Кодекс РФ об административных правонарушениях и УК РФ определили ответственность за правонарушения и преступления в сфере экономики.

Для устранения имеющихся недостатков законодательства, а также в целях прогнозирования появления новых способов совершения экономических преступлений необходимо на государственном уровне создать систему криминологической экспертизы разрабатываемых и принимаемых законов и нормативных актов, регулирующих сферу экономических отношений.

**Список литературы**

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 29.07.2017) (с изменениями и дополнениями, вступившими в силу с 26.08.2017).

2. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ).

3. Проект Федерального закона № 94800648-1 «О борьбе с организованной преступностью» (ред., принятая ГД ФС РФ в I чтении 22.02.1995).

4. Налоговый кодекс Российской Федерации (часть вторая) (с изменениями на 30 октября 2017 года).

5. Федеральный закон от 07.08.2001 № 115-ФЗ (ред. от 29.07.2017) «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

УДК 005.94

**А. С. Лобчикова**
Научный руководитель: Л. В. Астахова
Южно-Уральский государственный университет, Челябинск

## УПРАВЛЕНИЕ ЗНАНИЯМИ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

*Аннотация.* В данной статье проводится краткий анализ определений управления знаниями и анализ литературы по теме управление знаниями в информационной безопасности. Выделены основные направления исследований и подходы к данным темам.

*Ключевые слова:* управление знаниями; система управления знаниями; управление знаниями в информационной безопасности; управление знаниями в защите информации.

В современном мире в организациях все большее внимание уделяется знаниям и профессиональным компетенциям кадров. Для более эффективного использования этих ресурсов нужно построить модель управления — управления знаниями.

В научной литературе выделяется два подхода к определению понятия управление знаниями. В первом из них знание рассматривается как продукт, ресурс, обработав который можно получить прибыль.

Главное, на чем акцентируется внимание в данном подходе, — знание. Оно не обязательно должно быть связано с человеком, все процессы могут происходить независимо и самостоятельно. «Под управлением знаниями понимается система норм и правил, процедур и мероприятий, посредством которых приобретается и создается, используется и передается знание в организации» [1, с. 245]. Также в определениях данного вида говорится о том, что такой вид деятельности, как управление знаниями, должен приносить доход, как и любой другой ресурс в коммерческой организации, глобальная цель которой — получение прибыли.

Наиболее адекватен, на наш взгляд, другой подход к управлению знаниями, где делается акцент на том, что главным носителем знаний являются люди, и процесс управления в первую очередь будет связан именно с персоналом организации. Так, в определении А. Ю. Матвеева, выделены главные отличительные признаки управления знаниями — коллектив, мудрость и новаторство. Все эти слова не могут рассматриваться отдельно от человека, даже искусственный интеллект не сможет обеспечить эти качества [2]. А. И. Жилина в своем определении акцентирует внимание на том, что главная цель управления знаниями — это передача знаний от сотрудника к сотруднику для повышения эффективности деятельности организации [3]. А. В. Семенов с соавторами в своей книге на основе анализа существующих подходов к определению понятия «система управления знаниями» делает вывод о том, что управление знаниями «заключается в целенаправленном воздействии определенных субъектов социально-экономической деятельности на развитие корпоративного человеческого капитала с целью расширенного воспроизводства новых знаний и продуктов, обеспечивающих фирме конкурентные преимущества» [4, с. 43]. Здесь появляется новое понятие — «человеческий капитал» — значит, главным элементом системы управления знания является человек, и строиться она должна главным образом на процессах управления людьми.

Определение, данное Б. З. Мильнером, представляется нам наиболее полным, отражающим представление об управлении знаниями как отдельном и самостоятельном процессе, неотрывно связанным с человеком как главным элементом, протекающем в организации для достижения поставленных глобальных целей, в том числе и увеличение прибыли (путем повышения стои-

мости продукта) и уменьшение убытков, связанных с кадровой безопасностью и рисками, связанными с человеческим ресурсом (путем повышения лояльности сотрудников к компании) [5].

