Вестник Евразийской науки / The Eurasian Scientific Journal https://esj.today

2023, Том 15, № s6 / 2023, Vol. 15, Iss. s6 https://esj.today/issue-s6-2023.html

URL статьи: https://esj.today/PDF/32FAVN623.pdf

5.2.3. Региональная и отраслевая экономика (экономические науки)

Ссылка для цитирования этой статьи:
Сорокин, П. А. Разработка мер по совершенствованию системы защиты коммерческой тайны в целях повышения уровня экономической безопасности коммерческих организациях / П. А. Сорокин // Вестник евразийской науки. — 2023. — Т. 15. — № s6. — URL: https://esj.today/PDF/32FAVN623.pdf

For citation:
Sorokin P.A. Development of measures to improve the system for protecting trade secrets in order to increase the level of economic security of a commercial organization. *The Eurasian Scientific Journal*. 2023; 15(s6): 32FAVN623. Available at: https://esj.today/PDF/32FAVN623.pdf. (In Russ., abstract in Eng.)

УДК 338

Сорокин Павел Александрович
ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации», Москва, Россия
Факультет «Экономики и бизнеса»
E-mail: pavel.workspace@list.ru

Научный руководитель: **Гребенкина Светлана Александровна**
ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации», Москва, Россия
Факультет «Экономики и бизнеса»
Доцент кафедры «Экономической безопасности и управления рисками»
Кандидат экономических наук, доцент
E-mail: s.greb@list.ru

Разработка мер по совершенствованию системы защиты коммерческой тайны в целях повышения уровня экономической безопасности коммерческих организациях

Аннотация. Данная статья посвящена изучению института коммерческой тайны. Данный вопрос рассматривается в рамках деятельности коммерческих организаций. Автор утверждает, что для налаживания эффективной и стабильной защиты информации, представляющей ценность для собственника, прежде всего, необходимо учесть выявленные недостатки в правовой её составляющей. В статье проанализированы статистические данные относительно наиболее распространенных путей утечки информации. На основе проведенного анализа автор формулирует вывод о том, что руководству хозяйствующего субъекта необходимо уделять наибольшее внимание работе с персоналом, для необходимой защиты своих конфиденциальных данных. В работе представлен ряд рекомендаций, которые необходимо выполнять в случае, если сотрудник имел доступ к коммерческой тайне. При этом, по мнению автора, служба безопасности предприятия должна вести учет всех лиц, совмещающих работу в других компаниях. В рамках исследования также были выявлены наиболее распространенные проблемы в сфере обеспечения информационной безопасности организации. Внимание акцентируется на том факте, что для создания и поддержания необходимого уровня защищенности информации требуется слаженная работа всех служб под одним руководством. Автор считает, что для повышения уровня качества защиты информации необходимо ввести должность специалиста по информационной безопасности. В статье сформулированы требования, которые должны предъявляться к кандидатам на эту должность. Также автор отмечает, что существует вероятность разглашения информации, которой располагают сотрудники. В связи с этим были разработаны пути минимизации данного риска.

В заключительной части статьи автор рассчитывает эффективность предлагаемых мер, а также формулирует вывод о том, что обеспечение информационной безопасности — это многогранная проблема, которая требует задействования полного комплекса мер.

Ключевые слова: экономическая безопасность; информационная безопасность; организационная структура; коммерческая тайна; институт коммерческой тайны; внутренняя среда; управление рисками; оптимизация бизнес-процессов; минимизация экономических угроз

Введение

С увеличением объемов информации и глобализацией бизнеса, защита коммерческой тайны стала одной из наиболее актуальных и критических задач для современных организаций. В наше время информация — это не только ценный актив, но и ключевой элемент конкурентоспособности, который определяет успех или неудачу предприятия.

В мире, где технологические инновации моментально распространяются, а конкуренты стремятся выйти вперед, сохранение конфиденциальности бизнес-данных становится более сложной задачей. Организации должны не только обеспечивать безопасность своих коммерческих секретов, но и активно разрабатывать стратегии для защиты интеллектуальной собственности.

Цель данной работы — разработать меры по совершенствованию системы защиты коммерческой тайны коммерческих организаций.

Объект исследования — институт коммерческой тайны в системе экономической безопасности.

