4. История развития робототехники [Электронный ресурс]. – URL: https://zen. yandex.ru/media/id/5a20825dad0f22233a285e05/istoriia-razvitiia-robototehniki-5a82d 2211 410 c332-86ea1e01 (дата обращения 10.01.2020).

5. Промышленные роботы [Электронный ресурс]. – URL: http://www. tadviser.ru/index.php/-Статья: Промышленные_роботы (дата обращения 10.01.2020).

Abstract

It is given a complex analysis of transdisciplinary ties, at the junction of which scientific achievements are possible affect global technological development. Definitions and existing classifications of robots are given. It is estimated the market scale of industrial and service professional robots. An analytical list of identified conditions and threats of robotization is provided.

Key words: robotization, hybrid environment, technological structure, density of robotics, industrial robots, investments, market size.

МРНТИ 06.01.29

Шин С.А.

Докторант DBA, Алматы Менеджмент Университет

Научный руководитель: Мухамедиев Б.М. д.э.н., профессор КазНУ им. аль-Фараби

г. Алматы, Республика Казахстан

shin_s@mail.ru

ВЗАИМОСВЯЗЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ВНУТРЕННЕГО АУДИТА КОМПАНИИ: РЕГИОНАЛЬНОЕ ИССЛЕДОВАНИЕ

Аннотация

Цель данного исследования - выявить факторы, которые влияют на характер взаимосвязи между внутренним аудитом и информационной безопасностью. Для минимизации рисков и защиты информации, организации принимают различные меры информационной безопасности, в том числепроектируют, внедряют и управляют различными процедурами и технологиями. Однако, внутренний аудит, оценивающий риски в области информационной безопасности и предоставляющий рекомендации по улучшениюее эффективности, не рассматривается как неотъемлемая составляющая эффективной системы информационной безопасности.

В данной работе было проведены интервью с менеджерами на основе исследования Пола Джона Стейнбарта и соавторов «Связь между

внутренним аудитом и информационной безопасностью: исследовательское расследование» и определено влияниеразличных факторов на эффективную взаимосвязь между внутренним аудитом и информационной безопасностью.
Ключевые слова: внутренний аудит, информационная безопасность, системы информационной безопасности.

Информация является одним из наиболее важных ресурсов компании, который формирует ее конкурентное преимущество. Сегодня защита информации становится одним из стратегических приоритетов делового мира в связи с быстрым развитием технологий. Компании могут столкнуться с потерей денег, времени, клиентов, рынка, репутации и различными штрафными санкциями из-за несоблюдения информационнй безопасности и, как следствие, потери информации. В связи с этим, все чаще компании принимают меры предосторожности и выделяют значительные инвестиции в обеспечение информационной безопасности (Yurtsever; 2013).

Информационная безопасность компании обеспечивает непрерывность бизнеса, а именно отсутствие перерывов и простоев, в тоже время минимизируя потери и используя коммерческие возможности (Doğantimur, 2009: 6). Угрозы информационной безопасности могут быть внутренними, внешними, случайными или вредоносными. С ростом использования новых технологий для хранения, передачи и получения информации учреждения все больше подвержены растущему числу угроз.

Основной целью информационной безопасности является защита информации от несанкционированного доступа, использования, обмена с другими, изменения, повреждения и уничтожения (Yurtsever; 2013).

Для компании прежде всего важно разработать последовательную политику снижения рисков информационной безопасности. Кроме того, следует создать разбивку информационных активов, принадлежащих компании, и назначить ответственных за каждый тип информации. Информационная безопасность должна решаться с использованием подхода, охватывающего весь персонал, а не как вопрос, который входит в обязанности одного или нескольких сотрудников компании (Yurtsever, 2013).

Руководство несет ответственность за обеспечение информационной безопасности всей важной информации, в то время как внутренний аудит оценивает риски в обеспечении информационной безопасности. Внутренний аудит рассматривается как одно из обязательных действий для надежности системы финансовой отчетности, соблюдения законов и нормативных актов, экономической эффективности, действенности и эффективности информационных систем, безопасности и надежности информационных систем (Uzun, 2013). Руководитель аудита должен иметь достаточные ресурсы для анализа внутренних и внешних рисков информационной безопасности (Solms, 2005: 443-446). Несмотря на важность и ценность взаимосвязи между внутренним аудитом и информационной безопасностью,

очень мало экспериментальных исследований о взаимосвязи этих функций. В Казахстане такие исследования не проводились.

