УДК 336.051
DOI 10.18413/2411-3808-2018-45-3-492-496

ЗЕРКАЛЬНАЯ ИНФОРМАЦИЯ КАК ИСТОЧНИК ФИНАНСОВОГО РИСКА
MIRROR INFORMATION AS A SOURCE OF FINANCIAL RISK

А.А. Салкуцан
A.A. Salcutan

ФГБОУ ВО «Российский экономический университет им. Г.В. Плеханова»,
Россия, 117997, г. Москва, Стремянный переулок, д. 36

FGBOU VO "The Russian Economic University named after G.V. Plekhanov",
36 Stremyanniy lane, Moscow, 117997, Russia

E-mail: asalcutan@bk.ru

Аннотация
На определенном этапе своего развития любая организация сталкивается с серьёзными рисками по защите своих данных, разного рода информации от различных типов мошенников, начиная с конкурентов и заканчивая хакерами. Защита информации внутри организации как на локальном, так и на внешнем уровне не всегда соответствует современным угрозам, так как у каждой организации есть своя уникальная автоматизированная система, обеспечивающая целостность, конфиденциальность и доступность информации. В различных странах мира в средствах массовой информации распстраняется огромное количество информации по поводу потери больших баз данных ценной информации, в результате чего множество компаний и даже государства терпят убытки и теряют репутацию. Поэтому развитие и совершенствование методов защиты информации определены наличием целого ряда рисков и источников угроз, которые в той или иной степени влияют на информационную безопасность организации.

Abstract
In a certain period of development every organization faces serious risks for the protection of their data different kind of information from various types of scams from the competition and endmg with the hackers. Protection of information within the organization on a local appearance level do not always meet modern threats, as each organization has its own unique automated system, to ensure the integrity, confidentiality and availability of information. In various countries of the world in the media funneling a huge amount of information about the loss of large databases of valuable information, resultmg in many companies and even the state loses not only the losses, but also reputation. Therefore, the development and improvement of methods for information protection identified a number of risks and threat sources, which in varying degrees affect the information security of the organization.

Ключевые слова: идентификация, конфиденциальность, утечка данных, бюджетирование, риск-менеджмент, денежный поток.
Keywords: dentification, privacy, data leakage, budgeting, risk management, cash flow.

Введение

На сегодняшний день в мировой экономике наблюдается огромное число утечек конфиденциальной информации на уровне бизнес-структур и государств. Подобное явление объясняют кластеризацией экономики и процессами налоговой и финансовой консолидации. Данные структуры (кластеры) в условиях информатизации и компьютеризации являются частью мировой информационной среды, главным инструментом достижения конкурентоспособности территорий, но при этом таят в себе множество угроз, которые парализуют всю внутреннею локальную среду, нарушая при

этом весь финансово-информационный контур информационной безопасности [Цифровой клан: как устроен IT-бизнес детей куратора интернета в ФСБ, 2017]. Максимальные прецеденты затрагивают кредитные организации и денежные потоки организаций. Внедрение новых автоматизированных систем, которые ставит себе организация, зависит от её политики безопасности и финансирования. Риск-менеджмент в компаниях начинается с финансовых потоков. Современные управленческие технологии, например бюджетирование, ориентированы прежде всего на денежный поток. Бюджетирование должно обеспечить контроль над расходованием денежных средств на всех этапах и адресность респондентов. Наличие современных технических средств обработки и передачи данных, методов и алгоритмов обработки в виде соответствующего программного обеспечения персонала предопределяет судьбу организации на уровне безопасности в целом [Dudin M.N., 2015].

