



Теневая экономика в контексте угроз экономической безопасности государства

М. М. Бегичев

*Кандидат технических наук, доцент,
mmbegichev@gmail.com
Российский университет транспорта,
Москва, Россия*

А. В. Власов

*Кандидат экономических наук, доцент,
alessandro.vlasov@mail.ru
Российский университет транспорта,
Москва, Россия*

К. Ю. Автомонова

*Преподаватель,
ksu.avtomonova@yandex.ru
Российский университет транспорта,
Москва, Россия*

Аннотация: *Статья посвящена исследованию сущности и различных последствий теневой экономики. Наиболее существенным признаком теневой экономики является тот факт, что она оказывает существенное негативное влияние на экономику региона, страны и/или экономических союзов. Стоит отметить тот факт, что достаточно долго ведется достаточно успешная работа по борьбе с теневой экономикой, все равно угрозы, исходящие от нее, остаются достаточно высокие. По результатам исследования, авторы приходят к выводу о необходимости дальнейшего совершенствования работы государственных органов и предпринимательских структур, направленных на совместную работу по противодействию теневой экономики.*

Ключевые слова: *теневая экономика, экономические угрозы, риски, финансовая деятельность предприятий.*

Shadow economy in the context of threats to the economic security of the state

M. M. Begichev

*Cand. Sci. (Tech.), Assoc. Prof.,
mmbegichev@gmail.com
Russian University of Transport,
Moscow, Russia*

A. V. Vlasov

*Cand. Sci. (Econ.), Assoc. Prof.,
alessandro.vlasov@mail.ru
Russian University of Transport,
Moscow, Russia*

K. I. Avtomonova

Lecturer,

ksu.avtomonova@yandex.ru

*Russian University of Transport,
Moscow, Russia*

Abstract: *The article is devoted to the study of the essence and various consequences of the shadow economy. The most significant feature of the shadow economy is the fact that it has a significant negative impact on the economy of the region, country and/or economic unions.*

It is worth noting the fact that quite successful work has been carried out to combat the shadow economy for quite a long time, all the same, the threats emanating from it remain quite high. Based on the results of the study, the authors come to the conclusion that it is necessary to further improve the work of state bodies and business structures aimed at working together to counter the shadow economy.

Keywords: *shadow economy, economic threats, risks, financial activity of enterprises.*

Проблема теневой экономики в России, как и во всем мире, является весьма насущной. Она в 2022 году включает в себя все основные виды финансовой деятельности.

По каким основным причинам теневая экономика скрывается от государственной власти:

- институциональной;
- нормативной;
- монетарной.

Какие негативные последствия оказывает теневая финансовая деятельность на российское общество:

- деморализует все общественные отношения и связи;
- осложняется реальная оценка финансового состояния страны, а также прогнозирование дальнейшего развития экономического сектора;
- искажаются макроэкономические показатели;
- бюджет государства из-за теневой экономики ежегодно не получает миллиарды рублей.

Это обстоятельство негативно отражается не только на людях, которые работают бюджетной сфере, но и на всех гражданах. Например: подвергается опасности здоровье и жизнь людей, которые приобретают некачественные товары или услуги, процветает нездоровая конкуренция в предпринимательской среде.

Теневая финансовая область выдавливает легальный бизнес.

На сегодня нет какого-то четкого алгоритма оценки реальных объемов нелегального финансового сектора Российской Федерации, а также его влияния на самые важные макроэкономические параметры.

Имеющиеся современные методы по определению истинного масштаба теневого экономического сектора носят оценочный характер, они могут вычислить размер нелегальной экономики только по косвенным признакам.

Самая авторитетная организация по ведению российской статистики — Росстат производит расчеты показателей неформального сектора по следующим методам:

- при помощи оценок авторитетных финансовых экспертов РФ;
- балансовый способ;
- при помощи косвенной информации, которая просачивается в различные СМИ: интернет, телевидение и т. д.

