

УДК 339.9:621.39

Одаренко О.В.*старший преподаватель кафедры украинской литературы,
компаративистики и социальных коммуникаций
Киевского университета имени Бориса Гринченко*

СОВРЕМЕННЫЕ АСПЕКТЫ УПРАВЛЕНИЯ ФРОД-РИСКАМИ ТЕЛЕКОММУНИКАЦИОННЫХ КОМПАНИЙ

Статья посвящена анализу современных аспектов управления фрод-рисками телекоммуникационных компаний. Отмечен глобальный характер фрода. Указано на постоянный рост убытков телекоммуникационных компаний от фрода. Отмечен недостаточный уровень изученности экономических последствий фрода в украинском научном контексте. Указано на отсутствие научного внимания к фроду как важной части риск-менеджмента телекоммуникационных компаний. Отмечено усложнение фрод-рисков в телекоммуникациях. Указано на новейшие тенденции антифрода как части риск-менеджмента телекоммуникационных компаний.

Ключевые слова: риск, риск-менеджмент, компании рынка телекоммуникаций, фрод-риск, мошенничество, фрод-менеджмент.

Одаренко О.В. СУЧАСНІ АСПЕКТИ УПРАВЛІННЯ ФРОД-РИЗИКАМИ ТЕЛЕКОМУНІКАЦІЙНИХ КОМПАНІЙ

Статтю присвячено аналізу сучасних аспектів управління фрод-ризиками телекомунікаційних компаній. Наголошено на глобальному характері фроду. Відзначено постійне зростання збитків телекомунікаційних компаній від фроду. Зазначено недостатній рівень дослідженості економічних наслідків фроду в українському науковому контексті. Відзначено відсутність наукової уваги до фрод-менеджменту як важливої частини ризик-менеджменту телекомунікаційних компаній. Зазначено ускладнення фрод-ризиків у телекомунікаціях. Наголошено на новітніх тенденціях антифроду як частини ризик-менеджменту телекомунікаційних компаній.

Ключові слова: ризик, ризик-менеджмент, компанії ринку телекомунікацій, фрод-ризиками, шахрайство, фрод-менеджмент.

Odarenko O.V. MODERN ASPECTS OF MANAGEMENT OF FRAUD-RISKS OF THE TELECOMMUNICATION COMPANIES

Article is devoted to the analysis of modern aspects of management of fraud-risks of the telecommunication companies. Global character of a fraud is noted. It is specified continuous growth of losses of the telecommunication companies from a fraud. Insufficient level of study of economic consequences of a fraud in the Ukrainian scientific context is noted. It is specified absence of scientific attention to a fraud as important part of a risk management of the telecommunication companies. Complication of fraud-risks in telecommunications is noted. It is specified the newest tendencies of an antifraud as parts of a risk management of the telecommunication companies.

Keywords: risk, risk management, companies of the market of telecommunications, fraud-risk, fraud, fraud-management.

Постановка проблемы. Одним из наиболее существенных риск-факторов для телекоммуникационных компаний является фрод. Единого определения фрода не существует. Вот одно из них: «FRAUD – ФРОД – несанкционированный доступ к услугам связи, а также получение услуг в режиме неправомерного доступа» [1]. В данном исследовании нам интересно определение фрода в контексте современных бизнес-реалий: «Фродом можно назвать умышленные действия или бездействие физических и/или юридических лиц с целью получить выгоду за счет компании и/или причинить ей материальный и/или нематериальный ущерб» [2]. «Фрод в сети связи – вид фрода, связанный с умышленной деятельностью лиц в сетях связи (в том числе мошеннической), по неправомерному получению услуг и использованию ресурсов оператора связи без надлежащей их оплаты, а также по неправомерному доступу к любой конфиденциальной информации оператора (в том числе с целью извлечения дохода), а также иные действия, направленные на причинение убытков и иного вреда оператору» [2].