Предмет исследования — система защиты коммерческой тайны в коммерческих организациях.

1. Методы и материалы

Для достижения данной цели в работе были поставлены следующие задачи:

- рассмотреть данные статистики относительно утечки информации;
- выделить наиболее распространенные проблемы в сфере обеспечения информационной безопасности;
- определить основные навыки, которыми должен обладать ИТ-специалист организации;
- оценить эффективность предлагаемых мер.

В рамках проведения данного исследования автором использовался общенаучный метод, теоретический, методы анализа и синтеза, обобщение научных публикаций отечественных авторов.

Особое внимание было уделено теоретическим и практическим разработкам таких авторов, как: Золотарева И.В. [1], Есикова Р.С. [2], Колосов А.В. [3], Лебедь В.Н. [4], Графеев О.Е. [5], Оногда А.В. [6], Федорова Г.В. [7].

32FAVN623
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

2. Результаты и обсуждения

Согласно определению, закрепленному в Гражданском кодексе Российской Федерации, поддержка малого бизнеса считается жизненно необходимой для его развития. Однако развитие малых предприятий требует значительной поддержки со стороны государства, прежде всего в создании благоприятных экономических условий. Обеспечение экономической и финансовой безопасности становится важнейшим аспектом экономического развития страны и ее устойчивости к внутренним и внешним угрозам, особенно санкциям. Стратегия финансовой безопасности страны почти целиком сосредоточена на развитии малого бизнеса, который служит краеугольным камнем рыночной экономики, способствуя социальной и политической стабильности.

Распространение малых предприятий не только повышает качество жизни, но и способствует росту общих экономических показателей. В отличие от них крупные корпорации стараются оперативно адаптироваться к колебаниям рынка и удовлетворять меняющиеся запросы населения.

Для создания прочной и надежной защиты экономической и информационной безопасности первостепенное значение имеет устранение сложившихся правовых и организационных недостатков. Данные мероприятия предполагают определение субъекта и объекта защиты данных, выделение структур отделов, ответственных за охрану коммерческой тайны, и внедрение надежных мер безопасности в организации. Кроме того, настоятельно рекомендуется формализовать обязанности сотрудников по сохранению коммерческой тайны.

По статистике, вероятность утечки коммерческой тайны, вызванной различными факторами, такими как взяточничество, промышленный шпионаж или манипуляции сотрудников, составляет — 43 %. Получение информации непосредственно от сотрудников — 24 %, в то время как проникновение в компьютерные системы составляет — 18 %. Кража документов представляет собой 10-процентную угрозу, а на перехват телефонных разговоров приходится 5 % уязвимостей. Поэтому компаниям необходимо уделять первостепенное внимание защите конфиденциальных данных, делая особый акцент на эффективном управлении персоналом. Внутренняя динамика практически каждой организации включает в себя текучесть кадров, что подчеркивает важность соблюдения специальных протоколов при уходе сотрудника, имеющего доступ к конфиденциальной информации. В этой связи необходимо выполнить следующие действия:

1. Прежде всего убедитесь, что собраны все документы сотрудника, базы данных, носители информации и другие предметы. Очень важно принять у сотрудника удостоверение личности, ключи, печати и официальный бейдж.
2. С увольняющимся сотрудником следует начать подробный диалог, чтобы подчеркнуть важность защиты конфиденциальной информации и его роль в ее сохранении. Одновременно с этим первостепенное значение имеет своевременная выплата заработной платы. Воспитание сильной эмоциональной связи с бывшим местом работы служит мощным сдерживающим фактором против разглашения конфиденциальной информации.

На отдел безопасности компании возложена задача вести учет лиц, занимающих параллельные должности в разных компаниях. Соблюдение правил требует от сотрудников воздерживаться от работы на конкурентов, заниматься такой деятельностью только в нерабочее время, чтобы избежать конфликтов с основными обязанностями, защищать репутацию и финансовые интересы компании, соблюдать внутренние правила конфиденциальности коммерческой тайны и информировать своих непосредственных руководителей и службы безопасности [8].

