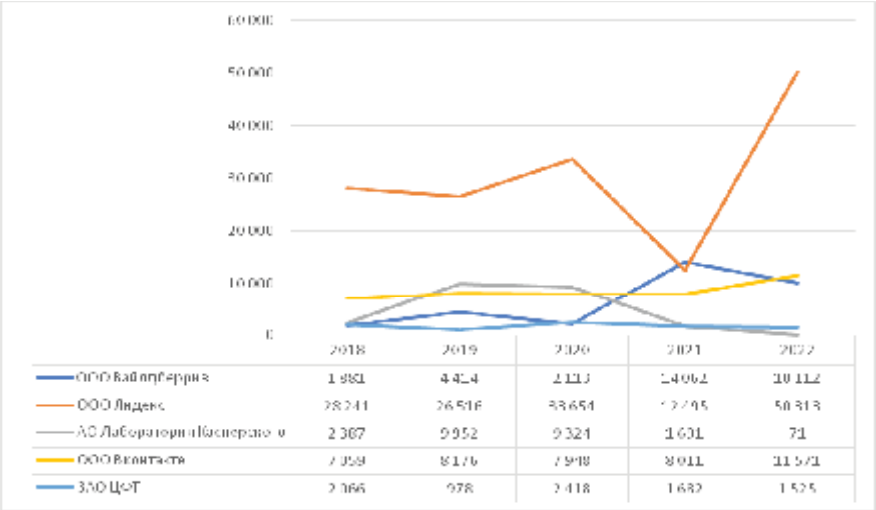

Рис. 2. Динамика показателя «Чистая прибыль» некоторых организаций, применяющих платформенную бизнес-модель (млн руб.)

Причин, объясняющих такое положение дел, может быть множество. В частности, на данные финансовые показатели оказывают влияние колебания рыночной конъюнктуры, политика компании, направленная на ускоренную модернизацию, которая несет дополнительные расходы, и др. Однако на диаграммах представлена информация по одним из крупнейших компаний. Специфической чертой цифровизации субъектов малого и среднего предпринимательства является отсутствие в ряде случаев четкой стратегии по перестройке бизнес-процессов, разногласия управляющего звена и руководителя организации, вызванное неготовностью менеджмента к внедрению инновационных методов ведения деятельности. Проведение цифровых преобразований в условиях внутрикорпоративных разногласий непосредственно участвующих в этом процессе сторон, может стать почвой для злоупотребления отдельным сотрудникам. Таким образом, возможен рост противоправных деяний, связанный с понятием присвоения и растраты, злоупотреблением полномочиями и т. д.

Отличительной чертой платформизации экономики в России является также преобладание в качестве ключевых игроков институтов финансового сектора. По данным Банка России, в 2022 г. объем сделок, произведенных в целом на финансовых платформах, превысил аналогичный показатель 2021 г. в семь раз, перейдя черту в 36 млрд руб. По состоянию на конец 2022 г. было установлено 54 финансовые организации и эмитента, которые присоединились к финансовым платформам. Общий их прирост за год составил 18 ед. Число пользователей финансовых услуг за 2022 г. выросло с 26 250 до 142 749 человек. В этом ключе также целесообразно отметить, что все большее распространение получает так называемый инструмент коллективного финансирования – краудфандинг. Его работоспособность во многом обусловлена функционированием инвестиционных платформ. По состоянию на декабрь 2023 г. в реестре действующих операторов цифровых платформ, по данным Банка России, насчитывается 76. За 2022 г. объем совершенных на рынке краудфандинга сделок составил 20,4 млрд руб., что на 48 % превышает объем денежных средств, которые были привлечены на соответствующих площадках в 2021 г. Наиболее активные пользователи – физические лица. Относительно них существует определенный набор рисков и угроз, поскольку под деятельностью инвестиционных платформ могут скрываться финансовые пирамиды, недобросовестные кредиторы и иное.

Для самих аналогичных интернет-площадок актуален риск наличия недобросовестных заемщиков. Так, на конец 2022 г. объем просроченной задолженности составил 828 млн руб., т. е. 9,9 % от общей суммы привлеченных клиентами денежных средств. Кроме того, Международная комиссия по ценным бумагам выделяет ряд рисков, в целом присущих инвестированию на цифровых платформах, – это вероятность технических сбоев и невыполнение платформой своих обязательств по этой причине, асимметрия информации, риск дефолта проекта.

Таким образом, в ситуации, когда цифровые преобразования в бизнес-среде стали неотъемлемым элементом современного пути ее развития, видится необходимым расстановка акцентов на констатации имеющихся и прогнозировании возможных негативных их последствий, способных нанести ущерб экономической безопасности корпоративным структурам, государству, как одним из объектов защиты со стороны правоохранительных органов. В этой связи требуется совершенствование методической базы выявления и раскрытия преступлений, совершаемых в киберпространстве; развитие нормативной правовой базы, учитывающее специфику сделок, совершаемых на платформах; законодательное закрепление норм, гарантирующих защиту интересов участников данных правоотношений.