Основные результаты исследования

Развитие управленческих технологий существенно изменило правила хранения и накопления конфиденциальной информации. Поэтому любое вмешательство во внутренние денежные потоки организации может не только привести к краже, искажению или несанкционированному доступу к секретным данным, но и создать угрозу персоналу и вызвать риск потери капиталов. Нужно всегда помнить, что уязвимыми звеньями в информационной среде всегда являются клиенты, акционеры и партнеры. Поэтому, говоря об обеспечении их финансовой безопасности, нужно понимать, что если обеспечить защиту от нападения мошенников соответствующих субъектов, которые взаимодействуют в процессе автоматизированного информационного обмена, организация может минимизировать свои финансовые убытки. Термин «информационно-финансовая безопасность» является общесистемным, наиболее масштабно отражающим предпосылки для устойчивого развития организации в соответствии с её приоритетами и целями [Kiseleva I.A., 2017]. Поэтому информационно-финансовая безопасность подразумевает в первую очередь создание финансовой безопасности, которая обеспечивает стабильное функционирование организации, защиту её интересов и гармоничное развитие. К основным целям финансовой безопасности организации относятся [Грызунова Н.В., 2014]:

– обеспечение высокой финансовой эффективности, платежеспособности и автономности организации;

– обеспечение технологоемкости и достижения высокой конкурентоспособности технического потенциала;

– достижение оптимального и эффективного организационного бюджетирования как системы управления;

– достижение высокого уровня квалификации и конкурентоспособности персонала;

– минимизация негативных конъюнктурных и арбитражных результатов производственно-хозяйственной деятельности;

– финансово-правовая защищенность всех аспектов деятельности организации.

Для решения поставленных целей организация должна провести оценку рисков и сформировать прогноз своего состояния с точки зрения выполнения мер защиты от воздействия различных внутренних и внешних факторов [РосБизнесКонсалтинг. Киберспецслужба].

Так, мировой тренд утечек информации затрагивает различные отрасли экономики, что приводит к огромным финансовым потерям. Так, например, в начале сентября в США 2017 г. произошла масштабная утечка данных, которую допустило одно из крупнейших бюро кредитных историй в мире – Equifax. Хакерами была украдена личная информация 143 млн человек. В России среди всех утечек данных можно выделить несколько наиболее значимых. Самой крупной среди них является атака на базу учетных данных Mail.ru, в ходе которой было скомпрометировано более 25 миллионов записей [Новая доктрина информационной безопасности России, 2015].

Однако сегодня в условиях все более усиливающейся глобализации меняются денежные потоки. Они трансформируются в главный фактор, который определяет условия

развития как организации, так и экономики в целом любого государства. С развитием цифровой экономики вопросы финансовой безопасности переросли отраслевые рамки и широко обсуждаются на самом высоком уровне. Сама тема утечек финансовой информации становится все более прозрачной, и это должно позитивно сказаться на общем уровне экономической безопасности [РосБизнесКонсалтинг].

Даже в России пострадавшие организации начинают рассчитывать ущерб, который был нанесен им в результате той или иной утечки. В июне 2017 г. стало известно о том, что объем утечек конфиденциальной информации в России за год вырос в 100 раз. Данные привела компания InfoWatch, специализирующаяся на корпоративной информационной безопасности. По итогам 2016 г. эксперты насчитали в России около 213 случаев утечки информации, в результате чего было скомпрометировано 128 млн записей конфиденциальных данных, в том числе относящихся к банковским картам и счетам. Количество утечек, по сравнению с 2015 годом, повысилось на 89%, а объем данных, утерянных из-за этих инцидентов, увеличился более чем 100-кратно [РосБизнесКонсалтинг].

