материалы I Респ. науч.-практ. форума, Барановичи, 30 сент. 2021 г. / Баранович. гос. ун-т. — Барановичи, 2021. — С. 25–35.

Bondar, A. V. Digital transformation of the education system as a factor in the development of human capital / A. V. Bondar, Yu. V. Guts // Theory and Practice of Social Sphere Management : proc. of I Rep. sci. and practical forum, Baranovichi, 30 Sept. 2021 / Baranovichi State Univ. — Baranovichi, 2021. — P. 25–35.

5. *Базылева, М. Н.* Цифровизация экономики и ее последствия для рынка труда / М. Н. Базылева // Цифровизация экономики и общества: проблемы, перспективы, безопасность : материалы III Междунар. науч.-практ. конф., Донецк, 25 марта 2021 г. / Донбас. юрид. акад. ; редкол.: С. И. Охременко [и др.] ; отв. ред. И. П. Подмаркова. — Донецк : Цифровая тип., 2021. — С. 156–162.

Bazyleva, M. N. Digitalization of the economy and its implications for the labor market / M. N. Bazyleva // Digitalization of the economy and society: problems, prospects, security : proc. of the III Intern. sci. and practical conf., Donetsk, 25 Mar. 2021 / Donbass Law Acad. ; ed. board: S. I. Ohremenko ; chief ed. I. P. Podmarkova. — Donetsk : Digital Print. House, 2021. — P. 156–162.

6. *Базылева, М. Н.* Информационная экономика и трансформация рынка труда / М. Н. Базылева // Экономический рост Республики Беларусь: глобализация, инновационность, устойчивость : материалы XIV Междунар. науч.-практ. конф., Минск, 20 мая 2021 г. / Белорус. гос. экон. ун-т ; редкол. : В. Ю. Шутилин (отв. ред.) [и др.]. — Минск, 2021. — С. 14–15.

Bazyleva, M. N. Information economy and transformation of the labor market / M. N. Bazyleva // Economic growth of the Republic of Belarus: globalization, innovation, sustainability : proc. of the XIV Intern. sci. and practical conf., Minsk, 20 May 2021 / Belarus State Econ. Univ. ; ed. board: V. Yu. Shutilin (chief ed.) [et al.]. — Minsk, 2021. — P. 14–15.

Статья поступила в редакцию 30.11.2021 г.

УДК 343.9

A. Beloborodko
Moscow Economical Institute (Moscow)

CYBER SECURITY AS ONE OF THE KEY FACTORS OF INTEGRATION OF THE EAEU STOCK MARKET

The article presents the experience of the international organization for the securities market IOSCO in combating cybercrimes in the financial markets of the EU countries; there is presented analysis of the results of a survey of representatives of the securities market, conducted in order to determine the scale of the threat posed by an organized cyberattack to the stock market. This article demonstrates the different types of cyber threats and the measures of regulations aimed to eliminate them. The author of the article demonstrates the dynamics of the growth of cybercrime in the financial markets of the EAEU countries and provides legislative regulations designed to combat it. A possible adaptation of the institutions developed by IOSCO on cybersecurity can be successfully implemented in the process of integrating the EAEU stock market.

Keywords: *cybersecurity; regulator; financial market; stock exchange; cyberspace; risk; depository; information technology; internet.*

А. М. Белобородько
кандидат экономических наук
Московский экономический институт (Москва)

КИБЕРБЕЗОПАСНОСТЬ КАК ОДИН ИЗ КЛЮЧЕВЫХ ФАКТОРОВ ИНТЕГРАЦИИ ФОНДОВОГО РЫНКА ЕАЭС

В статье представлен опыт международной организации по ценным бумагам IOSCO по пресечению киберпреступлений на финансовых рынках стран ЕС; анализируются результаты опроса

представителей биржевого сообщества, проведенного с целью определения масштаба угрозы, которую представляет организованная кибератака для фондового рынка. Представлена типология киберугроз и меры регуляторов, направленные на их отражение. Автор статьи демонстрирует динамику роста киберпреступности на финансовых рынках стран ЕАЭС и приводит законодательные постановления, призванные бороться с нею. Возможная адаптация институций, разработанных IOSCO по кибербезопасности, может быть успешно реализована в процессе интеграции фондового рынка ЕАЭС.