32FAVN623
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

Информационная безопасность сталкивается с огромным количеством трудностей. Эти сложности вращаются вокруг элементов системы, связанных с защитой корпоративных данных, тонкого балансирования защиты жизненно важной информации в организации на фоне меняющейся динамики персонала и стремления к гармоничной рабочей среде. Важнейшее значение имеет преодоление вопросов, связанных с текучестью кадров, улучшением динамики коллектива и укреплением системы защиты информации в рамках организации.

Обеспечение создания и постоянного поддержания оптимального уровня информационной безопасности требует гармоничного сочетания всех служб, работающих под общим руководством. Волшебство раскрывается, когда существует негласная гармония — нерушимая связь понимания и непоколебимой поддержки, звучащая в каждом взаимодействии, будь то между самими руководителями или эхом разносящаяся по организационным коридорам, в конечном итоге приводящая к желаемым результатам [9].

Особенно важна интеграция ИТ-отдела и бухгалтерии в единую службу управления документами и информацией. Бухгалтерия должна принять и активно использовать современные технологии в своей работе, в то время как ИТ-отдел должен уделять больше внимания пониманию важности управления документами и информацией. Они также должны быть полностью осведомлены о важнейших вопросах, связанных с соблюдением законодательных и нормативных требований к управлению документами и информацией. Практический аспект управления информационной безопасностью в рамках бизнес-структуры в первую очередь находится в ведении ИТ-отдела, однако несколько отделов играют свою роль в этой сфере. Каждый отдел самостоятельно решает свои конкретные задачи, не координируя свои усилия с другими бизнес-функциями, что приводит к существенным пробелам в общей системе информационной безопасности. Чтобы решить эту проблему и повысить уровень защиты информации, необходимо ввести должность специалиста по информационной безопасности [9]. Этот специалист будет выполнять целый ряд задач, связанных с усилением мер безопасности (рис. 1).

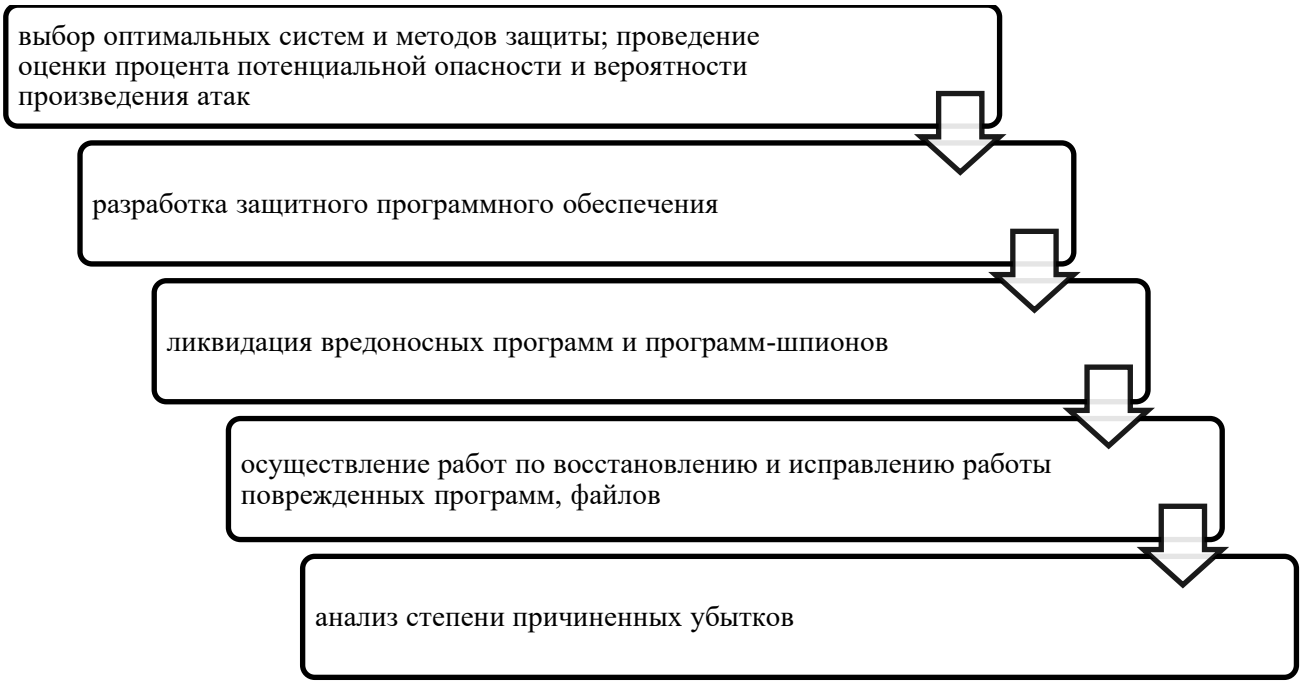

Рисунок 1. *Направления деятельности специалиста экономической безопасности [10]*

