации и развития информационной деятельности субъекта, который представлен в ценностно ориентированных моделях его информации, взаимодействие как отправителя и получателя информации, при котором он определяет и контролирует единство существования и развития информационных объектов в их познавательных и коммуникативных проявле-

ниях [6]. А. Малюк и Н. Милославская рассмотрели гуманитарную проблематику культуры кибербезопасности, связанную с этическими вопросами развития информационных технологий. Они предложили собственную, не основанную на западных аналогах, программу курса обучения кибербезопасности ИТ-специалистов, благодаря которой они должны будут иметь возможность формулировать и аргументировать свои предложения, убеждать высшее руководство организации в необходимости принятия мер по защите информации, чтобы иметь возможность работать с персоналом, и т.д. [4].

При анализе научных изысканий по тематике КИБ в России ограничение только рамками Scopus не позволило бы сформировать полноценной картины. Поэтому для более глубокого изучения российского опыта по данной теме было проведено дополнительное исследование российских источников. Был предпринят анализ российской теории и практики в области КИБ за последнее десятилетие, произведено сравнение предметов исследования КИБ, оценена зрелость становления тематики КИБ, выделены особенности КИБ в России.

В eLIBRARY по запросу «Культура информационной безопасности» OR «Культура кибербезопасности» за период с 2010 по 2017 годы найдено 5 статей, соответствующих заявленной тематике и не рассмотренных выше при анализе материалов из Scopus. Так, Л.И Купрюхина [8] и А. А. Ахметвалиева [9] рассматривают проблематику КИБ в органах государственной власти и в правоохранительной сфере соответственно. КИБ в органах государственной власти определяется как форма деятельности, направленная на сохранение ценной государственной информации, обеспечение национальной безопасности и рассматривается как часть корпоративной культуры. Культура информационно-психологической безопасности будущего специалиста по защите информации в правоохранительной сфере интерпретируется как культура информационно-психологической безопасности отдельной личности, при этом подчеркивается актуальность проблемы развития данной культуры. Н. С. Дерендяева приводит методику исследования сформированности культуры информационной безопасности школьников [10]. Л. В. Астахова обосновывает понятие корпоративного культурного капитала информационной безопасности как составной части культурного капитала организации, основываясь на анализе современных тенденций в сфере информационной безопасности: культура информационной безопасности как императив для снижения рисков информационной безопасности, подход к человеку как к капиталу, «безопасность через развитие» [11]. Также среди данных публикаций находится научная статья В. В. Сергеева, где автор исследует информационную безопасность как социокультурное явление и выявляет основные национальные интересы в культурно-информационной сфере, а затем рассматривает правовые основы культурно-информационной безопасности на примере российского мегаполиса [12].

Анализ стандартов по информационной безопасности показал, что напрямую о КИБ нигде речи не идет. Однако в стандартах по управлению информационной безопасностью серии 27000 и в стандартах по информационной безопасности ЦБ РФ присутствуют пункты о повышении осведомленности и об обучении персонала, что является одной из составляющих КИБ. В ГОСТ Р ИСО/МЭК 27005-2010. «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» в п. 11 «Коммуникация риска информационной безопасности» одними из целей для осознания риска причастными сторонами являются повышение осведомленности и получение новых знаний об информационной безопасности [13]. В ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» пункт 5.2.2 посвящен подготовке, осведомленности и квалификации персонала [14].

В стандарте ЦБ РФ СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» также отдельные требования (п. 8.9) предъявляются к разработке и организации реализации программ по обучению и повышению осведомленности в области информационной безопасности [15]. Соответственно в стандарте ЦБ РФ СТО БР ИББС-1.2-2014 «Обеспечение информационной безопасности организаций банковской системы РФ. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-

1.0-2014» имеется групповой показатель М18 «Разработка и организация реализации программ по обучению и повышению осведомленности в области информационной безопасности» [16].