Но какими знаниями можно управлять? Всеми знаниями компании или можно выделить подсистемы по бизнес-процессам? Можно построить как общую систему управления знаниями компании, также можно разделить его на подсистемы по разным целям и предметам изучения. В качестве основы моего исследования за предмет изучения предлагается взять знания компании об информационной безопасности. В данной сфере существует большое количество определений, документов, событий и путей решения возникающих проблем, и построенная система защиты будет куда эффективнее, если одной из подсистем будет являться система управления знаниями. Такое построение поможет более быстро реагировать на инциденты и устранять их, работать с сотрудниками и обучать их, построить более защищенную систему.

В российской и зарубежной литературе встречается несколько подходов к построению системы управления знаниями в сфере информационной безопасности.

Один из них — использование программных продуктов для управления личной базой знаний для реализации системы управления знаниями об информационной безопасности. Это позволяет построить наглядную модель, отражающую все имеющиеся знания в компании. П. Ю. Филяк и С. Н. Федирко в своей статье предлагают для построения системы управления знаниями об информационной безопасности использовать программный продукт «Brain». В их статье описывается актуальность и необходимость применения визуализации накопленных знаний, так как это поможет специалистам решать задачи информационной безопасности, не углубляясь в знания законодательства — основной источник знаний в этой сфере. В данном случае знания рассматриваются отдельно от человека, как некий продукт, который можно внести на график, и стает понятно, как его обработать и передать, но это исключает из системы процессы управления людьми, что является недостатком данного подхода [6].

M. C. Kasapbaşi предложил к рассмотрению модель и программный пакет WebCoach, который работает как система управления учебной программой. Это веб-система, которая использует методы управления знаниями, чтобы преобразовать молчаливое знание опытных сотрудников отдела информационной безопасности и экспертов в этой области в явные знания, доступные сотрудникам всей организации, для обеспечения требуемого уровня их компетенций в процессах защиты информации [7].

В. Ф. Комарович в своей статье выделил три подхода к созданию системы управления защитой информации: системный, кибернетический и информа-

ционный подходы. Системный подход говорит о том, что в системе защиты информации участвуют и люди, и технические средства, поэтому в системе управления нужно учитывать их взаимодействие друг с другом. Иначе будет невозможно оценить защищенность системы комплексно. Кибернетический подход основан на том, что система должна быть динамичной, так как информация, необходимая для управления системой защиты информации, появляется в процессе жизни этой системы. Информационный подход вытекает из кибернетического, является его расширением. Целью этого подхода является грамотное отражение информации, полученной в результате наблюдения и анализа деятельности системы. В новой системе, которая будет дополнена опытом предыдущей системы защиты информации, должно происходить постоянное пополнение системы знаний. Данный автор выделяет общие элементы и качества, которыми должна обладать система управления знаниями об информационной безопасности, но в этой статье не хватает информации для практического применения этого подхода, отсутствуют примеры и на основание этой статьи, без дополнительного изучения темы, сложно представить действующую систему [8].

Изучение проблемы компьютерного мошенничества внутри организаций побудило исследователей подчеркнуть необходимость учета социальных аспектов информационной безопасности. В попытке свести к минимуму возможности для компьютерного мошенничества в статье S. Kesar утверждается, что осведомленность сотрудников и знание того, как организация функционирует, могут существенно повлиять на эффективность процессов обеспечения безопасностью [9]. Это связано с тем, что одни сотрудники могут отправлять «сигналы» другим сотрудникам, которые влияют на то, как последние воспринимают и соблюдают правила информационной безопасности в своей повседневной деятельности.

A. Schilling в своей статье предлагает создание общей базы решений проблем информационной безопасности [10]. Это позволит повторно использовать накопленные знания для разрешения возникающих инцидентов, что приведет к уменьшению времени устранения инцидента и уменьшению возможных рисков. Создание такой базы позволит повысить уровень защищенности системы и уменьшению денежных затрат на восстановление этой системы.

O. Lunacek обращает внимание читателей на то, что большое количество рисков в информационной безопасности связано с человеческим фактором, поэтому очень важно в процессе работы продолжать совершенствовать профессиональные навыки своих сотрудников. Для обмена знаниями между сотрудниками, внутреннего обучения и общения автор предлагает построить систему управления знаниями. Такая система поможет работникам понять процессы

обеспечения безопасности в контексте их собственной деятельности, деятельности организации и постоянно меняющейся окружающей обстановки [11].