Квалификация специалиста экономической безопасности очень важна: он должен обладать широким спектром необходимых технических знаний и компетенций; иметь инженерное и математическое образование; понимать правовые нормы, касающиеся передачи

32FAVN623
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

и хранения данных; быть в курсе последних достижений и актуальных исследований; гарантировать комплексную систему защиты хранилища документов. Механизм безопасности с тремя уровнями воспринимается как более эффективный (рис. 2).

Рисунок 2. *Три уровня обеспечения информационно-экономической безопасности организации [10]*

Существует вероятность непреднамеренного разглашения информации сотрудниками, владеющими ею. Чтобы минимизировать этот риск, руководители отделов должны придерживаться следующей стратегии:

1. Работодатель должен создать благоприятную рабочую среду, которая снижает склонность сотрудников к поиску альтернативных возможностей трудоустройства. Для этого необходимы финансовые стимулы, сопоставимые с зарплатами в отрасли, и поощрительная бонусная структура, способствующая созданию гармоничного рабочего пространства и соблюдению этических норм.
2. Работодатели должны понимать, что ни один сотрудник не является незаменимым. Крайне важно иметь в штате резерв кадров. В условиях стабильности, когда сотрудники уверены в своем карьерном росте, они часто охотно передают свои знания для будущего продвижения по службе.
3. Формализация процедур и операций в различных областях путем их документирования в виде подробных инструкций по выполнению задач. Главная цель — обеспечить точное выполнение действий даже теми, кто не знаком с процедурами. Кроме того, подчеркивается важность делегирования полномочий и обязанностей отсутствующим сотрудникам.
4. Непосредственные руководители должны сообщать своим подчиненным исключительно важные детали. Для оптимизации эффективности задач важно избегать ситуаций, когда сотрудники могут получить доступ к данным, не соответствующим их должностным обязанностям. Слежение за ценными сведениями, которые собирают сотрудники, может значительно повысить уровень знаний организации.

Информационная безопасность представляет собой многогранную задачу, требующую целостного подхода, включающего в себя различные меры — от юридической документации до технических решений. Межличностный аспект имеет первостепенное значение в этом контексте, являясь одной из самых сложных областей. Без надежных высокопрофессиональных и преданных своему делу сотрудников, а также сплоченной команды обеспечение защиты

32FAVN623
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

информации остается недостижимым. Для проведения тщательного анализа необходима всесторонняя оценка. Необходимо тщательно изучить вопросы, описывающие уровень риска утечки информации (особенно коммерческой тайны до принятия контрмер), предлагаемые действия и уровень риска после принятия контрмер (табл. 1).

Таблица 1

Оценка эффективности мер

Проблема	Вероятность утечки информации до принятия мер	Решение проблемы	Уровень риска после принятия мер
Документооборот и техника			
Разрозненность мест хранения и отсутствие резервного копирования документов в подразделения	Высокая	Внедрение в организацию электронного архива, который позволит: решить проблему физического хранения документов путем их перевода в электронный вид; дать возможность при необходимости мгновенно блокировать доступ к информации; обеспечить конфиденциальности информации, защищенность документов архива от несанкционированного доступа любых частных лиц или организаций; обеспечить оперативный доступ к необходимой документации специалистов, работающих в различных подразделениях компании; исключить факты потери и распространения конфиденциальной информации	Низкий
Неполное или ненадежное документирование своей деятельности подразделениям	Высокая	Разработать общий регламент документирования сделок с покупателями. Назначить ответственных за исполнением.	Средний
Сбои в работе автоматизированных программ	Средняя	Поиск альтернативных провайдеров и способов подключения к сети Интернет (предпочтительней через оптоволокно)	Низкий

Составлено автором [11]

Исходя из приведенной выше таблицы, можем видеть, что существует высокая вероятность утечки секретной информации, однако после принятия рекомендуемых мер, рисковая вероятность снижается. Отдельно стоит упомянуть риск возникновения хакерских атак, в связи с цифровизацией экономики.

