РАЗДЕЛ XV. МЕНЕДЖМЕНТ И УПРАВЛЕНИЕ ОРГАНИЗАЦИЕЙ

Унижаев Н.В.

Методика применения комплексного подхода для выявления атак конкурентов

ФГБОУ ВО «Национальный исследовательский университет «МЭИ»

(Россия, Москва)

doi: 10.18411/sr-10-02-2020-22

idsp: sciencerussia-10-02-2020-22

Аннотация

Проведенное исследование, позволило выявить основные проблемы, связанные с атаками конкурентов нацеленными на увеличение доли рынка. Такие атаки появились как негативное явление рыночной экономики. Методика применения комплексного подхода для выявления атак конкурентов предложенная автором основана на концептуальной модели сложного экономического процесса. Исследование показало наличие различных специалистов, связанных с областями юриспруденции, экономики и новых информационных технологиях участвующих в процессах атак со стороны конкурентов. Это обстоятельство требует научной проработки данной проблемы. В качестве гипотезы к основным профилактическим мерам отнесены аналитические возможности специализированных информационных систем. Однако использование таких систем возможно только при наличии специалистов способных интерпретировать полученные результаты. Организация защиты от атак конкурентов не может быть одинаковой для всех. Каждый случай таких атак уникален по своей природе. Однако, проведение профилактических, научно-обоснованных мероприятий может позволить руководителю минимизировать последствия атак.

Ключевые слова: атаки конкурентов, экономические процессы, рейдер, информационные технологии, специализированные информационные системы.

Abstract

The study gave problems. The problems are related to competitor attacks. This aims to increase market share. Attacks have become a negative phenomenon. The methodology for applying an integrated approach to detect attacks by competitors was proposed by the author of this article. The study led to the conclusion that there are various specialists involved in the attacks. This requires scientific study. The main hypothesis - the basis of protection is prevention. However, the use of such systems is possible only if there are specialists capable of interpreting the results. Organization of protection against competitor attacks may not be the same for everyone. Each case of such attacks is unique in nature. Conducting preventive and scientific measures allows the leader to minimize the consequences of attacks.

Keywords: competitor attacks, economic processes, raider, information technology, specialized information systems.

Чаще всего атаки конкурентов преследуют цель увеличения доли рынка. Стратегия маркетинга таких компаний определяется общей долей компании на региональном или глобальном рынке. Стратегия вырабатывается в соответствии с условиями: является ли она лидером рынка, претендентом на лидерство, последователем за лидерами или занимает другую более простую нишу.

Лидеру рынка обычно принадлежит наибольшая доля рынка [1]. Именно лидер как правило преследуют цель увеличения доли рынка в том числе за счет непрерывных атак на конкурентов. Сама суть рыночной экономики для надёжности позиций лидерства заставляет расширять рынок, привлекая новых потребителей, находя новые

способы привлечения клиентов. Поэтому для защиты своей доли рынка все организации стремятся использовать стратегии позиционной, фланговой и мобильной обороны, упреждающих ударов и отражения атаки. Данная терминология не случайно так схожа с армейской. При таких атаках речь идет не просто о потере доли рынка, а о полном банкротстве и потере всего бизнеса. Учитывать следует и то обстоятельство что большинство лидеров рынка стремятся лишить основных конкурентов даже небольшой возможности перехода в наступление.

Увеличения доли рынка может использовать механизмы рейдерства [2]. Рейдерство или недружественные поглощения, стали возможными в середине 90-х годов прошлого столетия. История таких поглощений уходит в века и вероятно будет проявлять себя и в дальнейшем. Все это требует научного исследования и разработки множественных методик для выявления атак конкурентов. Рейдерство – это недружественное, силовое поглощение юридического лица, осуществляемое против воли действующего руководства и собственников [3].

Анализ событий, связанных с атаками конкурентов показывает широкое использование статистической информации и множественной информации о конкурентах. Это обстоятельство можно взять как одно из исходных данных необходимых для методики применения комплексного подхода для выявления атак конкурентов

В последние годы с широким внедрением в бизнес цифровых технологий методы атак конкурентов изменились. Анализ показывает, что они стали более продуманными и проработанными. Кроме этого, в планировании атак конкурентов стали участвовать команды, включающие различных специалистов [4]:

- в области юриспруденции;
- в области экономики;
- в области новых информационных технологиях.

При организации атак на конкурентов специалисты в юриспруденции решают вопросы, связанные с антимонопольным законодательством. Специалисты в экономике нацелены на выявление активов конкурентов и организации процесса монополизации цен. Специалисты в новых информационных технологиях могут обладать навыками хакинга или организации компьютерных атак на конкурентов.

