ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ И ИННОВАЦИОННОГО РАЗВИТИЯ ВНУТРЕННИХ ВОДНЫХ ПУТЕЙ В БАССЕЙНАХ ВЕЛИКИХ РЕК
Труды конгресса «Великие реки» 2018
Выпуск 7, 2018 г.

18-й МЕЖДУНАРОДНЫЙ НАУЧНО-ПРОМЫШЛЕННЫЙ ФОРУМ ВЕЛИКИЕ РЕКИ
ЭКОЛОГИЧЕСКАЯ, ГИДРОМЕТЕОРОЛОГИЧЕСКАЯ, ЭНЕРГЕТИЧЕСКАЯ БЕЗОПАСНОСТЬ
РОССИЯ - НИЖНИЙ НОВГОРОД, 17-20 мая 2018 года

ISBN 978-5-901722-60-2

УДК 658.15:004.056

И.П. Самойлова, старший преподаватель, ФГБОУ ВО «ВГУВТ»
603951, г. Нижний Новгород , ул. Нестерова, 5

СОВРЕМЕННЫЙ ФУНКЦИОНАЛ ФИНАНСОВОГО ДИРЕКТОРА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ключевые слова: IT-стратегия, кибербезопасность, ответственность финансового директора

Рост киберпреступности приводит к изменению приоритетов в работе финансового директора и повышению его внимания к вопросам IT-стратегии и кибербезопасности.

За последние несколько лет в России, как и во всем цивилизованном мире вырос уровень киберпреступности. Всё большее развитие информационных технологий постепенно переносит в информационные системы все процессы деятельности организации. Так, на сегодняшний день большинство банковских переводов производится посредством интернет-банкинга; активно развиваются электронные системы документооборота как внутри компаний, так и между различными компаниями. Всё это приводит к важности решения вопросов, связанных с информационной безопасностью.

Проблема становится ещё более актуальной, если учесть тот факт, что скорость развития информационных технологий превышает скорость подготовки (повышения квалификации) работников IT-служб компаний. В то же время, как на российском, так и на международном уровне активно формируются крупные сообщества киберпреступников. На встрече руководителей прокурорских служб стран БРИКС в 2017 году, которая была посвящена вопросам противодействия киберпреступности, генеральный прокурор России Юрий Чайка озвучил статистические данные о преступлениях, связанных с использованием информационных технологий. Так, за три с половиной года, с 2013-го по июнь 2017-го число таких преступлений возросло почти в десять раз. По прогнозам экспертов, в 2018 году по сравнению с предыдущим годом киберпреступления вырастут в 4 раза, возможный ущерб составит примерно два триллиона рублей.

На сегодняшний день достаточно сложно получить объективную информацию об уровне киберпреступности в отдельно взятых компаниях. Однако, если провести опрос среди финансовых директоров крупных корпораций, то все они подтвердят наличие попыток в этих компаниях воровства денежных средств путём вмешательства извне в информационные системы этих организаций, подмен реквизитов контрагентов, осуществление несогласованных платежей.

Таким образом, вопросы информационной безопасности не только приводят к росту вероятности рисков в деятельности отдельно взятой компании, но и к реальным денежным потерям, что формально находится в зоне ответственности финансового директора. Несмотря на то, что собственно вопрос информационной безопасности не относится к функционалу финансовых служб, мы рекомендуем ряд мероприятий, наличие которых сегодня должно стать частью обязательного регламента работы финансового

директора. Наиболее эффективным, на наш взгляд, будет соединение подобных мероприятий с бюджетным процессом организации и осуществление последних на регулярной основе.

Задачи финансового директора в области информационной безопасности мы рекомендуем реализовывать через процесс подготовки и контроля бюджета IT-подразделений предприятий. В первую очередь, такой бюджет должен базироваться на IT-стратегии организации. На практике финансовые директора нередко сталкиваются с инвестиционными запросами IT-служб, которые по факту оказываются неэффективными в силу того, что приобретение специального оборудования или технологии на поверку может оказаться устаревшим либо невостребованным. Последнее может быть актуальным в случае замены персонала IT-подразделения.

Важным моментом является тот факт, что, как показывает практика, повышение уровня информационной безопасности не всегда зависит от объема финансирования IT-службы, а зачастую определяется последовательным применением эффективной IT-стратегии. Как и многие другие сферы деятельности, область кибербезопасности является специфической и требует специальных знаний, которыми не всегда обладает финансовый директор, поэтому в качестве инструмента независимой оценки IT-стратегии компании, а также эффективности используемых средств защиты информации может выступить проведение IT-аудита. Услуги в области такого типа аудита на сегодняшний день обретают всё большую формализацию. Различные международные организации (ISACA, IIA, IAASB, PCAOB и др.) разработали стандарты и руководства в области IT-аудита: «IT Audit Framework 2nd Edition, «Cobit 5 for Assurance», «Global Technology Audit Guide». Однако наличие этих стандартов не исключают вариативность проведения IT-аудита. В российской практике нередко услуги по аудиту информационных технологий дополнительно включают услуги этичного хакинга.

Если возвращаться непосредственно к функционалу финансовых директоров, то одной из их задач является обеспечение работоспособности финансовой информационной системы. Многие организации в настоящее время переходят на системы класса ERP (Enterprise Resource Planning). Требования в области повышения эффективности бизнеса заставляют организации получать информацию в существенно большем количестве аналитических разрезов, что увеличивает требования к производительности действующих информационных систем в области бухгалтерского учета и финансов. Смена информационных систем – это дорогостоящее и длительное мероприятие, поэтому решение о выборе новой информационной системы или модернизации существующей должно осуществляться заблаговременно в соответствии с долгосрочной стратегией развития компании.

Список литературы:

[1] Чайка Ю. Я. Выступление на III встрече руководителей прокурорских служб государств БРИКС / Официальный сайт Генеральной прокуратуры Российской Федерации. - Режим доступа: https://genproc.gov.ru/smi/news/news-1237284/

[2] Ибрагимов Р. С. Виноват ли робот / Материалы конференции «Телеком 2018. Курс на технологическое лидерство». - Режим доступа: https://www.vedomosti.ru/newspaper/articles/2018/05/28/770989-vinovat-robot

THE MODERN FUNCTIONAL OF FINANCIAL DIRECTOR IN THE FIELD OF INFORMATION SECURITY

I.P.Samoilova

Keywords: IT strategy, cybersecurity, responsibility of CFO.

The growth of cybercrime leads to changes in the priorities in the work of the CFO and increases their attention to the issues of IT strategy and cybersecurity.