В связи с этим, данное исследование рассматривает концепцию информационной безопасности и внутреннего аудита, представлен обзор литературы и результаты структурированного интервью, а также даны рекомендации.

Информационная безопасность

Ценности компании измеряются знаниями, которыми она обладает. Информация не должна рассматриваться только как актив, обрабатываемый информационными технологиями, она присутствует в различных структурах учреждения. Следовательно, информационная безопасность не должна рассматриваться как безопасность только информационных систем (AICPA и CICA, 2008).

Общим определением информационной безопасности является защита информации от опасности и угроз с целью обеспечения непрерывности производства и обслуживания, а также минимизации денежных потерь (Dlamini и др, 2009:1-10). Информационная безопасность может быть определена как обеспечение конфиденциальности, целостности и доступности защищаемой информации, которые рассматриваются как основные элементы информационной безопасности (Рис.1).

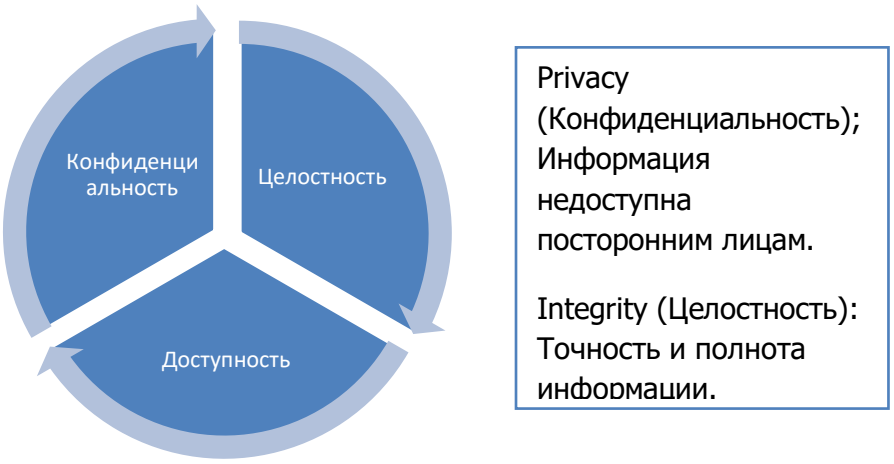

Рис.1 Основные элементы информационной безопасности (Doğantimur, 2009: 7).

В контексте информационой безопасности, данные аспекты не могуть быть расмотрены независимо друг от друга. Обеспечение конфиденциальности информации не должно препятствовать доступу к этой информации. Также важно обеспечить целостность доступной информации. Если защищена только информация и доступ к ней запрещен, эта информация, которая не может быть использована и не представляет никакой ценности. Если доступ предоставлен, но целостность не обеспечена, информация будет ложной или неполной, что может привести к

отрицательным результатам. Поэтому, чтобы иметь возможность говорить о концепции информационной безопасности, эти три элемента должны быть представлены вместе. В дополнение к этим элементам принципы информационной безопасности включают такие функции, как актуальность, ясность, непрерывность, прослеживаемость и надежность (Kaya Bengshir, 2008).

Обобщая опубликованную научную литературу по информационной безопасности, ИБ и корпоративное управление необходимо объединить через структуру управления информационной безопасностью (Posthumus, 2004: 638-646). В своем исследованиипо модели управления информационной безопасностью Солмс определяет действия, которые необходимо выполнить для функций управления, выполнения и контроля на всех уровнях организации (Solms and Solms, 2006: 408-412).В исследовании Мишры и Диллона, авторы заявляют, что роль отдельных действующих лиц и внутренних проблемы, связанных с управлением людьми в учреждении игнорировались в исследованиях и определениях, касающихся информационной безопасности (Mishra & Dhillon, 2006). В частности, исследование, проведенное Международным институтом внутреннего аудита, также ясно демонстрирует необходимость учета практики внутреннего аудита и информационной безопасности в рамках партнерского подхода (Phelps and Milne, 2008).