Существуют классификации фрода по функциональным областям. Это – VoIP-фрод, SMS-фрод, PRS-фрод. А также, роуминговый фрод, транзитный фрод. Также выделяют внутренний фрод, subscription-фрод [3]. Новейшие технологии и глобализация обуславливают рост и генерализацию новых видов корпоративного мошенничества. В настоящее время, согласно Международной ассоциации сотовой телефонии, известно 200 разновидностей фрода. Потери от фрода с каждым годом растут. Если в 1997 г., по данным Международной ассоциации сотовой телефонии (CTIA – Cellular Telecommunications Industry Association), они составляли около \$1 млрд, то уже в

2000 г. – более \$12 млрд. В 2011 г. этот показатель составлял \$40,1 млрд, а в 2013 г. – \$46,3 млрд [4]. Некоторые эксперты называют цифру до \$52 млрд в год. В структуре убытков телекоммуникационных компаний потери от фрода составляют львиную долю. В среднем – от 3% до 7% дохода от реализации услуг связи.

Анализ последних исследований и публикаций. Однако ввиду сложности технологических аспектов деятельности телекоммуникационных компаний, научных публикаций о фрод-рисках не так уж много. Более того, зачастую в этих публикациях фигурирует термин «мошенничество», что не дает возможности составить целостное представление о специфике фрода и его экономических последствиях для телекоммуникационных компаний.

Некоторая часть публикации дает общее представление о фроде и его видах, а также технических и технологических особенностях фрод-действий. В последние годы активизировалось обсуждение фрода и антифродовых стратегий на уровне экспертов. Примером тому – цикл конференций, посвященных противодействию мошенничеству в банках и компаниях реального сектора экономики, в том числе и телекоммуникационных (например, конференция «Современные методы и инструменты противодействия мошенничеству», март 2014 г., Москва).

Большое внимание проблеме фрода в телекоммуникациях уделяет Международный союз электросвязи (ITU). Существенным является упоминание о фроде в различных стандартах и рекомендациях в области электросвязи, например, в стандарте GSM.

В основном же о фроде говорят в контексте киберпреступности или же усовершенствования корпоративного управления. В этой связи стоит

отметить аналитические исследования компании PriceWaterhouseCoopers (например, исследование The Global Economic Crime Survey); ежегодные отчеты Communications Fraud Control Association (CFCA) (2013 Global Fraud Loss Survey доступен по адресу: http://www.cvidya.com/media/62059/global-fraud_loss_survey2013.pdf).

В финансово-банковской сфере фрод определяется Соглашением Basel II Базельским комитетом по банковскому надзору.

Отметим также такие исследования, касающиеся проблемы корпоративного фрода, как Всероссийское исследование «Практика противодействия корпоративному мошенничеству» (доступно по адресу: http://www.vegaslex.ru/analytics/analytical_reviews/71450/), в котором сделан акцент на новых методах и законодательных инициативах в области противодействия корпоративному мошенничеству.

Публикаций украинских исследователей, посвященных проблеме фрода – незначительное количество. Как правило, они посвящены проблеме фрод-рисков в финансово-банковской сфере. Например, научная статья Болгар Т.М. «Удосконалення моніторингу банківського кредитного процесу», доступная по адресу <http://duep.edu/uploads/vidavnistvo14/akademichnij-ogljad-2-13/6292.pdf>. Часто термин «фрод» используется журналистами в контексте описания мошеннических действий на сетях телекоммуникационных компаний.

Выделение не решенных ранее частей общей проблемы. Изучение научных публикаций и аналитических материалов свидетельствует о том, что в украинском научном контексте мало внимания уделяется проблеме фрода, как в финансово-банковской сфере, так и в компаниях рынка телекоммуникаций. Не изучаются экономические последствия фрода, в частности, его новых видов, для телекоммуникационных компаний. Фрод практически не анализируется в контексте новых видов киберпреступлений. Не изучаются современные методы противодействия фроду в телекоммуникациях. Фрод не рассматривается как важная часть корпоративного риск-менеджмента телекоммуникационных компаний. Нет научных публикаций, посвященных фрод-менеджменту как составляющей корпоративного риск-менеджмента компаний рынка телекоммуникаций.

