

Федеральное государственное образовательное бюджетное учреждение высшего профессионального образования

**Финансовый университет при Правительстве Российской Федерации
(Финансовый университет)**

Кафедра «Анализ рисков и экономическая безопасность»

**Доклад на тему:
«Противодействие корпоративному мошенничеству в условиях цифровой экономики»**

Выполнила:

аспирантка первого года
Абдулхакова К.Р.

Научный руководитель:
д.э.н., профессор Земсков В.В.

Москва -2017

Противодействие корпоративному мошенничеству в условиях цифровой экономики

Современный период развития общества – это эпоха постиндустриальной цифровой экономики, которая кардинально меняет ситуацию в мире, ставя на одно из первых мест проблемы, связанные с развитием информационной сферы, средств массовой информации и коммуникаций, использованием современных информационных систем для развития экономики и стабилизации общественного развития в целом [1]. При этом под цифровой экономикой нами понимается «тип хозяйствования, характеризующегося преобладающей ролью данных и методов управления ими как определяющего ресурса в сфере производства, распределения, обмена и потребления» [2].

Развитие цифровой экономики набирает обороты как в России, так и в других странах мира. Лидерами по развитию цифровой экономики является США, в которой доля цифровой экономики в ВВП страны составляет 10,9%, далее следует Китай (10,% в ВВП страны), Европейский Союз (таблица 1). В России доля цифровой экономики составляет в настоящее время 3,9% от ВВП, а в рамках программы «Развитие цифровой экономики в России до 2035» планируется ее увеличение до 8-10% ВВП [3].

Таблица 1 – Вклад цифровой экономики в ВВП некоторых стран в 2015 году, % к ВВП [3]

Наименование	США	Китай	5 стран Западной Европы	Индия	Бразилия	Чехия	Россия
Расходы домохозяйств в цифровой сфере	5,3	4,8	3,7	3,2	2,7	2,2	2,6
Инвестиции компаний в цифровизацию	5,0	1,8	3,9	2,7	3,6	2,0	2,2
Государственные расходы на цифровизацию	1,3	0,4	1,0	0,6	0,8	0,5	0,5
Экспорт ИКТ	1,4	5,8	2,5	5,9	0,1	2,9	0,5

Импорт ИКТ	-2,1	-2,7	-2,9	-6,1	-1,0	-2,1	-1,8
Общая доля цифровой экономики в ВВП	10,9	10,0	8,2	6,3	6,2	5,5	3,9

Развитие цифровой экономики привело к увеличению числа и расширению сферы определенных видов преступлений и мошенничества, в том числе корпоративного мошенничества.

Основными видами корпоративного мошенничества в данной сфере являются:

- несанкционированный доступ к корпоративным данным с целью копирования, изменения, стирания, подавления компьютерных данных, хищения информации, составляющей коммерческую тайну, кибервымогательства;
- вмешательство в работу компьютерных корпоративных систем с намерением помешать ее функционированию;
- использование компьютерных систем для обмена, хранения и распространения информации конфиденциального характера;
- компьютерные мошенничества, связанные с хищением денежных средств из банкоматов, с расчетных счетов кредитных организаций и предприятий и другие [5].

По видам совершаемых деяний основными видами компьютерных преступлений в России в последние годы являются:

- 1) кибершантаж (например, вредоносные программы типа Crypto Locker, попав в компьютер, шифруют все типы документов, которые могут представлять ценность для пользователя (электронные таблицы, документы, базы данных, фотографии и пр.), после чего жертву начинают шантажировать, требуя заплатить выкуп за возможность восстановления файлов);
- 2) направленные кибератаки на информационные ресурсы компаний, организаций, учреждений и т.д.;

3) кибератаки на платежные терминалы для кражи данных банковских карт клиентов;

4) АРТ-атаки (Advanced Persistent Threats) - так называемые «постоянные угрозы повышенной сложности», представляющие собой вид направленных атак, которые нацелены на крупные компании или стратегически важные институты.

5) Взлом подключенных к Интернету устройств («Интернет-вещей»). Данные устройства, начиная от IP-камер и заканчивая принтерами, являясь частью Интернета, обладают программным обеспечением, которое делает их весьма уязвимыми для взлома киберпреступниками и причинения ущерба пользователю.

6) Атаки на смартфоны, а также иные мобильные устройства для кражи паролей и данных пользователей [6].

Основные преступные деяния, образующие компьютерную преступность в Российской Федерации в 2015 году, приведены на рис.1.



Рисунок 1 - Виды преступных деяний в сфере компьютерных технологий в Российской Федерации в 2015 году, % от общей компьютерной преступности [6].

Таким образом, наибольший удельный вес среди совершенных компьютерных преступлений приходится на преступления в сфере компьютерной информации (ст.ст. 272, 273 УК РФ) и мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ), которые в данное время и составляют основу компьютерной преступности в России [4; 6].