Другой особенностью атак на конкурентов стала открытая или латентная близость к исполнительной и судебной системе. Это вопрос выходит за рамки исследования данной статьи и требует дальнейшей проработки.

Сегодня атаки на конкурентов носят массовый характер [5]. Сведения о таких атаках поступают из всех регионов. Кроме этого, не сложно сделать прогнозы о всплеске таких атак после выборов в 2024 году. Следовательно, собственникам и руководителям организаций к прогнозируемому витку требуется подготовиться. Для этого можно использовать методику применения комплексного подхода для выявления атак конкурентов.

Для решения проблем своевременного выявления атак со стороны конкурентов в условиях внедрения цифровой экономики в качестве профилактической меры можно использовать различные научные методы в том числе комплексный подход. С позиции комплексного подхода недружественных поглощений следует рассматривать как единую составляющую множественных предпосылок, сигнализирующих о возможных атаках [4]. Важно, что в условиях внедрения комплексного подхода все бизнес-процессы следует рассматривать как единое целое. Это позволит решить множество проблем своевременного выявления атак в том числе и в условиях внедрения цифровой экономики.

Рассматривая атаки как предмет комплексного анализа можно сформулировать множество различных правил. В свою очередь такие правила можно синхронизировать с различными классами цифровых технологий [4]:

- большие данные;
- новые производственные технологии;
- промышленный интернет;
- технологии беспроводной связи;
- квантовые технологии; системы распределенного реестра;
- технологии виртуальной и дополненной реальностей.

Комплексный подход нацеленный на выявление признаков атак конкурентов включает:

- выявление общих черт и различий в атаках;
- анализ основ принципов на которых строится атака;
- анализ особенностей управления и стратегии атаки конкурентов;
- формирование этапов, правил стратегии атаки конкурентов.

Границы использования комплексного подхода для выявления признаков новых атак можно выявить, используя следующие признаки:

- все элементы, подвергшиеся атакам должны, оцениваться как единое целое независимо от динамики и цели детализации;
- выявление обстоятельств анализа признаков атак соответствует сценарию решения всех проблем комплексной системы;
- изучение процесса атак не должно ограничиваться анализом фактов, оно должно доходить до получения результата;
- учет отдельных элементов системы управления, имеющих незначительные результаты, могут стать существенными после начала атаки.

Примером последнего признака может быть «внедрение» в управление инсайдера, способствующего процессу развития атаки. С позиции повседневной деятельности такой инсайдер может незначительно ослабить хозяйственную деятельность, а с позиции процесса атаки его деятельность может привести к полному захвату организации.

Рассмотрение комплексного подхода для выявления признаков атак должно соответствовать взаимосвязанным уровням. Например, уровень классификации элементов характеризует из каких элементов состоит система защиты от атак конкурентов. Перечисление элементов должно соответствовать всему процессу управления защитой от атаки конкурентов, а не только тех элементов, которые потенциально подвержены атакам. Уровень структуры характеризует внутреннюю систему управления. Кроме этого, такой уровень должен показать логику связей и способов взаимодействия элементов. Уровень функционального разделения характеризует обязанности аппарата управления. Данный уровень позволяет рассматривать процесс с различных точек зрения. Уровень коммуникаций необходим для уточнения структуры. Он показывает коммуникации и, следовательно, может быть использован при построении семантических сетей. В свою очередь интегративный уровень используется для оценки развития системы безопасности организации. Используя данный уровень можно увидеть перспективу и сделать выводы о защитном потенциале.

Атаки конкурентов можно разделить на следующие классы [4]:

- осуществляемые в рамках нормативно-правовой базы;
- с нарушением общепринятых моральных устоев;
- с нарушением уголовно-процессуального законодательства.

Результатом атаки конкурентов из любого класса может быть полная потеря бизнеса. Это обстоятельство показывает высокую значимость данной проблемы. Методика применения комплексного подхода для выявления атак конкурентов преимущественно нацелена на действия с нарушением уголовно-процессуального законодательства. Защита по другим классам должна строиться исключительно на экономических постулатах.

Атаки с нарушением уголовного законодательства иногда называют «черными атаками» или «черными рейдерским атакам». Это криминальные атаки и, следовательно, руководитель атакуемой организации вправе обратиться за помощью в правоохранительные структуры.

Основываясь на этих данных можно предложить использование комплексного подхода для выявления признаков атак конкурентов. На Рис.1. представлена концептуальная модель применения комплексно подхода для выявления атак конкурентов.

