УДК 338.27

Современные инструменты бизнес-аналитики и обеспечение экономической безопасности хозяйствующих субъектов

Швецов А.В.
Доктор экономических наук, профессор кафедры информационных систем в экономике Поволжского государственного технологического университета (Йошкар-Ола)

Короткова А.В.
Доктор экономических наук,
профессор кафедры бухгалтерского учета, налогов и экономической безопасности Поволжского государственного технологического университета (Йошкар-Ола)

Рыжаков Е.Д.
Доктор экономических наук,
профессор кафедры финансов, экономики и организации производства Поволжского государственного технологического университета(Йошкар-Ола)

Аналитические методы исследования широко используются в деятельности по обеспечению экономической безопасности хозяйствующих субъектов, поскольку позволяют формировать необходимую для управления информацию. Актуальность инструментов бизнес-аналитики с применением новых информационных технологий только растет, особенно для решения вопросов информационной безопасности.

В рамках поставленной в работе цели авторами представлена оценка состояния информационной безопасности в России, что связано с ростом количества преступлений в сфере информационно-коммуникационных технологий, а также методами защиты информации. Показано значение интегрированных решений, необходимых для развития систем бизнес-аналитики.

Ключевые слова: экономическая безопасность, информационная безопасность, бизнес-аналитика, преступность

Не вызывает сомнений важность обеспечения экономической безопасности хозяйствующих субъектов, из чего складывается экономическая безопасность государства в целом. Развитие цифровых технологий на современном этапе несет не только перспективы в виде ускорения бизнес-операций и получение дополнительной прибыли или хотя бы выполнение нулевой нормы рентабельности, но и серьезные угрозы. Данные угрозы связаны с рядом последствий. Понятно, что последствия для бизнеса будут отличаться в зависимости от масштаба. Очевидно, что в случае малого и даже среднего бизнеса последствия реализации угроз безопасности будут несравнимо меньше, чем для крупного.

Негативные последствия для бизнеса могут наступить в ряде случаев, связанных с некомпетентностью персонала, саботажем решений, отказом

техники, умышленным взломом систем и доступом к информации.

В последние годы количество преступлений в сфере высоких технологий неуклонно растет. Это связано в том числе с повышением общей компьютеризации большинства процессов жизнедеятельности и бизнеса. Противоправные действия совершаются как против цифровой инфраструктуры, так и с использованием цифровых средств доступа и каналов связи.

На рисунке 1 представлена диаграмма динамики совершенных правонарушений с применением средств информационно-коммуникационных технологий в период с 2018 по 2022 гг.

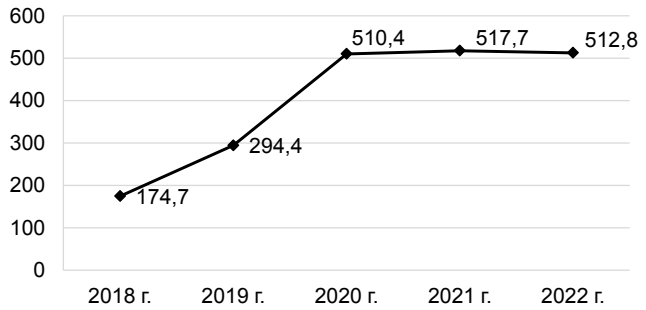

Рис. 1. Динамика совершенных правонарушений с применением средств информационно-коммуникационных технологий в РФ, тыс.

Следует также отметить удельный вес данных преступлений в общем объеме преступных деяний, который последние три года держится на уровне 25–26 %.

Между тем, уровень преступности в сфере экономики является одним из показателей состояния экономической безопасности, согласно Указа Президента Российской Федерации от 13.05.2017 г. № 208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года» [1].

Противодействие подобного рода преступным деяниям осуществляется не только со стороны правоохранительных органов. За технологической стороной проблемы следит Федеральная служба по техническому и экспортному контролю, в задачи которой входит в том числе мониторинг угроз и рисков информационной безопасности.

В общем смысле, под угрозой понимается потенциально возможное событие, действие (воздействие), процесс или явление, которые могут привести к нанесению ущерба чьим-либо интересам.