Эксперты по информационной безопасности в своих блогах аналогично больше всего внимания уделяют повышению осведомленности персонала в вопросах информационной безопасности: составлению программ, методике оценки. Очевидно, что они отождествляют осведомленность с КИБ. Об этом пишет и А.Лукацкий [17], предлагая метрики для оценки программы осведомленности, и А. Прозоров [18], рекомендуя для создания программы осведомленности использовать американский стандарт NIST. Инновационный подход к развитию КИБ предлагает статья А. Лукацкого [19] о геймификации процесса формирования культуры ИБ, которая заключается в выстраивании процесса вовлечения персонала в информационную безопасность в занимательной форме и в оценке и награде отличившихся сотрудников, а также в социализации этой темы.

Для ответа на вопрос о том, как варьируется тематика исследований в зависимости от страны и наглядной демонстрации различия в развитости культуры информационной безопасности было принято решение выбрать страны с примерно одинаковым количеством научных публикаций в этой области из разных частей света. Таким образом проводилось сравнение тематики научных работ из США, Великобритании и России. Переведенный с английского языка на русский перечень тем можно увидеть в таблице 1.

Таблица 1

Сравнительный анализ аспектов изучения КИБ в США, Великобритании и России (2010–2017 гг.)

США	Великобритания	Россия
Воздействие программы информационной безопасности на КИБ	Анализ КИБ как часть анализа информационной безопасности банка.	Концепция КИБ
Роль культурных факторов и индивидуальных ценностей в управлении безопасностью сотрудников	Исследования последствий инсайдерских угроз банку. КИБ как средство их предотвращения	КИБ как элемент подготовки специалистов по защите информации
Человеческий фактор в КИБ. КИБ на предприятии по очищению воды	Исследования для оценки принятия КИБ в розничном магазине	КИБ в органах государственной власти
Трансформация КИБ при изменении структуры организации	Определение переменных, влияющих на создание системы КИБ	Проблема развития культуры информационно-психологической безопасности будущего специалиста по защите информации в правоохранительной сфере
Трансформация КИБ при объединении компаний	КИБ с позиций общей теории систем	Структура, критерии, уровни и показатели сформированности КИБ школьников
Влияние КИБ на принятие решений в области информационной безопасности	Пример оценки КИБ Конфиденциальность как процесс. КИБ как часть этого процесса	Информационная безопасность: риски, связанные с культурным капиталом персонала
Вариации КИБ в различных профессиях	Создание персонализированной КИБ	Актуальные проблемы обеспечения КИБ в современном обществе

Из табл.1. видно, что в США понятие КИБ используется давно, а потому исследования направлены на изучение того, как культура информационной безопасности влияет на другие части системы, где она развивается, как проявляет себя в разных профессиях, как меняется при изменении структуры компании. Понятие КИБ в США успешно интегрировано в деятельность человека в рамках организации, а потому проводится анализ того, как это сформировавшееся явление влияет на другие области. Такой набор аспектов изу-

чения свидетельствует о зрелости данного направления деятельности в этой стране.

Если в Америке КИБ заняла устойчивое место в системе информационной безопасности, то в Европе, в частности в Великобритании, КИБ находится в фазе активного внедрения в организационную среду. Создаются работы о том, как сотрудники принимают КИБ, производятся оценки культуры информационной безопасности, внедряются различные подходы к культуре с целью поиска оптимального подхода. Здесь пока нельзя говорить о зрелости сферы деятельности КИБ, но процессы ее развития уже активно реализуются в организациях.

В России почти вся тематика КИБ носит теоретический характер и не имеет дальнейшего применения на практике. Практика формирования КИБ на предприятиях, за исключением единичных случаев, ограничивается мероприятиями по повышению осведомленности сотрудников в области информационной безопасности, при этом зачастую - не самым эффективным способом. Тематика КИБ на отечественном поле весьма слабо исследована и в широкой практике понятие КИБ почти не применяется.

Следует также отметить, что в отличие от запада, где цель большинства исследований – повышение культуры безопасности отдельного гражданина, в России существует тенденция к приоритетному изучению КИБ применительно к структурам государственной власти. Это достаточно категорично замечает А. Лукацкий: «Ведь у нас нет культуры безопасности у граждан. Не только информационной, а вообще. У нас совершенно иная доктрина в стране. На первом, и похоже единственном месте у нас безопасность государства. Про безопасность общества и граждан у нас думают мало или совсем не думают» [20].