Ключевые слова: *кибербезопасность; регулятор; финансовый рынок; биржа; киберпространство; риск; депозитарий; информационные технологии; интернет.*

Надежность, развитие и эффективность интеграции рынков ценных бумаг зависят от достоверности, полноты и сохранности предоставляемой клиентам биржи информации, а также от качества предоставления услуг, институциональной эффективности регулирования процесса обмена прав собственности, высокой надежности поддерживающей технологической инфраструктуры. Киберпреступность является одним из наиболее серьезных технологических вызовов современности, поэтому кибербезопасности финансовых институтов в целом и фондовых рынков в частности посвящено значительное количество исследований как зарубежных, так и отечественных авторов [1, 2]. В условиях роста межнациональных противоречий и глобальной политической напряженности происходит трансформация рисков на фоне роста системного, санкционного и операционного рисков, обусловленных многими факторами, в том числе изменениями в информационных технологиях, рациональности деятельности участников биржевой торговли и биржевой институциональной среде [3]. Риски, связанные с кибератаками на фондовую биржу, кроме финансовых мошенничеств, несут в себе опасность краха и биржевой паники из-за падения котировок, взлома депозитария, поэтому тема кибербезопасности финансовых рынков представлена сейчас в значительном количестве зарубежных исследований и докладов [4].

Целью настоящей статьи является выявление основных операционных рисков, связанных с инфраструктурной и депозитарной структурой фондовых бирж государств — членов ЕАЭС, на основе систематизации и анализа источников и видов кибератак, а также разработка их профилактики. Для достижения этой цели определены основные направления трансформации рисков и их профилактики на основании мер, разработанных Международной организацией комиссий по ценным бумагам (далее — IOSCO) [4].

Под *киберпреступностью* в этой статье понимается любая противозаконная деятельность, предполагающая использование любого электронного устройства, подключенного к сети Интернет, от смартфона до спутника. *Киберпространство* определяется как сфера человеческой деятельности в информационном пространстве, представленном всей совокупностью коммуникационных каналов с соответствующей технологической инфраструктурой, обеспечивающей их функционирование. *Риск кибератак* означает вероятность наступления финансовых убытков или иных нежелательных последствий для участников биржевых торгов.

По оценке зарубежных и отечественных исследователей, большая часть (около 70 %) киберпреступлений во всем мире направлена против кредитно-финансовых организаций [5]. С каждым годом киберпреступность становится все более изощренной, что затрудняет борьбу с нею. Особенно тревожит появление относительно нового класса кибератак, именуемого «устойчивой повышенной угрозой» (Advanced Persistent Threat — APT). Киберпреступность наносит обществу значительные финансовые убытки — по данным некоторых исследований, от 388 млрд до триллиона долларов США [6].

Угроза киберпреступности для мировых бирж. Чтобы собрать уникальную информацию об угрозе киберпреступности в сфере финансовых рынков, в частности на рынке ценных бумаг, исследовательский отдел IOSCO совместно с Всемирной федерацией

бирж (далее — WFE) провел исследование воздействия киберпреступности (далее — WFE/IOSCO) на фондовые биржи. В этом опросе подавляющее большинство (89 %) респондентов согласилось с тем, что киберпреступность на рынках ценных бумаг может рассматриваться как прогнозируемый системный риск. Более половины биржевых респондентов сообщили о фактах кибератак [4], причем многие из них носили разрушительный характер, а не преследовали легкую наживу (это были атаки типа «отказ в обслуживании» и вредоносный код (вирусы)). Финансовые кражи не упоминались до 2013 г. ни в одном из ответов. Все это говорит о смене мотивов киберпреступлений на рынках ценных бумаг: от немедленной финансовой выгоды к более глобальным дестабилизирующим целям. Кибератаки оказывают разрушающее влияние на институциональную целостность и эффективность рынка, проникая в процесс проведения сделок [7, с. 131].