Для бизнеса наличие мощной системы управления финансовой безопасностью играет огромную роль, так как разработка стратегии финансовой безопасности в период падения спроса и производства связана с целым рядом негативных факторов:

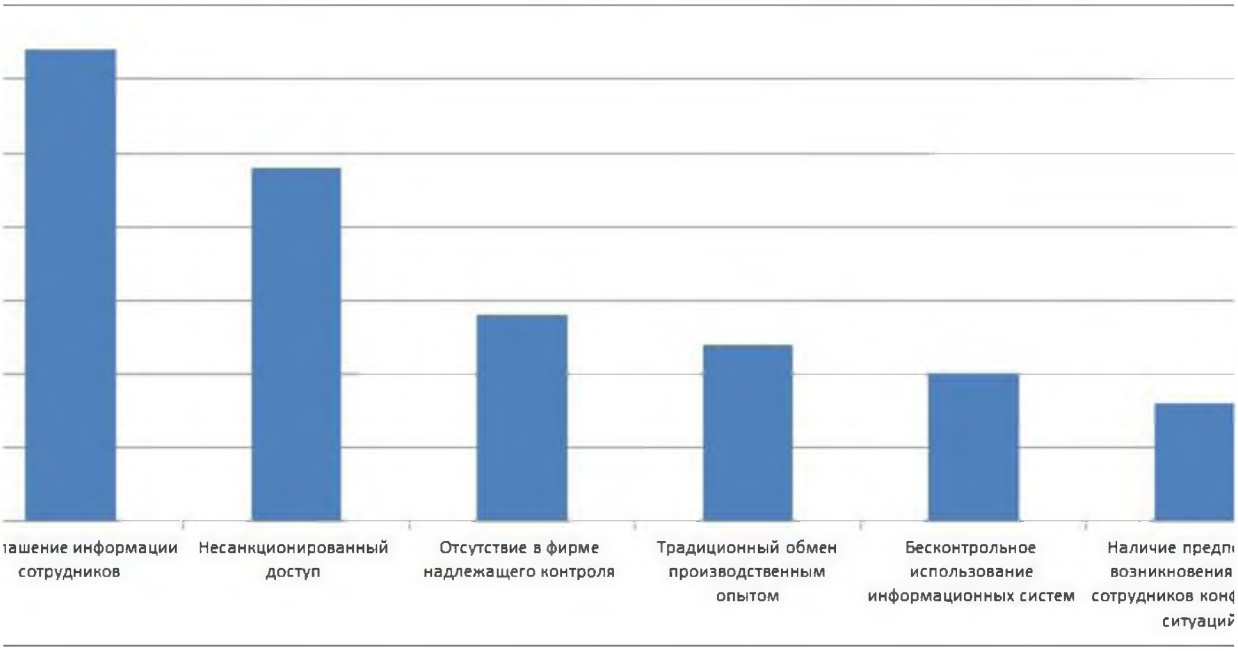
– угрозой уменьшения запаса финансовой прочности компании по отношению к возможным потерям и убыткам в том числе за счет хищений, халатности и ошибочных действий персонала;

– учащением случаев недобросовестных действий менеджеров и сотрудников;

– повышенным риском мошенничества со стороны контрагентов и др.

Наиболее актуальными и значимыми, как это ни печально, оказываются угрозы, источником которых выступают пользователи системы и ее обслуживающий персонал, то есть сотрудники компаний. Согласно данным портала информационной безопасности Content Security степень опасности внутренних и внешних угроз такова (рис.).

Рис. Источники угрозы финансовой безопасности [Церцеил Ю.С., 2017]
Fig. 1. Sources of threats to financial security [Tsertseil J.S., 2017]



Сегодня, как показывает практика, существуют различные каналы утечки финансовой информации. Так, сотрудники организации как случайно, так и целенаправленно передают за пределы родной организации чаще всего следующие сведения [Церцеил Ю.С., Кокуева В.В., Грызунова Н.В., 2017]:

– документы, характеризующие финансовое состояние и планы организации (управленческие финансовые отчеты, налоговые декларации, первичную бухгалтерскую документацию, меморандумы и бизнес-планы, договоры и т.д.);

– персональные данные клиентов и сотрудников организации;

– технологические и конструкторские разработки, ноу-хау компании и т.п.;

– внутренние документы (служебные записки, аудиозаписи совещаний, презентации «только для сотрудников» и т.д.);

– технические сведения, необходимые для несанкционированного доступа в сеть организации третьих лиц (логины и пароли, сведения об используемых средствах защиты и т.п.).