Два основных способа оценки теневой экономики, по мнению Международного валютного фонда:

- косвенный;
- прямой.

К прямому способу относят метод расхождений в самой национальной системе статистики. Это опросы директоров фирм, репрезентативные опросы, нахождение производственной деятельности, подлежащей учету.

Косвенный метод оценки определения основан в какой-то мере на употреблении населением иностранной валюты. Косвенный способ чаще всего обретает макроэкономический характер.

Косвенный подход основан на следующих несоответствиях:

- денежных объемах и финансовых операциях;
- количества потребляемого электричества;
- фактического и официального количества рабочих рук;
- государственных доходов и расходов.

В 2018 году Международный валютный фонд опубликовал статистику по теневому сектору экономики в 160 странах мира. Самый высокий уровень теневого экономического сектора оказался у Боливии — 63%. Российская Федерация заняла 49-е место, так, у нас доля «скрытого» сектора экономики составила 40%. Россия согласно этого рейтинга оказалась между Казахстаном (48-е место) и Киргизией (50-е место).

Экономические эксперты 49-е место РФ связывают со следующими факторами:

- слабое государственное регулирование на рынке товаров и финансовых рынках;
- невысокий уровень национальных институтов;
- низкий уровень отчетности на всех предприятиях, особенно малого частного бизнеса;
- негибкость рынка труда;
- высокие налоги, особенно на труд;
- большие социальные взносы;
- много административных барьеров при ведении бизнеса. Особенно в этой ситуации страдает малый бизнес — лакмусовая бумажка для определения стабильности финансовой ситуации в любом государстве;
- коррупция различных проверяющих государственных органов;
- невысокое качество всех государственных услуг.

Мировыми экспертами было замечено, что объем теневого сектора растет при следующих факторах:

- в стране повышается уровень безработицы;
- понижается удовлетворенность граждан качеством государственных услуг;
- общественные институты начинают хуже работать;
- повышение налогов.

Основные подходы, предпринимаемые в 2022 году, которые позволят понизить объем теневого сектора России:

- формирование специальной службы связи с налогоплательщиками — она призвана обеспечивать помощь гражданам и мониторить реальное положение дел. Этот метод успешно применен в ряде стран ЕС;
- введение дополнительных штрафов для злостных неплательщиков налогов, которые были уличены повторно, — способ удачно опробован в Великобритании;
- обязательное применение регистров для наемных работников — в данном регистре должны вводиться следующие данные: название фирмы, чем она занимается, количество отработанного времени всех работников, их личная информация. Метод успешно опробован в Швеции;
- обязательное использование сертифицированных кассовых аппаратов для всех компаний, которые применяют в своей работе наличный расчет, — кассовые аппараты должны быть с «черным» ящиком, чтобы инспекционная государственная служба в любой момент времени могла их проверить. Способ удачно опробован в следующих государствах: Греция, Швеция, Канада;
- формирование национальных типовых показателей и систем стандартов для производственных областей, показывающие соотношение между выпуском продукции и затрат на ее изготовление — метод успешно применен в Австралии;
- публикация имен самых ярких неплательщиков. Способ удачно опробован в Великобритании;

· ужесточение требований к заявкам, которые дают право на налоговый вычет, — особенно в тех областях экономики, где имеется большой риск для ухода в теневой сектор. Этот метод успешно применен в таких странах, как Сингапур, Китай.

Среди задач, которые ставит перед собой Правительство России, намерение сделать любые административные процедуры, связанные с ведением бизнеса, особенно налоговые, более открытыми, и стоит отдельно подчеркнуть тот факт, что это удастся сделать и достаточно быстро. За последние несколько лет были внедрены различные программы поддержки предпринимателей как на федеральном, так и на региональном уровне.

Необходимо отметить, что теневой рынок, безусловно, подрывает информационную безопасность в России, на которую в последнее время стали обращать достаточно много внимания.