Формулирование целей статьи (постановка задачи). Ввиду этого объектом данного исследования являются фрод-риски телекоммуникационных компаний. Предметом – современные аспекты управления фрод-рисками телекоммуникационных компаний. Целью работы, реализованной на основании аналитических методов с привлечением статистического аппарата, является изучение фрод-менеджмента как важной составляющей риск-менеджмента телекоммуникационных компаний.

Изложение основного материала исследования. Усиление фрод-рисков в телекоммуникациях произошло на фоне новых технологических и потребительских стратегий компаний 2010–2015 гг. Влияние новых видов фрода как следствия новых технологий и услуг ощутили ведущие телекоммуникационные компании мира. Фрод в телекоммуникационной сфере ныне рассматривается как с позиций технологических угроз бизнесу компаний, так и с позиций ущерба для клиентов. Последний аспект особенно важен в контексте развития технологий «облачных вычислений» (cloud computing) и «интернета вещей». Эксперты отмечают, что именно потребители, а не инфраструктура телекоммуникационных

компаний являются ныне объектом действий фрод-мошенников.

Анализ последних тенденций в сфере антифрода позволяет говорить о ряде приоритетных направлений в процессе минимизации фрод-рисков, в частности для телекоммуникационных компаний. Фрод перестает рассматриваться в отрыве от иных рисков компаний, что коррелирует с последними тенденциями в риск-менеджменте, направленными на учет синергического влияния двух и более рисков. Происходит стратификация фрод-деятельности. В настоящее время выделяют персональные и корпоративные фрод-риски (см, например, практикум «Антифрод в интересах топ-менеджеров. Управление персональными и корпоративными фрод-рисками», Москва, 2015 г.).

Речь идет не просто о локализации фрод-рисков и их последствий, а о формировании полноценного фрод-менеджмента (по аналогии с репутационным менеджментом). На наш взгляд, фрод-менеджмент должен стать неотъемлемым элементом системы корпоративного риск-менеджмента телекоммуникационных компаний.

К базовым принципам построения защиты от фрода добавляется еще целый ряд существенных моментов. «Существует пять основных принципов построения эффективной системы защиты от фрода: Фрод в сети связи – вид фрода, связанный с умышленной деятельностью лиц в сетях связи (в том числе мошеннической), по неправомерному получению услуг и использованию ресурсов оператора связи без надлежащей их оплаты, а также по неправомерному доступу к любой конфиденциальной информации оператора (в том числе с целью извлечения дохода), а также иные действия, направленные на причинение убытков и иного вреда оператору. Принцип 1. В системе управления организацией должна быть разработана программа управления уровнем мошенничества, включающая в себя специальную политику (документ), отражающую требования совета директоров и высших топ-менеджеров в части снижения уровня фрода. Принцип 2. В каждой компании риск фрода должен периодически проверяться (оцениваться) для идентификации специальных потенциальных схем и событий с целью его снижения до приемлемого уровня. Принцип 3. Технические приемы предотвращения (снижения) риска мошенничества должны быть внедрены, где это возможно. Принцип 4. Технические приемы выявления риска мошенничества должны быть внедрены для нахождения новых схем (методик) фрода, когда превентивные меры не оправдывают себя или когда выявлен риск мошенничества, уровень которого нельзя снизить. Принцип 5. Процесс подготовки периодических отчетов должен быть включен в карту бизнес-процессов организации для оценки уровня существующего фрода. Отчетность помогает координировать методы расследования и корректирующие действия с целью снижения уровня риска фрода должным образом в соответствующее время» [2].

Анализ публикаций, посвященных фроду, позволил выделить актуальные тенденции в борьбе с этим видом мошенничества в сфере телекоммуникаций. Эти тенденции таковы:

- Оценка фрода как актуального тренда киберпреступности. Получило распространение понятие «конвергентное мошенничество» («конвергентный фрод»), описывающее мошеннические действия на конвергентных сетях.
- Организация фрод-менеджмента как составляющей части корпоративного риск-менеджмента.