По статистике аналитического отдела компании Falcongaze, которая является разработчиком системы информационной безопасности SecureTower, за 2016 год около 57% всех случаев утечки конфиденциальных сведений из компаний произошли по вине самих сотрудников. Также стоит отметить наиболее часто используемые каналы потенциальной утечки:

– шифрованная электронная почта;

– социальные сети;

– USB-носители (флешки, внешние жёсткие диски и т.д.);

– внутренние принтеры и интернет-мессенджеры.

Подводя итоги, следует упомянуть о том, что существует большое число каналов утечки информации. Различные бизнес-структуры и государство предлагают различные способы по защите информации:

– программные средства, например продукты Kaspersky Office Security, Системы контроля и управления доступа компании СБ Цитадели и т.д;

– аппаратные средства, которые специализируются на обработке и шифровании информации, например «МФИ Софт», «Норси-Транс», «ТехАргос СпецСистемы», «Специальные Технологии» и Линтехно;

– законодательные средства, которые включают разработку комплекса нормативно-правовых актов: ГОСТ 28147-89, ГОСТР 34.10-94, ГОСТР 34.11-94, Закон РФ № 24-ФЗ, Приказ ФАПСИ № 152 и т.д.

Заключение

Объем рынка продаж средств информационной безопасности для госсектора, организаций, а также спецслужб составляет до 15 млрд руб. В этой сфере очень много регуляторов, и только получив ряд сертификатов и лицензий, организация сможет реализовывать свою продукцию.

Так, на сегодняшний день главный банк страны Сбербанк предлагает создать национальный центр кибер-безопасности, который должен обеспечить информационную безопасность в стране. Летом 2017 г. была предложена и подписана программа «Цифровая экономика», которая предлагает образовать централизованную систему мониторинга и управления сетями связи, снизить объемы трансграничного трафика в Рунете, законодательно закрепить контроль над использованием больших данных, а также содержит ряд других инициатив. Центр кибер-безопасности должен объединить в себе такие крупные IT-компании, как Сбербанк, «Ростелеком», «Ростех», «Росатом», фонд «Сколково», «Яндекс», Mail.Ru Group, «Яндекс», «МегаФон» [Церцеил Ю.С., 2017].

Аналоги такого центра имеются в ряде зарубежных государств. Например, в США такой центр уже существует в качестве подразделения Министерства внутренней безопасности США, но занимается только защитой сетей связи правительства страны. В Германии аналогичная структура создана в 2011 г. и подчиняется Федеральному управлению по информационной безопасности. В Великобритании центр был создан в 2016 г. и является подразделением центра правительственной связи.

Список литературы
References

1. Дудин М.Н., Frolova Е.Е., Грызунова Н.В., Шувалова Е.Б. 2015. Тройная модель спирали как механизм для сотрудничества между государством, бизнесом и научно-образовательным сообществом в области организации национального инновационного развития. Азиатская Социология, 11 (1): 230–238.

Dudm M.N., Frolova E.E., Gryzunova N.V., Shuvalova E.B. 2015. The triple helix model as a mechanism for partnership between the state, busmess, and the scientific-educational community in the area of organizmg national mnovation development. Asian Social Science, 11 (1): 230–238. (in Russian)

2. Киселева И.А., Тсетсги Б., Симонович Н.Е., Тихомиров Н.П., Тихомирова Т.М., Грызунова Н.В., Шувалова Е.В., Карманов М.В., Коротков А.В., Кузнецов В.И., Трамова А.М. 2017. Управление Rrisk в условиях экономического кризиса. Улан-Батор.