Информационная безопасность является одним из самых важных направлений для всех участников — как самого государства, так и предпринимательских структур. На поддержание ее на высоком уровне тратятся баснословные суммы, количество их с каждым годом только увеличивается. Например, в 2021 году в мире на безопасность информационных данных стали тратить на 6% больше, чем в 2020 году.

Более половины мировых топ-менеджеров заявили, что при планировании корпоративного бюджета они будут еще больше увеличивать суммы на информационную безопасность (ИБ). Эксперты утверждают, что эта тенденция сохранится ближайшие десять лет.

Повальное увлечение информационной безопасностью компаниями связано прежде всего с тем, что начиная с января 2020 года и по январь 2022 года количество кибер-атак на фирмы увеличилось в два раза. То же самое произошло на теневых рынках доступов.

Теневые рынки доступа в даркнете предлагают данные о многих компаниях. Злоумышленники специально взламывают корпоративные сети фирм и получают конфиденциальную информацию, которую потом продают. Количество предложений на даркнет-рынке начиная с 2020 года увеличилось в 2,5 раза.

Связано это обстоятельство прежде всего с тем, что для хакеров это стало очень прибыльным делом. Специалистами было проанализировано 15 самых популярных западных и русских хакерских форумов в даркнете.

В течение последних пяти лет рынок доступов развивался стремительными темпами. О его большом скачке в развитии говорит появление большого количества атак хакеров с применением специальных программ-вымогателей.

Если еще 10 лет назад было модно взламывать сети частных лиц, то сегодня под прицелом находится подавляющее большинство фирм, особенно крупных.

Количество объявлений на тему доступа в даркнете за последние 10 лет увеличилось в несколько раз, и эта тенденция сохраняется до сегодняшнего времени. Все чаще можно увидеть объявления о продаже приобретенных доступов к разным корпоративным сетям.

За весь 2020 год было зафиксировано 750 объявлений, связанных с продажей доступов. Если сравнить с 2019 годом, то количество подобных публикаций увеличилось в 8 раз! За первые три месяца 2021 года было выявлено 600 предложений. Выросло количество объявлений о поиске специалистов по взлому доступов. Набираются даже целые группы хакеров.

Эксперты связывают эту негативную тенденцию с расширением действующих команд злоумышленников и созданием ими новых партнерских программ шифровальщиков. Увеличился и интерес пользователей специфических форумов. Эти люди предлагают сотрудничество с хакерами, продают и покупают доступы. За весь 2021 год, если сравнить с 2020 годом, количество таких предложений увеличилось в 4 раза.

Стали известны интересные цифры продаж доступов: сегодня за каждые три месяца продаются и покупаются доступы на сумму 700 тысяч долларов США. Количество предложений на «сером» рынке неуклонно растет, а сумма оборота денежных средств увеличивается не так быстро. Этот факт говорит о том, что конечная цена одного доступа немного падает.

Например, снижается стоимость самых дешевых доступов. Эти доступы поступают в продажу обычно без привилегий. Чаще их продают начинающие хакеры, так как боятся развивать атаку дальше.

С каждым последующим годом модель поведения злоумышленников меняется. Начинающие хакеры объединяются с опытными профессионалами: новички обычно взламывают внешний периметр защиты компании, а профи — внутренний. Умудренные опытом специалисты обычно имеют все необходимые ресурсы для полного взлома доступа.

После этого могут наступить печальные для взломанной фирмы последствия:

- полная остановка всех бизнес-процессов компании;
- кража денежных средств со счетов корпорации.

Эксперты считают, что на многих фирмах устаревшая защита от кибератак. Ее нужно выстраивать таким образом, чтобы принимать во внимание все новые реалии сегодняшнего времени.

По данным Райффайзенбанка во время пандемии коронавируса очень сильно пострадал весь теневой сектор экономики. Главные ее последствия за 2021 год — начало 2022 года для теневой экономики:

- упал уровень заработной платы. Общий фонд зарплаты по итогам всего 2021 года снизился на 4,5%. Следует учесть, что официальные зарплаты не уменьшились в денежном отношении;
- «серый» сектор сбавил темпы роста. По оценкам специалистов того же Райффайзенбанка, теневая финансовая область Российской Федерации составляет 35% по фонду заработной платы и занятости.