В частности, в этом контексте большое внимание уделяется минимизации репутационного ущерба от фрода. Антифродовые стратегии рассматриваются в контексте бизнес-процессов компании. Анализируется проблема типологизации фродовых схем, ввиду отсутствия единой системы классификации фрода. Ряд экспертов, в частности Д. Шопин [3], усматривают в этом важнейшую составляющую фрод-менеджмента. Д. Шопин предлагает типологизацию фродовых схем, основываясь на методе их выявления, детектирования. Такая типологизация коррелирует с современной типологизацией киберпреступлений.

- Также важна оптимизация стоимости антифродовых мероприятий. Стоимость внедрения комплексной системы FMS колеблется от \$500 тыс. до \$2, 5 млн. Очевидно, что вопрос стоимости таких систем интересует небольшие телекоммуникационные компании. Также прогнозируется удорожание сетей в связи с необходимостью противостоять новым видам фрода.

- Введение должности фрод-офицера в корпоративной системе управления/структуре управления рисками компании.

- Усиление правой ответственности за фрод-деятельность.

- Унификация статистики от фрод-потерь. В настоящее время отсутствует единая статистическая база в этой области, как на глобальном, так и локальном уровнях телекоммуникационного рынка.

- Появление на рынке программ страхования фрод-рисков, в частности, рисков телекоммуникационных компаний.

- Понимание специфичности фрод-рисков для каждой телекоммуникационной компании и, одновременно, вычленение актуальных фрод-трендов.

- Дальнейшее совершенствование автоматизированных процессов борьбы с фродом. Как правило, данное направление широко не освещается, ввиду специфики деятельности каждой из телекоммуникационных компаний.

- Развитие антифродовых стратегий в контексте аналитики «Больших данных». Аналитика в настоящее время постулируется как необходимый инструмент противодействия фроду. Эксперты отмечают недостаточность консервативных методов противо-

действия фроду в условиях все большего усложнения киберпреступных схем (конференция «Современные методы и инструменты противодействия мошенничеству», март 2014 г., Москва).

Фрод-менеджмент включает как технологический, так и организационный аспект. Практики риск-менеджмента подчеркивают необходимость включения фрод-менеджмента в общую систему риск-менеджмента компаний.

Выводы из проведенного исследования и перспективы дальнейших исследований в данном направлении. Из вышесказанного можно сделать следующие выводы. Фрод является одной из существенных угроз для бизнеса телекоммуникационных компаний. Усложнение бизнес-моделей телекомов, развитие IT-технологий, внедрение новых практик взаимодействия с клиентами обуславливают появление так называемого «конвергентного» фрода, отвечающего реалиям конвергентных бизнес-моделей в телекоммуникациях. Разработка и внедрение фрод-менеджмента как составной части риск-менеджмента способны минимизировать влияние фрод-рисков на бизнес телекоммуникационных компаний. Перспективным является исследование синергий фрод-рисков и иных видов рисков, специфики новых видов фрод-рисков в контексте противодействия киберугрозам для бизнеса телекоммуникационных компаний.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. Термины [Электронный ресурс]. – Режим доступа : <http://like-android.ru/termins.php?p=2>, свободный. – Назв. с экрана (дата обращения 22.05.2015).
2. Костров Д. Фрод – реальность современного бизнеса [Электронный ресурс]. – Режим доступа : <http://www.itsec.ru/articles2/focus/frod-realnost-sovremennogo-biznesa>, свободный. – Назв. с экрана (дата обращения 22.05.2015).
3. Шопин Д. Прагматическая классификация телекоммуникационного фрода [Электронный ресурс]. – Режим доступа : <http://www.jetinfo.ru/author/dmitrij-shopin/?nid=2fecbd56d93e9a0794c562d990cd36b6>, свободный. – Назв. с экрана (дата обращения 22.05.2015).
4. 2013 Global Fraud Loss Surve [Электронный ресурс]. – Режим доступа : http://www.cvidya.com/media/62059/global-fraud_loss_survey2013.pdf, свободный. – Назв. с экрана (дата обращения 22.05.2015).