Уровень киберпреступности, по мнению биржевых агентов. 70 % опрошенных биржевых респондентов отметили, что они делятся информацией с представителями государственной власти, контролирующими организациями или регулирующими органами, однако большая часть этих договоренностей по обмену информацией носит внутренний характер и достаточно закрытый для широкой общественности формат; около 93 % респондентов сообщили, что киберугрозы обсуждаются на уровне исполнительных директоров, и почти 90 % опрошенных рассказали о наличии внутренних планов и документации по борьбе с киберпреступностью. Вместе с тем некоторые из опрошенных признают, что 100%-ная безопасность иллюзорна, около 25 % — что текущие превентивные меры и меры аварийного восстановления биржевых институций могут оказаться неспособными противостоять крупномасштабной и скоординированной кибератаке, около 22 % охваченных опросом биржевых агентов сообщили, что их фирмы имеют страховку от киберпреступлений [4].

Эффективность регулирования. Только 59 % опрошенных сообщили, что в их юрисдикции действуют режимы санкций за киберпреступность, причем только половина из них считает, что нынешние режимы санкций эффективны для сдерживания киберпреступности [4]. Регуляторами рынка ценных бумаг в борьбе с киберпреступностью на европейских рынках ценных бумаг были предприняты следующие действия: обновление/внедрение правил и стандартов (в сотрудничестве с другими органами); выявление и предоставление рекомендаций по применению имеющейся передовой практики; создание, участие и продвижение каналов обмена информацией; skills sharing, создание архива знаний для участников рынка ценных бумаг, чтобы быть в курсе тенденций, располагать техническими знаниями, отвечать на вопросы отрасли, собирать и регистрировать дела, выявлять самые большие риски.

Многие из опрошенных подчеркнули необходимость продолжения выбранной политики по профилактике киберпреступлений, но отметили, что нужно: сохранять гибкость для адаптации к изменяющимся рискам; концентрироваться на обмене информацией на основе действующих нормативных актов/законодательства; конкретизировать руководящие указания и принципы; не вмешиваться в индивидуальные внутренние операционные меры или политику учреждения [4].

Таксономия угроз безопасности рынка ценных бумаг ЕАЭС. При мониторинге размера киберугроз на фондовых рынках ЕАЭС целесообразно использовать следующие индикаторы, применяемые в Европе:

- количество целей атак на рынке ценных бумаг, сгруппированных по типу спецификации участников (например, хедж-фонд, биржа и т.д.);
- средняя частота атак на каждого участника рынка в год;
- процент критически важных услуг и конфиденциальной информации участников фондового рынка, содержащихся в сети;
- средние затраты (прямые и косвенные), понесенные участниками рынка ценных бумаг в связи с киберпреступностью.

Департамент исследований IOSCO Market Intelligence выявил глубокую обеспокоенность участников рынка этой угрозой. Так, по результатам опроса, проведенного PWC в 2011 г., киберпреступность была признана вторым по частоте регистрирования организациями финансового сектора видом экономических преступлений (на его долю в указанном году приходилось 38 % экономических преступлений); в опросе, проведенном Marsh and Chubb, 74 % респондентов из сферы финансовых услуг отнесли киберпреступность к категории высокого или очень высокого риска; в отчете Verizon за 2013 г. об утечках данных отмечалось, что более 1/3 всех нарушений, зарегистрированных в 2012 г., касались финансовых организаций [8].

Меры повышения кибербезопасности и киберустойчивости. Рост киберпреступности связан с динамичным расширением сети Интернет, электронной коммерции и социальных цифровых систем. Российское правительство пытается противодействовать киберпреступности с помощью законодательства и совместных инициатив, изложенных в программном меморандуме, однако данные меры малоэффективны в силу транснационального характера и таких технических особенностей киберпреступности, как отсутствие физических следов взлома, анонимность пользователей интернета, а также из-за нехватки квалифицированных сотрудников правоохранительных органов и практических методов расследования.

Киберпреступность сегодня является одним из ключевых операционных рисков для интеграции финансовых рынков стран ЕАЭС, например, на протяжении последних лет в Беларуси наблюдается устойчивый рост количества регистрируемых киберпреступлений.

За первые месяцы 2021 г. в Беларуси зафиксирован рост количества хищений с банковских карточек белорусов более чем на 270 % по сравнению с аналогичным периодом 2020 г. Имитация интернет-площадки KUFAR позволила мошенникам совершить в 2018 г. 51 преступление, в 2019 г. — 126, а в 2020 г. — 3879 краж [9]. В Казахстане в 2020 г. было зарегистрировано свыше 14 000 преступлений, связанных с интернет-мошенничеством; в январе 2021 г. их было уже почти 2000 [10].