Так как коммерческие организации подвержены риску, то данный риск имеет место быть. Для минимизации данного риска необходимо принять следующие меры: установка на ЭВМ компании доверенной загрузки; средства межсетевого экранирования; средства антивирусной защита и системы защиты от вторжений; средства учета и контроля программного и аппаратного обеспечения; средства защиты информации от несанкционированного доступа (табл. 2).

Рассмотрение проблемы текучести кадров проливает свет на ключевую роль персонала в информационной безопасности. Они сталкиваются с различными рисками и проблемами, возникающими под влиянием руководителей.

32FAVN623
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

Таблица 2

Оценка эффективности мер

Персонал и текучка кадров			
Проблема плохой адаптации или ее отсутствие у сотрудников на испытательном сроке	Средняя	Во время испытательного срока необходимо назначить новому сотруднику наставника (опытного сотрудника), который помогал бы ему на этапе освоения в компании	Низкий
Перспектива получения более высокой зарплаты в другой компании	Средняя	Анализ рынка поставщиков оборудования, разработка системы внутреннего контроля	Низкий
Отсутствие карьерного роста	Средняя	Необходимо разработать программы по профессиональному и карьерному развитию персонала	Низкий
Некорректное поведение руководителей	Средняя	Требуется разработать или дополнить кодекс корпоративной этики, регламентировать взаимоотношения между руководителем и подчиненным, ввести анонимную горячую линию	Низкий

Составлено автором [11]

Текучесть кадров в организации служит важнейшим показателем эффективности ее кадровой политики. Речь идет не только об удержании персонала, но и об обеспечении успешного перехода сотрудников из одной организации в другую. Уход ценного сотрудника может вызвать дополнительный стресс, что подчеркивает необходимость организационной готовности. Задача руководства — разработать набор решений, направленных на стабилизацию уровня текучести кадров, стремясь снизить его ниже критического порога.

Выводы

Коммерческие предприятия во всех отраслях подвержены рискам экономической и информационной безопасности, связанных со сбором и использованием разнообразных данных. Сегодня информация рассматривается как товар, имеющий особую ценность. Бизнесмены часто выборочно работают с данными, которые приносят им прямую выгоду, и любая их потеря представляет собой угрозу экономической стабильности. Законодательство относит ограниченный круг данных к коммерческой тайне, однако от этой секретной информации часто зависит финансовое процветание компании.

Улучшение защиты конфиденциальной информации, особенно касающейся сотрудников, — важнейшая задача. Она служит основополагающей стратегией для предотвращения утечки данных и раскрытия конфиденциальной информации. Кроме того, становится очевидным, что гарантия защиты служебных знаний существенно переплетается с финансовой стабильностью организации в целом.

Такая взаимосвязь подчеркивает необходимость комплексного подхода, включающего правовые и технические меры по защите служебных знаний. Данный подход играет ключевую роль в обеспечении целостной экономической безопасности предприятия и поддержании высокого уровня конфиденциальности в операционной сфере компании. Поддержание и защита коммерческой тайны, также известной как коммерческая тайна, которая имеет огромную ценность для ее владельцев, напрямую затрагивает интересы как заинтересованных сторон, так и персонала компании. Поэтому она, несомненно, требует специальной защиты.