Внутренний аудит

Внутренний аудит по определению Международного института внутренних аудиторов является независимой и объективной деятельностью по обеспечению и консультированию, направленная на улучшение деятельности учреждения. Внутренний аудит помогает организации достичь своих целей, внедряя системный и дисциплинированный подход для оценки и повышения эффективности процессов управления рисками, контроля и корпоративного управления в организации (IIA, 2013).

Внутренний аудит оказывает поддержку в оценке рисков и контролирует деятельность по оценке, вносит предложения относительно деятельности, связанной с рисками и мониторингом, проверяет пригодность и эффективность средств контроля. Являясь одной из незаменимых мер по обеспечению надежности системы финансовой отчетности, соблюдения законов и нормативных актов, экономики, эффективности и результативности деятельности, безопасности и надежности информационных систем, внутренний аудит вносит большой вклад в установление управленческой ответственности на предприятии (Long, 2013).

Управление предприятием несет главную ответственность за обеспечение безопасности личной информации путем создания и наблюдения за инфраструктурой информационной безопасности. Внутренние аудиторы оценивают существующую структуру, выявляют риски и вырабатывают корректирующие предложения. При этом внутренние

аудиторы должны оценивать законы, нормативные акты, практики, взгляды юридического подразделения и методы обеспечения безопасности ИТ-отдела. Роль внутреннего аудитора в этом процессе может включать выполнение программы, выявление рисков и аудиторскую работу.

Уровень сотрудничества между внутренним аудитом и информационной безопасностью тесно связан с уровнем соответствия организации требованиям внутреннего контроля, связанным с информационными технологиями (Wallace et al. 2011: 185-212). Учитывая тесную связь и влияние между информационной безопасностью и внутренним аудитом, данные вопрос незаслужено остался не достаточно изученным.

Корпоративная информационная безопасность и внутренний аудит

Корпоративная информационная безопасность должна быть обеспечена в любой среде, где информация производится, обрабатывается и хранится. Для этого следует учитывать имеющееся программное обеспечение, оборудование, среду и человеческие ресурсы (Barrett, 2003: 56-58). Учреждения используют множество инструментов и методов для достижения желаемого уровня информационной безопасности. Меры информационной безопасности можно объединить под тремя основными заголовками (Рис. 2).

Рис.2 Меры информационной безопасности (Doğantimur, 2007: 22; Kaya Bensghir, 2008).

Корпоративная информационная безопасность - это живой процесс, который требует преемственности и должен включать управление, технологии и образование. Если между этими тремя элементами отсутствует взаимодополняемость, то невозможно обеспечить эффективную безопасность (Vural, 2007).

Информационные системы подчеркивают роль функции безопасности в реализации этих элементов управления. Однако функция внутреннего аудита организации должна периодически оценивать эффективность внутреннего контроля, включая безопасность информационных систем (IIA, 2005 и ITGI, 2007). Надежная инфраструктура информационной безопасности компании должна включает среды внутреннего контроля и мер обеспечения ИБ.

Посредством внутреннего аудита, эффективность и результативность мер обеспечения информационной безопасности могут быть повышены. Отсутствие связи между внутренним аудитом и менеджерами информационной безопасности может оказать негативное влияние на отношения между этими двумя функциями.

Отдел внутреннего аудита действует под руководством совета директоров, отчеты внутреннего аудита влияют на решения высшего руководства, особенно в отношении контроля. Например, внутренний аудит может сообщить о недостаточности используемой компьютерной системы на аппаратном и программном уровне. Необходимость предоставления достоверной информации удовлетворяется внутренним аудитом, а эффективность внутреннего аудита напрямую связана с эффективностью системы внутреннего контроля. Поэтому ряд мер информационной безопасности, в которые не включен внутренний аудит, будет недостаточен для решения проблем ИБ (Рис.3).

Рис.3. Взаимосвязь внутреннего аудита и средств управления ИБ

Метод исследования

В данном исследовании было проведено 20 интервью с менеджерами, отвечающих за внутренний аудит, обработку данных и информационной безопасности на 10 предприятиях, среди которых 2 университета, 2 представительства государственной администрации, 4 частные компании в г. Алматы. Целью интервью было выявить возможные факторы вляющие на

взаимосвязь между функциями информационной безопасности и внутреннего аудита. Средний опыт работы менеджеров более трех лет.