С целью противодействия киберпреступности в 2015 г. в России был создан Департамент информационной безопасности Банка России (далее — ФинЦЕРТ). Сегодня ФинЦЕРТ объединяет 718 различных организаций, в том числе 517 банков. В 2018 г. для упрощения процесса обмена информацией, а также повышения эффективности и уровня безопасности сети была создана автоматизированная система обработки инцидентов (ASOI).

В России понятие «киберпреступление» на нормативном уровне отсутствует, вместо него в УК РФ употребляется термин «преступления в сфере компьютерной информации». Вместе с тем большинство отечественных авторов (например, В. А. Номоконов, Т. Л. Тропина) чаще всего в своих работах используют термин «киберпреступление», считая его более обширным, нежели «компьютерная преступность», и полнее описывающим такое явление, как преступность в информационном пространстве [11]. В гл. 28 Уголовного кодекса Российской Федерации к данной категории преступлений отнесены:

- неправомерный доступ к компьютерной информации (модификация, копирование или уничтожение информации с помощью компьютера) (ст. 272 УК);
- создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК);
- нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК).

Тем не менее статистический анализ подчеркивает высокий уровень криминализации цифровой сферы в Российской Федерации в последние 17 лет. Общее количество преступлений, совершенных с использованием компьютеризированных телекоммуникационных технологий, увеличилось с 1300 в 2001 г. до 174 674 в 2018 г. И динамика не меняется: в 2019 г. было совершено 97 524 таких преступлений, что на 53 % больше, чем в 2018 г. Большая их часть относится к мошенничеству (52 %), краже (19 %) и незакон-

ному обороту наркотиков (11 %) [12]. По мнению автора, основной мерой профилактики киберпреступлений является ежегодное ИТ-обучение персонала на бирже (не связанного с информационными технологиями).

Борьба с киберпреступностью в Российской Федерации. В соответствии с программой «Цифровая экономика Российской Федерации», которая была утверждена 28 июля 2017 г., основными проблемами, препятствующими развитию цифровой экономики, являются рост киберпреступности внутри страны и за рубежом, увеличение технических возможностей хакеров и отсутствие квалифицированных экспертов ИТЦ по безопасности. Программа предполагает, что и системные, и государственные операторы должны взять на себя ответственность за:

- повышение безопасности критически важной информационной инфраструктуры и стабильности ее функционирования;
- разработку механизмов обнаружения и предотвращения киберугроз и своевременное устранение их последствий;
- повышение защиты граждан и территорий от чрезвычайных ситуаций, вызванных взломом информационных систем;
- проведение профилактики преступности и своевременное противодействие любым подобным нарушениям (через Доктрину информационной безопасности Российской Федерации, 2016 г.).

В мае 2019 г. Президент Российской Федерации Владимир Путин подписал закон «О суверенном рунете», гарантирующий стабильную работу рунета в случае его отключения от мировой паутины [13]. Новая мера, которая вступила в силу 1 ноября 2019 г., потребовала от интернет-провайдеров установки оборудования для маршрутизации российского веб-трафика через отечественные серверы.

Международное сотрудничество в сфере кибербезопасности. Для России и, безусловно, для всех государств ЕАЭС международный подход к проблеме имеет преимущества и недостатки. Россия — единственная страна, участвующая в Совете Европы, которая не подписала Будапештскую конвенцию о киберпреступности (EST № 185, 2001). Главная причина заключалась в том, что в п. 32 Конвенции использовалась формулировка, допускающая трансграничный доступ к сохраненным компьютерным данным во время расследования киберпреступлений со стороны разведки других народов. В 2017 г. МИД России подготовил и предложил новые формулировки Конвенции Генеральной Ассамблее ООН о противодействии цифровой преступности. В декабре 2018 г. Ассамблея приняла две предложенные Россией резолюции по теме «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» [14]. Резолюции призваны защитить так называемые конфиденциальные данные государства, продвигая при этом глобальный консенсус и разработку конкретных и практических подходов к противодействию киберпреступности.