Рисунок 1. Концептуальная модель применения комплексного подхода для выявления атак конкурентов

Модель включает в себя процесс выявления атак. Такой процесс может быть основан на информации циркулирующей в Интернет и СМИ. Для поиска такой информации можно использовать специализированные информационные системы, например, Интегрум, Контур-Фокус или Спарк.

Вместо руководителя контроль за сотрудниками, участвующими в бизнес-процессах может быть возложен на службу безопасности. Хороший эффект может получиться, когда руководитель такой службы входит в круг топ-менеджмента. Тогда он совместно с руководством может легко осуществлять контроль за [2]:

- продажей долей общества (организации) физическими и юридическими лицами;
- возложением новых обязанностей на участников общества (организации);
- незаконным исключением из общества (организации);
- организацией и решениями общего собрания;
- соблюдением требований регулирующих органов.

Использование комплексного подхода для выявления недружественных поглощений может потребовать дополнительной проверки различных документов, например, документов о регистрации и документов о долях собственности. Периодичность такой проверки не регламентирована. Обычно ее принято проводить один раз в год. Считается обязательной проверка регистрации новых компаний по юридическому адресу. Такая проверка может позволить сделать профилактику атак со стороны конкурентов.

Использование комплексного подхода для выявления признаков атак со стороны конкурентов должно способствовать выстраиванию и оптимизации системы управления в соответствии с требованиями инвесторов. Отсутствие рисков, связанных

с атаками, будет способствовать повышению уровня доверия со стороны инвесторов, и как следствие увеличению активов хозяйствующего субъекта.

Методика применения комплексного подхода для выявления атак конкурентов подразумевает простоту отчетных форм. Если формы отчетности являются сложными, то их требуется переработать. Чем более простой и «прозрачной» будут формы отчетности, тем меньше шансов у конкурентов использовать уязвимости документооборота для проведения своих атак.

Подводя итог можно констатировать, что организация защиты от атак конкурентов не может быть универсальной. Каждый случай таких атак уникален. Однако проведение профилактических, научно-обоснованных мероприятий может позволить руководителю находиться в состоянии готовности к отражению атак со стороны конкурентов и минимизации последствий.

1. Власенко М.Н., Информационно-аналитическое обеспечение принятия управленческих решений - значимый фактор повышения экономической безопасности хозяйствующих субъектов в условиях развития рыночной системы хозяйствования. Журнал «Национальные интересы: приоритеты и безопасность». 2010. Т. 6. № 33 (90). С. 59-69.
2. Унижаев Н.В. Проблемы внедрения модели управления электронной информационно-образовательной средой в очной форме обучения. Вестник университета. 2018. № 3. С. 24-27.
3. Татаринов В.В. Современные подходы к построению курса высшей математики для подготовительных отделений технических университетов. Современные информационные технологии и ИТ-образование. 2015. Т. 11. № 1. С. 234-238.
4. Унижаев Н.В. Информационно-аналитическое обеспечение безопасности организации. Для вузов и для дополнительного образования / Санкт-Петербург, 2018.
5. Шаталов Р.Н., Брежнева А.Н. Проблемы и методы обработки GPS информации. Программная инженерия: современные тенденции развития и применения сборник материалов Всероссийской конференции. 2017. С. 183-188.

Усман Е.В.¹, Федотова А.В.²

Анализ эффективности инвестиционных проектов в условиях применения концепции бережливого производства

¹*Национальный исследовательский ядерный университет «МИФИ»*

²*Московский авиационный институт (национальный исследовательский университет)*
(Россия, Москва)

doi: 10.18411/sr-10-02-2020-23

idsp: sciencerrussia-10-02-2020-23

Актуальность темы исследования определяется необходимостью разработки методического подхода к оценке инвестиционных проектов на действующих предприятиях в рамках применения концепции бережливого производства.

Целью использования концепции бережливого производства на современных предприятиях является минимизация потерь на всех этапах создания ценности продукции.

Активное применения данной концепции в рамках холдингов Росатом, РЖД и других государственных корпораций, требует разработки методического обеспечения оценки эффективности предлагаемых мероприятий.

Оценка эффективности предложений на действующих предприятиях, требующих дополнительных вложений, подразумевает использование одного из методов: метод целевого выделения проекта; метод анализа изменения денежных потоков; метод объединения; метод наложения проекта.

Наиболее приемлемым в рамках количественной и качественной оценки эффективности применения технологий бережливого производства представляется