В нашей стране существуют также пробелы в исследованиях оценки КИБ, взаимовлияния КИБ и смежных культур, а также управления изменениями в этой области. Это обусловлено отсутствием самих процессов формирования и развития КИБ. Как было отмечено ранее, практическое применение теории к развитию КИБ на практике ограничивается мероприятиями по повышению осведомленности в этой теме. Причина заключается в отсутствии регулирования этого вопроса со стороны государственных регуляторов, в особенностях содержания стандартов и руководящих документов по информационной безопасности. Кроме того, стандарты в России имеют рекомендательный характер и не обязательны к исполнению.

Исходя из обоснованных выводов, определим понятие КИБ и обоснуем организационно-документационную модель ее развития. Эту модель можно использовать как полноценный инструмент управления этой сферой защиты информации с целью повсеместного применения на реальных объектах.

На начальном этапе уточним определение понятия КИБ на основе предложенных ранее. Четкая дефиниция КИБ необходима для того, чтобы в дальнейшем опираться на нее в организационно-документационных решениях. На основе [1-3, 5-6] представим наиболее цитируемые определения в таблице 2.

В последние годы акцент с изучения культуры информационной безопасности сместился на культуру кибербезопасности. R. Von Solms и J. F. Van Niekerk и др. обосновывают различия между культурой информационной безопасности и культурой кибербезопасности. Они справедливо подчеркивают, что кибербезопасность включает в себя не только защиту информационных ресурсов, но и человека: от угроз киберзапугивания, кибертерроризма, домашней автоматизации, незаконного совместного использования цифровых носителей информации в индустрии развлечений [21, 22]. В более чем 50 странах мира разработаны и внедряются стратегии кибербезопасности, предпринимаются активные попытки образования по вопросам кибербезопасности личности и организаций. Например, большой опыт развития культуры кибербезопасности в образовании накоплен Южно-Африканским академическим альянсом по кибербезопасности (SACSAA).

Расширение фокуса зрения от культуры информационной безопасности до культуры кибербезопасности – это, безусловно, важный шаг в развитии науки. Однако, по нашему мнению, кибербезопасность может рассматриваться как часть целого - информационной безопасности. Мы утверждаем, что информационное пространство – это более широкое понятие, чем киберпространство, поскольку в него включены не только электронные, но и бумажные носители информации, например, информации, составляющей государственную тайну предприятия. Поэтому субъектами информационных отношений в информационном пространстве выступают

Таблица 2

Авторские определения понятия КИБ

Автор(ы)	Переводная версия определения	Оригинал определения
Mirza, AlHogali	Набор знаний, гипотез, установок и ценностей, определяющих подход организации к соответствию требованиям информационной безопасности: защита информационных активов и воспитание техники безопасности сотрудников таким образом, чтобы информационная безопасность стала для них неотъемлемой частью профессиональной деятельности.	The collection of perceptions, attitudes, values, assumptions and knowledge that guides how things are done in organization in order to be consistent with the information security requirements with the aim of protecting the information assets and influencing employees' security behavior in a way that preserving the information security becomes a second nature
Da Viega	Отношения, предположения, убеждения, ценности и знания, которые сотрудники / заинтересованные стороны используют для взаимодействия с системами и процедурами организации в любой момент времени. Взаимодействие приводит к допустимому или неприемлемому поведению, проявляемому в артефактах и творениях, являющихся частью информационных активов организации.	defined information security culture as the "attitudes, assumptions, beliefs, values and knowledge that employees/ stakeholders use to interact with the organisation's systems and procedures at any point in time. The interaction results in acceptable or unacceptable behaviour evident in artefacts and creations that part of the way things are done in the organisation its information assets
Dhillon	Совокупность моделей поведения в организации, которые способствуют защите информации всех видов.	ISC is the totality of patterns of behaviour in an organization that contribute to the protection of information of all kinds
Martins	1) набор характеристик информационной безопасности, имеющих ценность в организации 2) предположение о приемлемости 3) поощрение соблюдения политик информационной безопасности 4) и то, как люди ведут себя по отношению к информационной безопасности в организации	a set of information security characteristics valued in organization the assumption about what is acceptable the assumption about encouraged information security behavior and the way people behave towards information security in the organization
Schlienger and Teufel	Все социально-культурные меры, которые поддерживают технические методы деятельности, так что информационная безопасность становится естественным аспектом повседневной деятельности каждого сотрудника	all socio-cultural measures that support technical activity methods, so that information security becomes a natural aspect in the daily activity of every employee
Ramachandran	Определение идей, убеждений и ценностей, связанных с безопасностью группы, которые формируют и определяют поведение, связанное с безопасностью	identifying the security related ideas, beliefs and values of the group, which shape and guide security-related behaviors
Von Solms	Внедрение аспектов информационной безопасности каждому сотруднику как естественного способа воплощения его повседневной работы	Von Solms calls for security culture creation within organization: By instilling aspects of information security to every employee as a natural way of perfoming his or her daily job