Встречи проводились с представителями, отвечающими как за внутренний аудит, так и за информационные системы и функции безопасности. Участники были проинформированы о цели исследования до интервью. Вопросы исследования были подготовлены на основе исследования Пола Джона Стейнбарта и соавторов «Связь между внутренним аудитом и информационной безопасностью: исследовательское расследование», в частности касались тем:

- Отношение высшего руководства к безопасности;
- Должность, ответственная за безопасность, которому предоставляются отчеты;
- Объем времени, потраченного на безопасность, используемые меры безопасности/ИТ;
- Особенности ИТ-инфраструктуры, численность ИТ-персонала;
- Количество ИТ-специалистов, отвечающих за ИБ, уровень образования, количество сотрудников с сертификатом безопасности, ИТ-бюджет, бюджет ИТ-безопасности;
- ИТ безопасность персонала и внутренний аудит участников;
- Уровень знаний в области ИТ, которыми обладают внутренние аудиторы;
- Демографические характеристики аудитора, наличие сертификатов, бюджет внутреннего аудита.

Результаты

По результатам интервью, были определены факторы, влияющие на отношения между внутренними аудиторами и экспертами, ответственными за информационную безопасность. В частности, личные и профессиональные характеристики аудитора (такие как уровень технических знаний, навыки общения и отношение) влияют на взаимосвязь между внутренним аудитом и функциями безопасности информационной системы. Этот вывод частично совпадает с результатами предыдущих исследований.

Как внутренние аудиторы, так и эксперты по безопасности информационных систем заявили, что недостаточный уровень знаний ИТ у внутреннего аудитора отрицательно сказался на их отношениях.

Было отмечено, что отношение и коммуникабельность участников влияют на отношения между ними. Участники вновь заявили, что физическое расположение (близость и удаленность) отделов внутреннего аудита и обработки данных, помимо организационной структуры, влияет на качество и частоту общения. Кроме того, ИТ-менеджер частной компании, которая ранее привлекала аутсорсинговую компанию для внутреннего аудита, определил отношения между ними как более формальные и только деловые отношения.

ИТ-специалисты, работающие в государственных органах и в университетах, отметили, что аудиторы превратили аудиторскую работу в инспекцию, которая создавала психологическое давление.

Все это показывает нам, что роль внутреннего аудита на предприятии не до конца понята другими отделами, но качество взаимоотношений и получаемой информации определяетя характеристиками аудитора и отношением.

Касательно роли высшего руководства в отношениях между внутренним аудитом и информационной безопасностью, результаты интервью совпадают с результатами аналогичных исследований, проведенных ранее. В частности; ИТ-специалисты и внутренние аудиторы, работающие в государственных предприятиях (местных администрациях и государственных университетах) заявили, что не считают, что высшее руководство в принципе поддерживает информационную безопасность, считают инвестиции очень высокими и не выделяют достаточный бюджет. С другой стороны, как ИТ-менеджеры, так и внутренние аудиторы, работающие в частных компаниях, считают, что необходимое бюджетное обеспечение информационной безопасности обеспечивается высшим руководством, и они поощряются в этом отношении.

Всеучастники определили, что тесная связь между внутренним аудитом и информационной безопасностью обеспечит учреждениям значительные преимущества. Эффективность и качество методов обеспечения информационной безопасности могут быть повышены за счет обратной связи, полученной от внутреннего аудита, при условии, что уровень технических знаний внутреннего аудитора соответствует.

Внутренние аудиторы также подчеркнули, что если роль и преимущества внутреннего аудита будут восприниматься положительно и приниматься всеми сотрудниками, могут быть достигнуты желаемые результаты в области информационной безопасности.

Заключение

Результаты внутреннего аудита повышают эффективность информационных систем безопасности организации, что в свою очередь повышает эффективность внутреннего аудита, поскольку хорошее управление информационной безопасности улучшит управление рисками на предприятии.

Регулярный мониторинг средств контроля информационной безопасности и обратная связь по их результатам повысят эффективность информационной безопасности учреждения. Хотя мониторинг средств контроля информационной безопасности обычно осуществляется ИТ-отделами, проверки и наблюдения со стороны внутреннего аудитора могут предоставить организации дополнительные преимущества (Wallace et al., 2011).