Самыми распространенными видами корпоративного мошенничества являются коммерческий подкуп (откат), различные формы хищения активов, а также использование имущества компании в личных целях. При этом в большей степени корпоративному мошенничеству подвержены такие бизнес-процессы как инвестиционные проекты, капитальное строительство, закупочная деятельность, финансовые операции.

Экономические преступления в киберпространстве приводит к дополнительным потерям компаний, которые ранее были неизвестны для традиционной экономики, наносят ущерб бренду компании, замедляют темпы развития бизнеса, ухудшают психологический климат в компании, ведут к потере доверия в коллективе. При этом в большинстве случаев устранение проблем от корпоративного мошенничества требует значительно больше средств, чем их предотвращение.

Чтобы снизить потери от корпоративного мошенничества в условиях цифровой экономики важным вопросом становится разработка и реализация комплекса мер, направленных на предупреждение подобных преступлений. Можно выделить три группы мер, направленных на предупреждение корпоративного мошенничества в условиях цифровой экономики:

1) Нормативные меры – включают совершенствование законодательства в сфере цифровой экономики. На уровне компаний к данной группе мер можно

отнести систематическую экспертизу внутренних нормативно-распорядительных документов компании на предмет устранения факторов, способных нанести вред компании (к числу таких факторов могут быть отнесены чрезмерные полномочия отдельных работников в доступности той или иной информации), разработка и периодический пересмотр положения о коммерческой тайне в компании.

2) Технические меры – включают защиту корпоративных информационных систем от несанкционированного доступа, установку резервных систем электропитания, ограничение доступа к отчетности, электронным цифровым подписям.

3) Организационные меры – включают тщательный подбор персонала, внедрение кодекса корпоративной этики, повышение квалификации персонала в сфере информационных технологий, создание специальных структур по обеспечению информационной и экономической безопасности компании, структур управления потоками информации, в том числе коммерческой тайной [7].

Чтобы выживать и развиваться в новых условиях, компаниям следует также динамично наращивать свою компетентность в области цифровых информационных технологий, чтобы минимизировать проявление корпоративного мошенничества в данной сфере.

Таким образом, переход к инструментам цифровой экономики требует от предприятий существенных организационных преобразований, в том числе построение такой организационно-правовой структуры, которая бы противодействовала корпоративному мошенничеству и способствовала развитию в новых условиях функционирования.

При этом поскольку угроза корпоративного мошенничества вызвана не только внутренними факторами компании, и в первую очередь, персоналом, но и исходит извне, т.е. от конкурентов, потенциальных контрагентов, клиентов, то при заключении сделок следует более тщательно подходить к выбору контрагентов, проверять партнеров по процедуре должной добросовестности *due diligence*.

Развитая система предупреждения корпоративного мошенничества в компании позволяет существенно повысить стоимость компании, свидетельствует о значительном развитии бизнес-процессов. Раскрытие информации о наличии систем предупреждения корпоративного мошенничества подтверждает, что качество продуктов компании гарантируется не только ее брендом, но и каждым связанным с ней лицом. В свою очередь, отсутствие механизмов управления рисками корпоративного мошенничества может стать весомым аргументом в пользу уменьшения стоимости компании в сделках М&А. Кроме того, наличие данных механизмов зачастую является условием привлечения инвестиций и выхода на ряд иностранных рынков.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1. Якушенко К.В., Шиманская А.В. Цифровая трансформация информационного обеспечения управления экономикой государств - членов ЕАЭС // Новости науки и технологий. 2017. №2 (41). С. 11-20.
2. Семячков К.А. Цифровая экономика и ее роль в управлении современными социально-экономическими отношениями // Современные технологии управления. 2017. №8 (80).
3. Харченко А.А., Конюхов В.Ю. Цифровая экономика как экономика будущего // Молодежный вестник ИрГТУ. 2017. № 3 (27). С. 17.
- 4 Иванцов С.В., Спасенников Б.А., Борисов С.В. Проблемы предупреждения преступлений в сфере цифровой экономики // Актуальные вопросы образования и науки. 2017. № 2 (60). С. 20-24.
- 5 Пономаренко Н.А. Компьютерная преступность в современном мире // Экономика и социум. 2016. №6 (25).
- 6 Евдокимов К.Н. Структура и состояние компьютерной преступности в Российской Федерации // Юридическая науки и правоохранительная практика. 2016. №1. С. 86-94.
- 7 Василенко Н.А. Преступления в сфере информационных технологий (киберпреступность) // Старт в науке. – 2016. – № 5. – С. 31-34; URL: <https://science->

start.ru/ru/article/view?id=428 (дата обращения: 28.11.2017).