Kiseleva I.A., Tsetsgee B., Simonovich N.E., Tikhomirov N.P., Tikhomirova T.M., Gryzunova N.V., Shuvalova E.B., Karmanov M.V., Korotkov A.V., Kuznetsov V.I., Tramova A.M. 2017. Rrisk management in the conditions of the economic crisis. Ulaanbaatar. (in Russian)

3. Грызунова Н.В. 2014. Управление финансами хозяйствующих субъектов: современные технологии кредитования рыночных субъектов в условиях дефицита ликвидности. Статистика и Экономика, 6–2: 285–288.

Gryzunova N.V. 2014. Fmancial management of busmess entities: the modern technology of lendmg market actors in the context of lack of LIQUIDITY. Statistics and Economics. 6–2: 285–288. (in Russian)

4. РосБизнесКонсалтинг. Киберспецслужба: Сбербанк предложил создать штаб борьбы с хакерами. URL: https://www.rbc.ru/technology_and_media/01/09/2017/59a9799f9a7947375702db15 (дата обращения: 3.12.2017).

RosBusinessConsulting. CyberSpetservice: Sberbank proposed to create a hackmg headquarters. Access mode: Available at: https://www.rbc.ru/technology_and_media/01/09/2017/59a9799f9a7947375702db15 (accessed: 3/12/2017). (in Russian)

5. РосБизнесКонсалтинг. Новая доктрина информационной безопасности России. URL: https://www.rbc.ru/politics/06/12/2016/584693759a79472bbf7195f3 (дата обращения: 3.12.2017).

RosBusinessConsulting. CyberSpetservice: Sberbank proposed to create a hackmg headquarters. Available at: https://www.rbc.ru/technology_and_media/01/09/2017/59a9799f9a7947375702db15 (accessed: 3/12/2017). (in Russian)

6. РосБизнесКонсалтинг. Объем утечек конфиденциальной информации в мире в 2017 г. вырос в 8 раз. URL: Объем утечек конфиденциальной информации в мире в 2017 г. вырос в 8 раз Подробнее на РБК: https://www.rbc.ru/technology_and_media/10/10/2017/59db57549a7947f8d8839ac3 (дата обращения: 3.12.2017).

RosBusinessConsulting. The volume of leakage of confidential mformation in the world in 2017 increased by 8 times. Available at: The volume of leakage of confidential mformation in the world in 2017 mcreased by 8 times. More on RBC: https://www.rbc.ru/technology_and_media/10/10/2017/59db57549a7947f8d8839ac3 (accessed: 3.12.2017). (in Russian)

7. РосБизнесКонсалтинг. Объем утечек конфиденциальной информации в России за год вырос в 100 раз. URL: https://www.rbc.ru/technology_and_media/08/06/2017/5937ddda9a79471a1683d2a2 (дата обращения: 3.12.2017).

RosBusinessConsulting. The new doctrine of mformation security in Russia. Available at: https://www.rbc.ru/politics/06/12/2016/584693759a79472bbf7195f3 (accessed: 3/12/2017). (in Russian)

8. РосБизнесКонсалтинг. Цифровой клан: как устроен IT-бизнес детей куратора интернета в ФСБ, 2017. URL:https://www.rbc.ru/technology_and_media/31/07/2017/597b46f99a7947c6ad71eda3 (дата обращения: 3.12.2017).

RosBusmessConsulting. Digital clan: how is the IT business of the children of the Internet curator in the FSB, 2017. Available at: https: //www.rbc.ru/technology_and_media/31/07/2017/597b46f99a7947c6ad71eda3 (accessed: 3/12/2017). (in Russian)

9. Церцеил Ю.С., Коокуева В.В., Грызунова Н.В. 2017. Инструменты кластерной политики в развитии инновационной экономики России (на примере отдельных особых экономических зон). ИТ-портал, 1 (13): 4.

10. Zertseil Yu.S., Kookueva V.V., Gryzunova N.V. 2017. Cluster policy tools in the development of the mnovative economy of russia (on the example of separate special economic zones). IT-portal, 1 (13): 4. (in Russian)