Астахова Л.В.	Особый способ организации информационной деятельности субъекта, представленной в виде ценностно-ориентированных моделей его действий как отправителя и получателя информации. Субъект определяет и контролирует существование и распространение единиц информации в их когнитивном и коммуникативном проявлении.	Information security culture is a specific mode of the organization and development of a subject's information activity, which is represented in the value oriented mod els of his information interaction as a sender and receiver of information, under which he determines and controls the unity of existence and development of information objects in their cognitive and communicative manifestations
Астахова Л.В.	Такой способ организации и развития человеческой жизнедеятельности в информационном пространстве, который обеспечивает качественную информационную среду: качество потребляемой информации, защищенность субъектов от негативных информационных воздействий (информационно-психологическая безопасность) и защищенность их информации (безопасность информации).	

пользователи не только компьютерных систем, но и традиционных, бумажных информационно-поисковых систем. Исходя из этого, будем использовать понятие культуры информационной безопасности.

Для уточнения понятия КИБ используем следующие обоснованные выше базовые требования к определению КИБ:

1. КИБ должна быть неотъемлемой частью повседневной деятельности сотрудника.

2. В состав КИБ должны включаться не только знания (осведомленность) в области информационной безопасности, но и ценностные модели информационного поведения субъекта.

3. КИБ должна способствовать не только защите информации, но и защите субъекта, который этой информацией оперирует.

4. КИБ должна способствовать не только защите информации и субъекта, но и их развитию, информационному обмену.

Исходя из этих принципиальных положений, **культура информационной безопасности** – это такой способ организации информационной деятельности субъекта, при котором знания и ценностные модели его поведения обеспечивают ему и другим субъектам безопасное функционирование и развитие в информационно-технологической среде.

Мы оцениваем это определение КИБ как наиболее полное и многоаспектное. Оно отражает современные тенденции развития общества и науки, имеет комплексный характер. Это определение КИБ является универсальным. Оно применимо к любому субъекту информационных отношений в современной культуре: личности, обществу и государству.

Уточним это определение в отношении пользователя информационной системы и предприятия в целом. **Культура информационной безопасности пользователя информационной системы** – это такой способ организации информационной деятельности пользователя, при котором знания и ценностные модели его поведения обеспечивают ему и другим пользователям безопасное функционирование и развитие в информационно-технологической среде. При необходимом и достаточном уровне КИБ пользователь контролирует существование и распространение информации, способствуя защите всех ее видов и защите других субъектов информационной деятельности таким образом, что это становится естественным аспектом выполнения его повседневной работы. **Культура информационной безопасности предприятия** – это такой способ организации информационной деятельности предприятия, при котором знания и ценностные модели поведения его сотрудников обеспечивают ему безопасное функционирование и развитие в информационно-технологической среде.

В качестве вектора направленности организационно-документационной модели развития культуры информационной безопасности предприятия мы берем за основу лучшие зарубежные практики. Ключевыми факторами успеха развития КИБ мы считаем следующие организационные решения:

• культивирование ценности информационной безопасности для бизнеса и активная поддержка развития КИБ руководством и заинтересованными сторонами;

• наличие ценностно-ориентированной стратегии развития КИБ, в которой были бы закреплены морально-нравственные установки информационного поведения сотрудников;

• развитие осведомленности и понимания сотрудниками угроз информационной безопасности и установление ответственности за нарушение ее правил. Важен не только сам факт наличия программы повышения осведомленности, но и качество и доступность ее содержания;