В официальной области экономики России ситуация, наоборот, улучшилась:

- Фонд заработной платы за 2021 год увеличился на 10%, если сравнивать с 2020 годом;
- занятость в «белом» секторе выросла: с 33,1 миллионов до 33,7 миллионов человек.

Правительство Российской Федерации разработало и запустило облегченный налоговый режим для самозанятых физических лиц: 6% при расчетах с индивидуальными предпринимателями и юридическими лицами, 4% — с физическими лицами. Им стало гораздо выгодней выйти из «тени», чем не платить налоги.

Особое место в теневой экономике занимает «Гидра» — основной инструмент для наркоторговцев. «Гидра» — это известная в определенных кругах торговая площадка в даркнете. Она «снижала славу» тем, что стала самой крупной в мире онлайн-площадкой по продаже наркотических веществ.

Основная функция «Гидры» — посредничество между покупателями и продавцами. Кроме наркотиков тут можно приобрести поддельные документы: паспорта, водительские удостоверения, дипломы и т. д., а также заказать разные хакерские услуги: взломать чужой аккаунт, корпоративную сеть.

На «Гидре» сегодня официально зарегистрировано 2,6 миллиона аккаунтов. Причем при помощи 400 тысяч из них на этом ресурсе была сделана хотя бы одна покупка. Как отмечают эксперты, количество пользователей «Гидры» из года в год неуклонно увеличивается. Лидер по закладкам на 2022 год — город Москва. На втором месте — Санкт-Петербург. Самыми популярными наркотиками на сегодня являются мефедрон и альфа-ПВП. Аналитики говорят, что это обстоятельство связано с дешевизной его производства. Например, доля героина составляет всего 0,4% от общей массы наркотических веществ.

С какими проблемами сталкиваются в 2022 году органы государственной власти России (в большей части МВД России) по борьбе с «Гидрой».

Сотрудники МВД России сталкиваются с такими трудностями при борьбе с «Гидрой», как:

- незаконная трудовая миграция — особенно те, кто остался не востребован для легального сектора экономики. Приезжие граждане очень легко вовлекаются в бизнес по продаже и распространению наркотиков. В руках организаторов фактически имеется бесконечный возобновляемый кадровый резерв;
- новые технологии — каждый день преступники совершенствуются в своем деле, применяя новейшие информационные технологии. Та же «Гидра» успешно организует каналы «бесконтактного» сбыта наркотиков с помощью сети Интернет. В руках преступников имеются специализированные сервисы и программы, которые скрывают действительные IP-адреса. Активное использование новейших информационных технологий помогает вербовать молодежь, а также затрудняет сбор доказательств сотрудниками МВД.

Как государственные органы России стоят на защите информационной безопасности государства.

Информационная безопасность в Российской Федерации в 2022 году является одной из важнейших проблем. Россия занимает второе место в мире по количеству хакерских атак. На первом месте находится США. Страдают не только организации, но и простые люди: взламываются личные аккаунты, «угоняются» номера банковских карт. Информационная безопасность — это комплекс технических и организационных мер, которые делаются для управляемости, доступности, целостности и защиты информации.

Комплекс мер, предпринимаемых Правительством России в лице правоохранительных органов для информационной безопасности государства:

- создание информационно-психологического блока — это государственная система методов, направленная на препятствие негативного информационного влияния извне;
- применение специализированного набора программных и аппаратных средств помогает сохранять информационные данные от незаконного доступа, перепрограммирования и разрушения;
- национальная защита государственных систем жизнеобеспечения и государственных учреждений;
- дополнительная защита информации, содержащей коммерческую или государственную тайну.