Таким образом, давая определения системы управления знаниями, многие авторы сделали акцент на человеческом факторе как важном элементе, без которого невозможно построение эффективного управления знаниями. Однако управление знаниями в информационной безопасности изучено недостаточно. В литературе по этой актуальной проблеме не было найдено упоминаний о том, как управлять людьми как носителями знания при построении такой системы, а также обоснования того, что затраты на это принесут прибыль компании. Это свидетельствует о необходимости более глубоких исследований управления знаниями в сфере информационной безопасности.

**Список литературы**


1. *Попов М. В.* Трансформация традиционной системы управления знаниями в условиях интернет-среды // Государственное и муниципальное управление. Ученые записки СКАГС. 2015. № 4. С. 245–250.

2. *Матвеев А. Ю.* Введение в процесс управления знаниями // Бизнес-образование в экономике знаний. 2016. № 3 (5). С. 46–50.

3. *Жилина А. И.* Управление знаниями в условиях формирующейся системной парадигмы управления образованием начала XXI века // Региональное образование XXI века: проблемы и перспективы. 2012. № 4. С. 184–192.

4. *Семенов А. В.*, *Салихов Б. В.*, *Салихова И. С.* Инновационные аспекты управления корпоративными знаниями : монография. М. : Дашков и К, 2013. 148 с.

5. *Мильнер Б. З.* Концепция управления знаниями в современных организациях // Рос. журнал менеджмента. 2003. № 1. С. 57–76.

6. *Филяк П. Ю.*, *Федирко С. Н.* Обеспечение информационной безопасности с помощью технологии управления знаниями «BRAIN» // Информация и безопасность. 2016. Т. 19, № 2. С. 238–243.

7. *Kasapbaşi M. C.*, *Varol H. S.* Knowledge management integrated web-based information security course tutoring system // International Journal of Engineering Education. 2009. № 25(5). P. 1013–1019

8. *Комарович В. Ф.*, *Королев И. Д.*, *Лобашев А. И.* Интеллектный подход к управлению защитой информации в вычислительных сетях // Информация и космос. 2008. № 3. С. 113–119.

9. *Kesar S.* Knowledge management within information security: The case of barings bank // International Journal of Business Information Systems. 2008. № 3 (6). P. 652–667.

10. *Schilling A.* A framework for secure IT operations in an uncertain and changing environment // Computers and Operations Research. 2017. № 85. P. 1339–1351.

11. *Lunacek O.* Knowledge system new tool of the security experts education // 6th International Conference on Military Technologies. 2017. P. 430–434.

УДК 304.2+316.723

**С. С. Лушникова**
Научный руководитель: д-р пед. наук, проф. Л. В. Астахова
Южно-Уральский государственный университет, Челябинск

# КУЛЬТУРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЗАРУБЕЖНЫХ И РОССИЙСКИХ ИССЛЕДОВАНИЙ

*Аннотация.* В данной статье произведен анализ литературы, посвященной информационной и кибербезопасности, изданной в период с 2010 года по настоящее время. Выделены основные аспекты содержания публикаций и методики исследований данной темы.

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

Согласно статистическим исследованиям, устойчивой тенденцией является тот факт, что более двух третей ущербов, имеющих злонамеренный характер, исходит от персонала предприятия [1]. Несмотря на то, что защита информационного капитала крайне важна для обеспечения стабильной экономики [2], а недоразвитость киберкультуры может привести к серьезному ущербу не только в экономической отрасли, но и пошатнуть безопасность целой нации [3], область культуры информационной безопасности и кибербезопасности, которая закладывает морально-этическую основу отношения человека к защите информации, до сих пор слабо изучена. Цель данной статьи — охарактеризовать результаты сравнительного анализа публикаций, появившихся во второе десятилетие XXI века, посвященных культуре информационной безопасности и культуре кибербезопасности в зарубежных и российских источниках, и показать их потенциальные возможности для развития практики защиты информации на предприятии.

Анализ был произведен при помощи базы данных Scopus. Исследовались статьи, найденные по запросу «Cybersecurity culture» OR «Information security culture» за временной промежуток с 2010 года по настоящий момент. Выбор данного отрезка времени обусловлен тем, что существующие обзоры литерату-