32FAVN623
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

ЛИТЕРАТУРА

1. Золотарева, И.В. Режим коммерческой тайны и организация защиты персональных данных в системе экономической безопасности предприятия / И.В. Золотарева, Т.В. Сушкова // Экономические исследования и разработки. — 2019. — № 12. — С. 110–114. — EDN VTYABJ.
2. Есикова, Р.С. Кадровая безопасность как одна из составляющих экономической безопасности организации / Р.С. Есикова // Социально-экономические явления и процессы. — 2017. — Т. 12, № 6. — С. 65–69. — EDN YNXFUD.
3. Колосов, А.В. Экономическая информация — как фактор определения и достижения хозяйственных целей / А.В. Колосов // Экономика. Предпринимательство. Окружающая среда. — 2005. — Т. 4, № 24. — С. 4–14. — EDN NXVIGX.
4. Лебедь, В.Н. Построение комплексной системы обеспечения экономической безопасности предприятия / В.Н. Лебедь, В.Н. Тисунова // Академик. — 2018. — № 3. — С. 12–21. — EDN YOHYEH.
5. Графеев, О.Е. Типовой перечень сведений конфиденциального характера для предприятий / О.Е. Графеев // Информация и безопасность. — 2018. — Т. 21, № 1. — С. 86–89. — EDN YNWKNN.
6. Оногда, А.В. Финансовые риски в системе обеспечения экономической безопасности предприятия / А.В. Оногда, Н.Н. Яркина // Евразийский научный журнал. — 2016. — № 3. — С. 204–208. — EDN WGXHMT.
7. Федорова, Г.В. Оценка процесса управления персоналом в системе обеспечения экономической безопасности организации / Г.В. Федорова, О.Ю. Иванова // Экономика и бизнес: теория и практика. — 2019. — № 11-3(57). — С. 113–117. — DOI 10.24411/2411-0450-2019-11405. — EDN ZTQTNV.
8. Ширко, Л.М. К вопросу о сущности экономической безопасности предприятия / Л.М. Ширко // Экономические отношения. — 2020. — Т. 10, № 4. — С. 1555–1564. — DOI 10.18334/eo.10.4.111327. — EDN LKUPOK.
9. Авдийский, В.И. Методологии определения пороговых значений основных (приоритетных) факторов рисков и угроз экономической безопасности хозяйствующих субъектов / В.И. Авдийский, В.К. Сенчагов // Экономика. Налоги. Право. — 2014. — № 4. — С. 73–78. — EDN TBILCX.
10. Безденежных, В.М. Формирование научной школы Департамента Экономической безопасности и управления рисками Финансового университета при Правительстве Российской Федерации / В.М. Безденежных // Экономика и управление: проблемы, решения. — 2023. — Т. 5, № 12(141). — С. 57–63. — DOI 10.36871/ek.up.p.r.2023.12.05.007. — EDN NOGNWD.
11. Сенчагов, В.К. Методология обеспечения экономической безопасности / В.К. Сенчагов // Федерализм. — 2007. — № 2(46). — С. 95–108. — EDN KWEIEB.

32FAVN623
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

Sorokin Pavel Alexandrovich
Financial University under the Government of the Russian Federation, Moscow, Russia
E-mail: pavel.workspace@list.ru

Academic adviser: **Grebenkina Svetlana Aleksandrovna**
Financial University under the Government of the Russian Federation, Moscow, Russia
E-mail: s.greb@list.ru

Development of measures to improve the system for protecting trade secrets in order to increase the level of economic security of a commercial organization

Abstract. This article is devoted to the study of the institution of trade secrets. This issue is being considered within the framework of the activities of commercial organizations. The author argues that in order to establish effective and stable protection of information that is valuable to the owner, it is first of all necessary to take into account the identified shortcomings in its legal component. The article analyzes statistical data regarding the most common ways of information leakage. Based on the analysis, the author formulates the conclusion that the management of a business entity needs to pay the greatest attention to working with personnel in order to ensure the necessary protection of their confidential data. The work presents a number of recommendations that must be followed if an employee had access to a trade secret. At the same time, according to the author, the enterprise security service must keep records of all persons combining work in other companies. The study also identified the most common problems in ensuring an organization's information security. Attention is focused on the fact that to create and maintain the required level of information security, the coordinated work of all services under one leadership is required. The author believes that in order to improve the quality of information security, it is necessary to introduce the position of information security specialist. The article formulates the requirements that must be presented to candidates for this position. The author also notes that there is a possibility of disclosure of information held by employees. In this regard, ways to minimize this risk have been developed. In the final part of the article, the author calculates the effectiveness of the proposed measures, and also formulates the conclusion that ensuring information security is a multifaceted problem that requires the use of a full range of measures.

Keywords: economic security; organizational structure; trade secret; Institute of Trade Secrets; internal environment; management of risks; optimization of business processes; minimizing economic threats

32FAVN623
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com