Согласно ГОСТ Р 50922-96, под угрозой информационной безопасности понимается совокупность условий и факторов, создающих опасность нарушения информационной безопасности. С точки зрения информационной безопасности некоторого информационного объекта можно выделить угрозы конфиденциальности, целостности и доступа.

По расположению источника угроз следует выделить внешние и внутренние. Так, например, согласно данным сборника «Состояние преступности в России за январь-ноябрь 2022 г.» [2], из 683495 случаев использования информационно-коммуникационных технологий при совершении преступлений, только 6973 (около 1 %) можно отнести к внутренним угрозам.

Угрозы можно классифицировать также по уровню наносимого ущерба – общие (значительный ущерб), локальные (причинение вреда отдельным частям объекта безопасности) и частные (причинение вреда отдельным свойствам элементов объекта безопасности). Согласно исследованиям, «в России в 2022 г. прогнозировались потери на уровне 165 млрд руб., однако обострение геополитической обстановки и ставший следствием шквал атак удвоили потери бизнеса и граждан» [3].

По природе возникновения угрозы информационной безопасности следует разделить на объективные и субъективные. Очевидно, что количество субъективных или искусственно вызванных угроз много больше, чем объективных. То же самое следует сказать и о рисках информационной безопасности и размере ущерба.

Важным является и то, что риски умышленных угроз в настоящее время намного превосходят непреднамеренные или случайные, что отражается в статистике преступлений в данной сфере.

Следует отметить, что в Российской Федерации действует методика оценки угроз безопасности информации, принятая Федеральной службой по техническому и экспортному контролю (ФСТЭК России) 05.02.2021 г. Кроме того, в соответствии с приказом ФСТЭК от 4 марта 2017 г. № 17 [4], использование банка данных угроз ФСТЭК является обязательным.

Для оценки угроз информационной безопасности ФСТЭК использует калькулятор, определяющий уровень угроз по трем группам метрик – базовым, временным и контекстным (рис. 2).

На основе численного значения базового вектора V уязвимости присваиваются один из четырех уровней опасности:

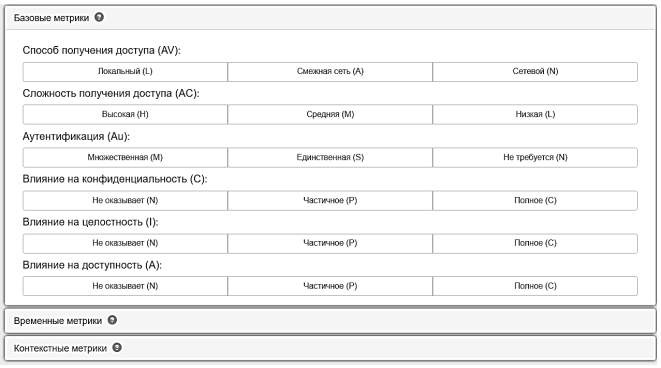

Рис. 2. Формы заполнения метрик в калькуляторе ФСТЭК РФ [5]

• низкий уровень опасности, если $0,0 \leq V \leq 3,9$;
• средний уровень опасности, если $4,0 \leq V \leq 6,9$;
• высокий уровень опасности, если $7,0 \leq V \leq 9,9$;
• критический уровень опасности, если $V = 10,0$.

В результате делается вывод об уровне уязвимости исследуемой системы, функционирующей в некотором бизнес-процессе. Итогом должно стать некоторое решение, повышающее уровень информационной и экономической безопасности.

Помимо использования техническими специалистами хозяйствующего субъекта данного калькулятора можно воспользоваться рядом других сервисов оценки уязвимости программного обеспечения, например, *ScanOval* или антивирусных программ.

Для повышения эффективности бизнеса необходимо не только защитить свои данные и технологические секреты от взлома или искажения, но и наладить аналитическую работу с накапливаемыми массивами производственной информации, внешними открытыми данными и прочим. С этой целью можно использовать множество разрозненных инструментов, позволяющих проводить кластерный, регрессионный, факторный анализы, использовать технологии *data mining* и даже нейронные сети. Однако средний и крупный бизнес страны на протяжении двух десятилетий все активнее начинает использовать системы бизнес-аналитики, а не отдельные инструменты.