• создание актуальных материалов, постоянное обновление и применение современных практик для повышения уровня знаний сотрудников в области информационной безопасности;

• организация обратной связи с сотрудниками, предоставление им возможности высказать свое мнение и внести предложения. Таким способом они получают инструмент, с помощью которого сами смогут влиять на развитие КИБ в своей организации;

• разработка и утверждение метрик для оценки уровня КИБ организации и осуществления его мониторинга. Метрики позволят объективно оценить уровень культуры, выявить слабые и сильные стороны и сосредоточиться на тех вопросах, которые требуют улучшений, тем самым минимизировав экономические затраты и др.

С учетом названных факторов мы считаем необходимым разработку и утверждение следующих локальных организационно-распорядительных документов на предприятии: Стратегия развития КИБ, Методика оценки КИБ, Отчет об оценке КИБ, Процедура обучения и повышения осведомленности персонала, График и программа обучения персонала, Учебные материалы для обучения и повышения осведомленности персонала в области информационной безопасности, Система мотивации и поощрения персонала, Формы обратной связи для персонала, Устав проекта развития КИБ, Календарный план проекта развития КИБ, Положение о ролях и ответственности за реализацию развития КИБ и др.

Таким образом, анализ мировых информационных ресурсов по проблемам КИБ за 2010-2017 годы показал существенные различия в научных и практических подходах к этому феномену в разных странах. Наиболее слабое развитие КИБ получила в России. В отличие от развитых зарубежных стран, она отождествляется исключительно со знаниями (осведомленностью), ее ценностная составляющая не развивается, не оценивается, ее нормы и ответственность за их нарушение не устанавливаются и т.д. Это усиливает угрозы со стороны внутренних пользователей корпоративных информационных систем, негативно влияет на состояние информационной безопасности российских предприятий. Необходимы широкомасштабные исследования культуры информационной безопасности и культуры кибербезопасности личности, общества и государства, а также принятие национальной стратегии и программы их развития. Уточненное в статье понятие КИБ позволило нам разработать ряд организационно-документационных решений для их последующего внедрения в практику защиты информации отдельного предприятия.

Литература

1. Астахова, Л. В. Проблема оценки HR-уязвимости объекта защиты информации. // Вестник УрФО. Безопасность в информационной сфере. – 2011. – №1. – С. 26-34.

2. Alhogali, A., Mirza, A. Information Security Culture: A Definition and A Literature Review – URL: https://www.researchgate.net/publication/282754259_Information_Security_Culture_A_Definition_and_A_Literature_Review - (дата обращения: 08.01.2018).

3. Gcaza, N., von Solms, R. A strategy for a cybersecurity culture: A South African perspective // Electronic Journal of Information Systems in Developing Countries. – 2017.– 80(1). – С. 1–17.

4. Malyuk, A., Miloslavskaya, N. Cybersecurity culture as an element of IT professional training // 2016. 3rd International Conference on Digital Information Processing, Data Mining, and Wireless Communications, DIPDMWC 2016 7529390, С. 205–210.

5. Karlsson, F., Karlsson, J., A., M. Information security culture – state-of-theart review between 2000 and 2013 // Information & Computer Security. – 2015. - Vol. 23. Iss.3. - P. 246 – 285.

6. Astakhova, L.V. The concept of the information-security culture // Scientific and Technical Information Processing/ - 2014/ - 41(1)/ - С. 22–28.

7. Астахова, Л. В., Ульянов, Н. Л. Проблема кадровой безопасности в системе стандартов информационной безопасности банка России. // Вестник УрФО. Безопасность в информационной сфере. - 2014. - № 14. - С. 58–62.

8. Купрюхина, Л. И. Культура информационной безопасности в органах государственной власти // Инновации в гражданской авиации. - 2016. - №1. - С. 83–88

9. Ахметвалиева, А. А. Проблема развития культуры информационно-психологической безопасности будущего специалиста по защите информации в правоохранительной сфере // Наука ЮУрГУ: материалы 66-й научной конференции. Секции технических наук. – Челябинск, 2014. - С. 674–677.