Когда элементы взаимосвязи между внутренним аудитом и информационной безопасностью будут полностью выполнены,

преимущества, которые он предоставит предприятиям, будут четко видны в результатах встречи. Комплексная и слаженная система внутреннего аудита и управления информационной безопасностью предприятия позволит определить угрозы и риски, обеспечить эффективное управление рисками, защитить и повымить корпоративную репутацию, обеспечить непрерывность бизнеса, контроль доступа к информационным ресурсам, повысить безопасность и информирование связанных сторон о безопасности, обеспечить целостность и точность информационных активов.

Несомненно, человеческий фактор и хорошие отношения между департаментами, отвечающими за внутренний аудит и информационную безопасность, являются важными инструментами для получения точной и надежной информации. Другие факторы влияющие на эффективность взаимосвязи этих функций включают постоянство процесса обеспечения корпоративной информационной безопасности, соблюдение установленных политик корпоративной безопасности, поддержка со стороны руководства. В качестве тем будущих исследований можно изучить взаимосвязь между внутренним аудитом и функциями информационной безопасности на разных уровнях и разных этапах деятельности компании.

Список литературы:

1. AICPA ve CICA, Trust Services Principles And Criteria. American Institute Of Certified Public Accountants And Canadian Institute Of Chartered Accountants, 2008.

2. Dlamini, M.T., Eloff, J.H.P, Eloff, M.M, Information Security : The Moving Target, Computer &Security, 2009.

3. Doğantimur, F., ISO 27001 StandardıÇerçevesindeKurumsaş Bilgi Güvenliği, TC MaliyeBakanlığıStratejiGeliştirmeBaşkanlığıMeslekiYeterlilikTezi, Ankara 2009.

4. Kaya Bensghir T., Kurumsal Bilgi GüvenliğiYönetimSüreci, TODAİ Mart 2008.

5. Kocameşe M., İçDenetimve Bilgi Güvenliği, http://denetimforumu. blogspot. com/2010/10/ic-denetim-ve-bilgi-guvenligi.html.

6. Mishra, S., And Dhillon, G., Information Systems Security Governance Research: A Behavioral Perspective in 1st Annual Symposium On Information Assurance, Academic Track Of 9th Annual NYS Cyber Securityconference, New York, USA , 18-26, 2006.

7. Uzun, Ali Kamil, İşletmelerde İçDenetim Faaliyetinin Başlatılmasında Başarı Faktörleri, http://www.denetimnet.com

8. Von Solms, Basie, Information Security Governance: COBIT or ISO 17799 or Both?, Computer &Security,vol 24, 2005.

9. Von Solms, Rossouw ve Von Solms, S.H. Bassie, Information Security Governance a Model Based on the Direct-control Cycle, Computer & Security, vol 25, 2006.

10. Vural, Y., Kurumsal Bilgi GüvenliğiveSızmaTestleri, YüksekLisansTezi, Gazi Üniversitesi Fen BilimleriEnstitüsü, 2007.
11. Wallace, L., Lin, H., And Cefaratti, M. A., Information Security And Sarbanes-Oxley Compliance: An Exploratory Study, Journal Of Information Systems 2011.
12. Yurtsever, G., Bilgi güvenliğiİçin Ne Yapmalı? TurcomoneyDergisi, Ocak 2013.
13. Сладкова М.Ю., Бекбаева З.А., Кабылхамит Ж.Т. Основные угрозы информационной безопасности. – Материалы межвузовской заочной научно-практической конференции «Современное состояние и перспективы развития науки и образования», 2014
14. Строков, К.А., Кузнецова, Т.В. Информационная безопасность предприятия. - Актуальные вопросы современной экономики. 2019 (1):271-274

Abstract

The purpose of this study is to identify factors that influence the nature of the relationship between internal audit and information security. In order to minimize risks and protect information, organizations take various information security measures, including design, implementation and management of various procedures and technologies. However, an internal audit assessing risks in the field of information security and providing recommendations for improving its effectiveness is not considered an integral part of an effective information security system.

In this work, interviews were conducted with managers based on a study by Paul John Steinbart et al "Relationship between Internal Audit and Information Security: A Research Investigation" and determined the influence of various factors on the effective relationship between internal audit and information security.

Key words: Internal audit, information security, information security system.