Использование программ *Business Intelligence* (*BI*-аналитики) позволяет минимизировать объем ручного труда при сборе и обработке больших массивов информации, ускорив тем самым работу аналитиков.

Принцип работы *BI*-систем базируется на трех основных процессах: сборе информации, систематизации и визуализации. Сбор информации как правило происходит из разных источников, в частности *CRM* и *ERP*-систем, электронных таблиц на жестком диске или размещенных в облаке и других. Систематизация заключается в переводе собранных на предыдущем этапе данных к единому формату.

Визуализация заключается в формировании аналитической информации в удобном для пользователя виде – отчеты, дашборды, диаграммы, презентации и проч. Гибкость настроек визуализации позволяет пользователю с начальным уровнем навыков создавать удобные для анализа формы.

Современный этап использования систем бизнес-аналитики связан с трудностями, обусловленными санкционным режимом разработчиков программного обеспечения относительно нашей страны. И если часть крупных разработчиков ПО для бизнеса еще присутствуют на отечественном рынке ПО, то значительная часть софтверных компаний ушли с него и не поддерживает тот софт, который ранее был приобретен отечественными покупателями. В сфере бизнес-аналитики таким продуктом является *Power BI*. При попытке физического или юридического лица купить систему или скачать ознакомительную версию через интернет, сайт выдает сообщение о том, что данный продукт в Российской Федерации не доступен.

Отечественными аналогами данного продукта следует считать системы: *Visiology, Modus BI*, 1С-Аналитика, Даталенс, Форсайт. Стандартная архитектура каждого из решений выглядит в соответствии с рисунком 3.

Рис. 3. Архитектура отечественных BI-решений

В соответствии с велением времени, на отечественном рынке систем *BI*-аналитики присутствуют и облачные решения, например, *Yandex Datalens*, являющаяся частью экосистемы *Yandex.Cloud* и предоставляется бесплатно для всех пользователей.

Следует сделать вывод о том, что процессы информатизации в Российской Федерации идут достаточно быстро. Они тесно связаны с ростом правонарушений, наносящих значительный ущерб экономике страны и благосостоянию граждан. Процессы защиты информации и данных зачастую сильно отстают от «продвинутых» методов взлома, кражи информации и мошенничества в сфере информационно-коммуникационных технологий.

Действительно, Федеральная служба по техническому и экспортному контролю, выполняя в том числе функцию контролирующего рынок ПО органа, формирует перечень угроз и рисков информационной безопасности, однако действовать на опережение не может.

Отечественный рынок систем бизнес-аналитики достаточно успешно развивается, чему способствуют решения Правительства РФ по поддержке сектора экономики, связанного с высокими технологиями.

Литература:

1. Указ Президента Российской Федерации от 13.05.2017 г. № 208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года» // СПС Гарант.

2. Состояние преступности в России за январь–ноябрь 2022 г. – URL: https://epp.genproc.gov.ru/web/gprf/activity/crimestat –
3. Ошанина О. Интернет несет потери. – URL: https://www.vedomosti.ru/importsubstitution/new_technologies/articles/2023/03/14/966290-internet-neset-poteri
4. Приказ Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (с изм. и доп.) // Российская газета. – 2013. – 26 июня. – № 136.
5. Калькулятор СТЭК РФ. – URL: https://bdu.fstec.ru/calc

Modern Business Analytics Tools and Ensuring Economic Security of Economic Entities

Shvetsov A.V., Korotkova A.V., Ryzhakov E.D.
Volga State University of Technology

Analytical research methods are widely used in activities to ensure the economic security of business entities, since they allow the generation of information necessary for management. The relevance of business analytics tools using new information technologies is only growing, especially for solving information security issues.

As part of the goal set in the work, the authors present an assessment of the state of information security in Russia, which is associated with the increase in the number of crimes in the field of information and communication technologies, as well as methods of information protection. The importance of integrated solutions necessary for the development of business intelligence systems is shown.

Key words: economic security, information security, business analytics, crime