На другом, похожем треке, признавая трансграничный характер киберпреступлений, Госдума РФ ратифицировала соглашение о сотрудничестве государств Содружества Независимых Государств в сфере борьбы с преступлениями в области информационных технологий; документ был подписан главами государств СНГ 28 сентября 2018 г. в Душанбе [15]. В целях обеспечения эффективного предотвращения, выявления и расследования киберпреступлений основные формы взаимного сотрудничества в странах ЕАЭС теперь определяются как:

- обмен информацией о совершенных преступлениях и вовлеченных в них лицах;
- исполнение запросов о предоставлении информации для содействия раскрытию преступлений;
- планирование и проведение скоординированных специальных операций;
- содействие в обучении/повышении квалификации сотрудников правоохранительных органов [16].

Таким образом, в случае выявления киберугроз все центробанки стран — членов ЕАЭС будут уведомлять Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере.

Многообразие финансовых технологий и многочисленные связи с поставщиками услуг делают фондовый рынок менее прозрачным для регулирующих органов, что предоставляет больше возможностей для совершения киберпреступлений.

Одним из инструментов по предотвращению киберпреступлений может стать обязательная цифровая идентификация клиентов как реквизит цифрового бейджа для участия на биржевых торгах. По мнению экспертов, это позволит найти разумный компромисс между защитой конфиденциальности данных и соблюдением требований законодательства, что обеспечит эффективное функционирование механизма защиты прав инвесторов и потребителей биржевых услуг в странах ЕАЭС [17]. Эффективные решения могут потребовать сотрудничества между всеми заинтересованными сторонами, представленными как национальными торговыми площадками, так и регулирующими их государственными органами, в целях повышения иммунитета к кибератакам. Агенты фондовых рынков должны продолжать повышать свою информационную квалификацию по кибербезопасности по мере развития информационных технологий. Кибербезопасность должна стать неотъемлемой частью программы управления рисками саморегулируемых организаций. Учитывая международный характер киберрисков, существует потребность в обмене информацией на международном уровне. Опыт международных организаций, таких как IOSCO, в сфере кибербезопасности на финансовых рынках ЕС может быть успешно использован в процессе интеграции фондовых рынков стран ЕАЭС и транслироваться по информационным каналам между юрисдикциями всех его членов.

Источники

1. *Масалков, А. С.* Особенности киберпреступлений: инструменты нападения и защиты информации / А. С. Масалков. — М. : ДМК Пресс, 2018. — 226 с.

Masalkov, A. S. Features of cybercrime: attack tools and information protection / A. S. Masalkov. — Moscow : DMK Press, 2018. — 226 p.

2. *Шелупанов, А. А.* Форензика. Теория и практика расследования киберпреступлений / А. А. Шелупанов, А. Р. Смолина. — М. : Горячая линия — Телеком, 2020. — 104 с.

Shelupanov, A. A. Forensic. Theory and practice of cybercrime investigation / A. A. Shelupanov, A. R. Smolina. — Moscow : Hotline — Telecom, 2020. — 104 p.

3. *Иншаков, О. В.* Биржа. Эволюция экономического института / О. В. Иншаков, А. М. Белобородько, Д. П. Фролов. — М., 2008. — 356 с.

Inshakov, O. V. Exchange. Evolution of the economic institute / O. V. Inshakov, A. M. Beloborodko, D. P. Frolov. — Moscow, 2008. — 356 p.

4. Cyber Security in Securities Markets — An International Perspective Report on IOSCO's cyber risk coordination efforts [Electronic resource] // IOSCO. — Mode of access: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD528.pdf. — Date of access: 10.09.2021.

5. Число киберпреступлений в России выросло в 11 раз за пять лет [Электронный ресурс] // ТАСС. — Режим доступа: https://tass.ru/obschestvo/10616343. — Дата доступа: 05.10.2021.

6. McAfee: международные убытки от киберпреступности превысили триллион долларов [Электронный ресурс] // ItWeek. — Режим доступа: https://www.itweek.ru/security/news-company/detail.php?ID=216167. — Дата доступа: 11.10.2021.

7. *Graham, J.* Cyber Security Essentials / J. Graham, R. Olson, R. Howard. — New York : Auerbach Publ., 2010. — 342 p.

8. Cyber-crime, securities markets and systemic risk 16 July, 2013 [Electronic resource] // IOSCO. — Mode of access: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD460.pdf. — Date of access: 11.10.2021.