На основании выше изложенных фактов, по мнению многих аналитиков, а также по нашему мнению, для дальнейшего укрепления информационной безопасности в Российской Федерации необходимо предпринимать следующие шаги:

- увеличивать эффективность органов местного самоуправления, других государственных органов, граждан и организаций при решении вопросов, которые так или иначе связаны с информационной безопасностью (далее ИБ);
- дальше продолжать улучшать технические, научные и информационно-аналитические аспекты функционирования системы ИБ;
- дорабатывать методы и формы взаимодействия сил обеспечения ИБ.

Каждый год в России следует повышать эффективность экономического, кадрового, информационно-аналитического, научно-технического, контрразведывательного, оперативно-разыскного, разведывательного, организационного, правового обеспечения сил информационной безопасности.

Безусловно, уже ведется достаточно большая работа по планированию и оценке эффективности комплекса действий, которые так или иначе связаны с обеспечением ИБ государства.

Государственным службам РФ, работающим в области по обеспечению информационной безопасности, необходимо каждый год выявлять наиболее важные направления киберугроз для уничтожения и предотвращения последствий их проявления.

Специалистами в сфере информационной безопасности РФ следует ежегодно прогнозировать и оценивать состояние информационной безопасности страны, а также разрабатывать оперативный план действий.

Государственным службам РФ, работающим в области по обеспечению ИБ, нужно более тщательно обеспечивать законные интересы и защиту прав организаций, граждан в информационной области.

Список литературы

1. Акимова И.П., Дмитриева О.А., Власов А.В. Корпоративная разведка: современный взгляд и тенденции развития. Путеводитель предпринимателя. 2020. Т. 13. № 3. С. 137–146.
2. Балабанова А.В. Интеграционные процессы как тренд глобального общественного развития. Ученые записки Российской Академии предпринимательства. 2019. Т. 18. № 4. С. 9–20.
3. Бегичев М.М., Потапов С.А., Власов А.В. Корпоративная разведка как инструмент конкурентной борьбы. Путеводитель предпринимателя. 2021. Т. 14. № 4. С. 136–141.
4. Ковтунова С.Ю., Губайдуллина И.Н. Теневая экономика в условиях глобализации как фактор экономической безопасности хозяйствующего субъекта. В сборнике: Экономическая безопасность: концепция, стандарты. 2016. С. 90–93.

5. Прохорова Л.М. Теневая экономика как основная угроза экономической безопасности государства. Актуальные вопросы современной экономики в глобальном мире. 2019. № 2. С. 34–37.
6. Официальный интернет ресурс АО «Райффайзенбанк» <https://www.raiffeisen.ru>.

References

1. Akimova I.P., Dmitrieva O.A., Vlasov A.V. Korporativnaya razvedka: sovremennyy vzglyad i tendencii razvitiya. Putevoditel' predprinimatel'ya. 2020. T. 13. № 3. S. 137–146.
2. Balabanova A.V. Integracionnye processy kak trend global'nogo obshchestvennogo razvitiya. Uchenye zapiski Rossijskoj Akademii predprinimatel'stva. 2019. T. 18. № 4. S. 9–20.
3. Begichev M.M., Potapov S.A., Vlasov A.V. Korporativnaya razvedka kak instrument konkurentnoj bor'by. Putevoditel' predprinimatel'ya. 2021. T. 14. № 4. S. 136–141.
4. Kovtunova S.YU., Gubajdullina I.N. Tenevaya ekonomika v usloviyah globalizacii kak faktor ekonomicheskoy bezopasnosti hozyajstvuyushchego sub»ekta. V sbornike: Ekonomicheskaya bezopasnost': koncepciya, standarty. 2016. S. 90–93.
5. Prohorova L.M. Tenevaya ekonomika kak osnovnaya ugroza ekonomicheskoy bezopasnosti gosudarstva. Aktual'nye voprosy sovremennoj ekonomiki v global'nom mire. 2019. № 2. S. 34–37.
6. Oficial'nyj internet resurs AO «Rajffajzenbank» <https://www.raiffeisen.ru>.