10. Дерендяева, Н. С. Структура, критерии, уровни и показатели сформированности культуры информационной безопасности школьников // Наука и Школа. - 2016. - №5. - С. 190–195.

11. Астахова, Л. В. Информационная безопасность: риски, связанные с культурным капиталом персонала // Научно-техническая информация. Серия 1: Организация и методика информационной работы. - 2015. - №4. - С. 1–13.

12. Сергеев, В. В. Актуальные проблемы обеспечения культурно-информационной безопасности в современном обществе // Социально-гуманитарные знания. - 2011. - №5. - С. 252–260.

13. ГОСТ Р ИСО/МЭК 27005:2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности – М.: Стандартинформ, 2011. – 46 с.

14. ГОСТ Р ИСО/МЭК 27001:2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – М.: Стандартинформ, 2008. – 31 с.

15. Стандарт ЦБ РФ СТО БР ИББС-1.0-2014. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения. – М., 2014

16. Стандарт ЦБ РФ СТО БР ИББС-1.2-2014. Обеспечение информационной безопасности организаций банковской системы РФ. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0.-2014. – М., 2014.

17. Лукацкий, А.В. Как оценить программу повышения осведомленности? – URL: http://lukatsky.blogspot.ru/2011/08/blog-post_19.html - (дата обращения: 08.01.2018).

18. Прозоров, А. Н. Про повышение осведомленности сотрудников (Awareness and Training, NIST 800-50) – URL: http://80na20.blogspot.ru/2013/04/awareness-and-training-nist-800-50.html - (дата обращения: 08.01.2018).

19. Лукацкий, А. В. Геймификация ИБ: Как это было сделано в Saleforce.com – URL: http://lukatsky.blogspot.ru/2016/05/salesforcecom.html - (дата обращения: 08.01.2018).

20. Лукацкий, А. В. Где основы госполитики по культуре? – URL: http://lukatsky.blogspot.ru/2014/01/blog-post_21.html - (дата обращения: 08.01.2018).

21. Reid, R., J. Van Niekerk, and K. Renaud. Information Security Culture: A General Living Systems Theory Perspective // Information Security for South Africa. - 2014.

22. von Solms, R., and J. van Niekerk. From information security to cyber security // Computers & Security. - 2013. - №38. - P. 97–102.

References

1. Astahova, L. V. Problema ocenki HR-uyazvimosti ob"ekta zashchity in-formacii. // Vestnik UrFO. Bezopasnost' v informacionnoj sfere. - 2011. - №1. - S. 26–34.

2. Alhogali, A., Mirza, A. Information Security Culture: A Definition and A Literature Review – URL: https://www.researchgate.net/publication/282754259_Information_Security_Culture_A_Definition_and_A_Literaure_Review - (data obrashcheniya: 08.01.2018).

3. Gcaza, N., von Solms, R. A strategy for a cybersecurity culture: A South African perspective // Electronic Journal of Information Systems in Developng Countries. – 2017. - 80(1). - С. 1–17.

4. Malyuk, A., Miloslavskaya, N. Cybersecurity culture as an element of IT professional training // 2016. 3rd International Conference on Digital In-formation Processing, Data Mining, and Wireless Communications, DIPDMWC 2016 7529390, S. 205–210

5. Karlsson, F., Karlsson, J., A., M. Information security culture – state-of-theart review between 2000 and 2013 // Information & Computer Security. – 2015. - Vol. 23. Iss.3. - P. 246 – 285.

6. Astakhova, L.V. The concept of the information-security culture // Scien-tific and Technical Information Processing/ - 2014/ - 41(1)/ - C. 22–28.

7. Astahova, L. V., Ul'yanov, N. L. Problema kadrovoj bezopasnosti v si-steme standartov informacionnoj bezopasnosti banka Rossii. // Vest-nik UrFO. Bezopasnost' v informacionnoj sfere. - 2014. - № 14. - S. 58–62.

8. Kupryuhina, L. I. Kul'tura informacionnoj bezopasnosti v organah gosudarstvennoj vlasti // Innovacii v grazhdanskoj aviacii. - 2016. - №1. - S. 83–88

9. Ahmetvalieva, A. A. Problema razvitiya kul'tury informacionno-psihologicheskoj bezopasnosti budushchego specialista po zashchite in-formacii v pravoohranitel'noj sfere // Nauka YUUrGU: materialy 66-j nauchnoj konferencii. Sekcii tekhnicheskih nauk. – CHelyabinsk, 2014. - S. 674–677.