9. Киберпреступность в Беларуси [Электронный ресурс] // БелТА. — Режим доступа: https://www.belta.by/infographica/view/kiberprestupnost-v-belarusi-24963/. — Дата доступа: 11.08.2021.

10. Случаи совершения киберпреступлений участились в Казахстане [Электронный ресурс] // Forbes. — Режим доступа: https://forbes.kz/news/2021/02/15/newsid_243941. — Дата доступа: 04.11.2021.

11. *Номоконов, В. А.* Киберпреступность, как новая криминальная угроза / В. А. Номоконов, Т. Л. Тропина // Криминология. Вчера. Сегодня. Завтра. — 2012. — № 1(24). — С. 47.

Nomokonov, V. A. Cybercrime as a new criminal threat / V. A. Nomokonov, T. L. Tropina // Criminology. Yesterday. Today. Tomorrow. — 2012. — № 1(24). — P. 47.

12. Департамент информационной безопасности [Электронный ресурс] // Банк России. — Режим доступа: https://www.cbr.ru/about_br/bankstructute/dib/. — Дата доступа: 05.09.2021.

13. Путин подписал закон о «суверенном интернете». Он вступит в силу через полгода [Электронный ресурс] // Русская служба BBC News. — Режим доступа: https://www.bbc.com/russian/news-48126218. — Дата доступа: 17.10.2021.

14. Генассамблея ООН проголосовала за российский проект резолюции по глобальной кибербезопасности [Электронный ресурс] // Digital Russia. — Режим доступа: https://d-russia.ru/genassambleya-oon-progolosovala-za-rossijskij-proekt-rezolyutsii-po-globalnoj-kiberbezopasnosti.html. — Дата доступа: 15.11.2021.

15. Госдума ратифицировала соглашение о сотрудничестве стран СНГ в борьбе с киберпреступлениями [Электронный ресурс] // Дума ТВ. — Режим доступа: https://dumatv.ru/news/gosduma-ratifitsirovala-soglashenie-o-sotrudnichestve-stran-sng-v-borbe-kiberprestuplenii. — Дата доступа: 19.11.2021.

16. Отчет по результатам работы «Подготовка предложений Российской Федерации по приоритетным инициативам в рамках реализации цифровой повестки ЕАЭС и проекта «дорожной карты» по гармонизации законодательства государств-членов ЕАЭС в цифровой сфере» / Автономная некоммерческая организация «Центр исследований в сфере экономики и права» (АНО «ЦИСЭП»). — М., 2018. — 259 с.

17. Новости ЕАЭС. Цифровизация дала импульс к развитию финансовых инноваций в ЕАЭС [Электронный ресурс] // Альта Софт. — https://www.alta.ru/ts_news/83990/. — Дата доступа: 12.10.2021.

Статья поступила в редакцию 08.12.2021 г.

УДК 339.13.017(476)

S. Belova
A. Karmyzov
BSEU (Minsk)

CAUSES AND CONSEQUENCES OF THE VARIABILITY IN THE DEFINITION OF PRODUCT MARKET BOUNDARIES

The analysis of the competitive environment, as well as the analysis and assessment of competition in the commodity markets, is currently rearranging a great practical and scientific interest both for antimonopoly law enforcement and for developing a business strategy and formation of antimonopoly compliance of entities in a certain market. In the course of the analysis of individual markets, problems related to the definition of the boundaries of commodity markets, the market capacity and the shares of economic entities working on them arise. The authors hypothesize that the absence of unambiguously interpreted criteria and an algorithm for their use to determine the product boundaries of markets can lead to variability in their designation. They are illustrating this by the example of the crop protection chemicals markets. It is shown that different options for determining product boundaries of markets can be used by interested parties (business entities and the regulator) to determine the market share occupied by the organization and establish the presence or absence of a dominant position on it, taking into account their own interests and goals, which can lead to the emergence of a conflict of interest. It can be used by the regulator — to increase the effectiveness of the administration of markets and provide conditions for the development of competition in them; business entities — to develop measures to minimize the risks associated with violation of antimonopoly legislation.

Keywords: *market; commodity market; market research; market boundaries; product market boundaries; market composition; market structure; crop protection chemicals; antitrust regulation; dominant position.*