УДК 004:34

С.В. Пилюшин

ИНФОРМАЦИОННОЕ ВОЗДЕЙСТВИЕ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ВЫЗОВЫ И ПЕРСПЕКТИВЫ

Внедрение информационных технологий во все сферы жизнедеятельности современного общества позволило сформировать к настоящему времени глобальную информационную среду, от которой напрямую зависит состояние политической, экономической, социальной и других составляющих информационной безопасности.

Появление облачных технологий, интернет вещей, блокчейн, искусственного интеллекта и машинного обучения, больших данных, виртуальной реальности привело к ряду изменений в обществе. Существенно возросли скорость передачи, объемы доступной информации, поспособствовавшие реализации процессов принятия решений. Стали более приемлемыми условия для глобализации – сложного и многогранного процесса межгосударственной интеграции в различных сферах. Широкое применение получили новые методы обучения, образовательные информационные ресурсы, позволившие пересмотреть традиционные способы получения знаний. Возникли новые направления деятельности в экономике: интернет-магазины; онлайн-сервисы; криптобиржи и др.

Таким образом, на фоне динамичных процессов актуальной стала разработка и внедрение эффективных методов и средств обеспечения конфиденциальности, целостности и доступности информации, защиты информационных систем, сетей, баз данных и других технологических ресурсов от постоянного воздействия негативных внутренних и внешних факторов.

В научной литературе существует достаточно широкий перечень определений и формулировок понятия информационной безопасности. Так, например, информационная безопасность рассматривается: как процесс обеспечения защиты информации от несанкционированного доступа, использования, распространения, модификации или уничтожения; как система мер по защите информации от угроз, включая кибератаки, вирусы, хакерские атаки и другие виды киберугроз; как область, занимающаяся защитой интеллектуальной собственности, сохранением данных и обеспечением надежности и достоверности научных исследований; как комплекс технологий, процедур и практик, направленных на защиту информации от угроз, включая физическую безопасность, защиту сетей, шифрование данных и управление доступом.

Представляется, что большинством исследователей информационная безопасность рассматривается как технологически сложное, многоуровневое явление, преимущественно состоящее из комплекса аппаратных и программных средств, применение которых направлено на обеспечение защиты информации и информационных систем от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации, несанкционированного копирования, блокирования информации, в том числе от случайных или преднамеренных воздействий на информацию и др.

Разработчики Концепции информационной безопасности Республики Беларусь под информационной безопасностью понимают состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере. В свою очередь, под информационной сферой понимается совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений.

Такой подход к определению информационной безопасности прежде всего рассматривает состояние защищенности национальных интересов – объективно значимых целей и задач национального государства как целого, формирующихся на стыке пересекающихся общих интересов личности, общества и государства. Видится, что этому определению не хватает конкретности, так как достаточно условным является возможность учета сбалансированных интересов в процессе обеспечения информационной безопасности при удовлетворении информационных потребностей отдельно взятых субъектов – личности и соответствующих государственных органов, ведомств.

Данное обстоятельство требует отдельного внимания с научной точки зрения, при рассмотрении вопросов, связанных с обеспечением надлежащих мер безопасности от информационных воздействий на конкретные объекты (например, сознание, психику, поведение людей).

Представляется, что в контексте информационного воздействия, обеспечение информационной безопасности должно рассматриваться как процесс принятия сбалансированных, адекватных мер защиты от потенциальных манипуляций и атак на информационные системы, и защиты от использования информационных ресурсов и других средств для достижения определенных целей, таких как манипуляция общественным мнением, дестабилизация внутренней обстановки, распространение дезинформации и т. д.

В связи с этим видится необходимость проведения более глубокой научной разработки проблемных вопросов, связанных с расширением теоретических представлений о взаимосвязи понятий информационной безопасности и информационных воздействий.

УДК 343.7

Е.Д. Прусенок

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ ПРЕФЕРЕНЦИАЛЬНОЙ ПОПРАВКИ ПРИ ПРОВЕДЕНИИ ГОСУДАРСТВЕННЫХ ЗАКУПОК В ОБЛАСТИ СТРОИТЕЛЬСТВА

Деятельность абсолютного большинства государственных органов, учреждений и предприятий представляется невозможной без наличия необходимых расходных материалов и иных товарно-материальных ценностей. При этом необходимость постоянного улучшения материально-технической базы государственных учреждений и предприятий находит свое отражение при планировании как бюджета государства в целом, так и годового плана закупок отдельного предприятия. В связи с указанным осуществление должного и беспрерывного контроля за расходованием бюджетных средств, обусловленным улучшением материально-технической базы указанных учреждений и предприятий, неоспоримо является ключевой деятельностью ряда правоохранительных органов.

На сегодня в Республике Беларусь действует ряд правовых актов, регламентирующих порядок проведения государственных закупок и закупок за счет собственных средств. Отметим, что ст. 4 Закона Республики Беларусь от 13 июля 2012 г.