10. Derendyaeva, N. S. Struktura, kriterii, urovni i pokazateli sformirovannosti kul'tury informacionnoj bezopasnosti shkol'ni-kov // Nauka i SHkola. - 2016. - №5. - S. 190–195.

11. Astahova, L. V. Informacionnaya bezopasnost': riski, svyazannye s kul'turnym kapitalom personala // Nauchno-tekhnicheskaya informa-ciya. Seriya 1: Organizaciya i metodika informacionnoj raboty. - 2015. - №4. - S. 1–13.

12. Sergeev, V. V. Aktual'nye problemy obespecheniya kul'turno-informacionnoj bezopasnosti v sovremennom obshchestve // Social'no-gumanitarnye znaniya. - 2011. - №5. - S. 252–260.

13. GOST R ISO/MEHK 27005:2010 Informacionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Menedzhment riska in-formacionnoj bezopasnosti – M.: Standartinform, 2011. – 46 s.

14. GOST R ISO/MEHK 27001:2006 Informacionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Sistemy menedzhmenta informacionnoj bezopasnosti. Trebovaniya. – M.: Standartinform, 2008. – 31 s.

15. Standart CB RF STO BR IBBS-1.0-2014. Obespechenie informa-cionnoj bezopasnosti organizacij bankovskoj sistemy Rossijskoj Federacii. Obshchie polozheniya. – M., 2014

16. Standart CB RF STO BR IBBS-1.2-2014. Obespechenie informa-cionnoj bezopasnosti organizacij bankovskoj sistemy RF. Metodika ocenki sootvetstviya informacionnoj bezopasnosti organizacij ban-kovskoj sistemy Rossijskoj Federacii trebovaniyam STO BR IBBS-1.0.-2014. – M., 2014.

17. Lukackij, A.V. Kak ocenit' programmu povysheniya osvedom-lennosti? – URL: http://lukatsky.blogspot.ru/2011/08/blog-post_19.html - (data obrashcheniya: 08.01.2018).

18. Prozorov, A. N. Pro povyshenie osvedomlennosti sotrudnikov (Awareness and Training, NIST 800-50) – URL: http://80na20.blogspot.ru/2013/04/awareness-and-training-nist-800-50.html - (data obrashcheniya: 08.01.2018).

19. Lukackij, A. V. Gejmifikaciya IB: Kak ehto bylo sdelano v Sale-force.com – URL: http://lukatsky.blogspot.ru/2016/05/salesforcecom.html - (data obrashcheniya: 08.01.2018).

20. Lukackij, A. V. Gde osnovy gospolitiki po kul'ture? – URL: http://lukatsky.blogspot.ru/2014/01/blog-post_21.html - (data obrashcheniya: 08.01.2018).

21. Reid, R., J. Van Niekerk, and K. Renaud. Information Security Culture: A General Living Systems Theory Perspective // Information Security for South Africa. – 2014.

22. von Solms, R., and J. van Niekerk. From information security to cyber security // Computers & Security. - 2013. - №38. - P. 97–102.

ЛУШНИКОВА Светлана Станиславовна, студент кафедры «Защита информации» Южно-Уральского государственного университета. 454080, г. Челябинск, пр. Ленина, 76. E-mail: sslushnikova@mail.ru

АСТАХОВА Людмила Викторовна, доктор педагогических наук, профессор, профессор кафедры «Защита информации» Южно-Уральского государственного университета. 454080, г. Челябинск, пр. Ленина, 76. E-mail: lvastachova@mail.ru

LUSHNIKOVA Svetlana, student of the department "Information Security" of the South Ural State University. 454080, Chelyabinsk, Lenin Ave., 76. E-mail: sslushnikova@mail.ru

ASTAKHOVA Lyudmila, Doctor of Pedagogical Sciences, Professor, Professor of the Department of Information Protection of the South Ural State University. 454080, Chelyabinsk, Lenin Ave., 76. E-mail: lvastachova@mail.ru