УДК 338

Цветникова Виктория Сергеевна

Санкт-Петербургский государственный экономический университет

tsvet.viktoriya@mail.ru

СОВЕРШЕНСТВОВАНИЕ ОРГАНИЗАЦИИ СЛУЖБЫ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Аннотация: В статье рассматривается понятие и сущность службы экономической безопасности организации, а также раскрывается сущность угроз экономической безопасности, препятствующих успешному её функционированию. Предложены мероприятия по нейтрализации наиболее часто встречаемых угроз экономической безопасности: внедрение Положения о проверке профессиональных компетенций потенциальных сотрудников, проведения детального анализа контрагента и внедрения многофункциональной антифрод-системы в крупных компаниях.

Ключевые слова: экономическая безопасность, предприятие, служба безопасности, контрагент, кадровая безопасность, антифрод.

Tsvetnikova V.S.

Saint-Petersburg State University of Economics

IMPROVING THE ORGANIZATION OF THE COMPANY'S SECURITY SERVICE

Abstract: The article deals with the concept and essence of the organization's economic security service, as well as reveals the essence of threats to economic security that prevent its successful functioning. Measures are proposed to neutralize the most common threats to economic security: the introduction of Regulations on checking the professional competencies of potential employees, conducting a detailed analysis of the counterparty and implementing a multifunctional anti-fraud system in large companies.

Keywords: economic security, enterprise, security service, counterparty, personnel security, anti-fraud.

Актуальность исследования связана с тем, что проблема обеспечения безопасности на предприятии является первостепенной и требующей незамедлительного решения в силу того, что функционирование предприятий в настоящее время происходит в условиях нестабильной рыночной среды. Успешность деятельности хозяйствующего субъекта напрямую зависит от обеспечения его безопасности.

Кризисные ситуации, возникающие в экономике в условиях социально-экономической и политической нестабильности, недобросовестности конкуренции, несовершенства законодательной базы порождают необходимость поиска российским бизнесом грамотных решений для успешного ведения дел предприятия, решения сложнейших задач, формирования и применения системного подхода для обеспечения безопасности.

Российский опыт ведения бизнеса показывает, что для его успешной работы, если речь идёт о средних и крупных предприятиях, существует потребность в создании надёжной системы безопасности, которую сложно представить без существования службы, которая осуществляет реализацию специальных мероприятий, защищающих организацию от различных угроз – Службы безопасности предприятия.

«Под безопасностью понимается такое состояние субъекта, при котором вероятность изменения присущих данному субъекту качеств и параметров его внешней среды невелика, меньше определённого интервала». [2]

Как правило, безопасность может быть оборонной, промышленной, экологической, информационной, силовой, экономической. Каждая из составляющих по-разному влияет на развитие бизнеса. Чтобы защитить организацию от внешних и внутренних угроз, руководству следует уделить особое влияние экономической составляющей безопасности.

«Экономическая безопасность предприятия – это состояние, при котором все ресурсы используются эффективно, предотвращаются внешние и внутренние угрозы и обеспечивается стабильное функционирование предприятия». [1]

Служба экономической безопасности – это обособленная

многофункциональная структурная единица предприятия, занимающаяся обеспечением безопасности внутренних и внешних процессов, защитой от умышленных посягательств персонала, а также злонамеренных действий конкурентов.

«Штатная численность и состав службы экономической безопасности утверждается директором исходя из условий и особенностей деятельности предприятия». [4]

«Основной целью Службы экономической безопасности предприятия является обеспечение условий защищенности на основании разработанных и внедрённых мероприятий». [3]

Служба экономической безопасности выполняет в организации ряд функций, среди которых самыми важными, на наш взгляд, являются функция кадровой, технико-технологической и информационной составляющих, так как угрозы со стороны персонала, контрагентов, а также угрозы, связанные с информационными системами и технологиями – наиболее часто встречающиеся угрозы современных предприятий (табл.1).

Таблица 1 – Наиболее часто встречаемые риски и угрозы экономической безопасности по функциональным составляющим на предприятиях

Функциональная составляющая угрозы экономической безопасности	Пример угрозы экономической безопасности
Кадровая	отсутствие профессиональных компетенций сотрудников
Технико-технологическая	угроза, которая может возникнуть вследствие поставки некачественных запчастей, оказания некачественных услуг, нарушений условий договора
Информационная	противоправные действия третьих лиц, наносящие ущерб информационной безопасности организации, а также использование уязвимостей информационных ресурсов с целью завладения конфиденциальной информацией

Данные угрозы наносят значительный ущерб функционированию Службы экономической безопасности, так как:

1) следствием реализации угрозы кадровой составляющей является нанесение экономического ущерба, подрыв делового имиджа компании,

возникновение конфликтов партнёрами, а также контролирующими и правоохранительными органами. Наличие данной угрозы затрудняет функционирование службы экономической безопасности, так как ущерб от реализации данной угрозы без принятия необходимых мер будет возрастать, и организация будет затрачивать финансовые средства и силы на восстановление делового имиджа, уплату штрафных санкций;

2) реализация угрозы технико-технологической составляющей ведёт, в первую очередь, к значительным финансовым потерям. Неслаженная работа с контрагентами приводит к тому, что деятельность службы экономической безопасности направлена не на предварительную проверку деятельности контрагентов перед заключением соглашений, а на судебные разбирательства, вопросы возмещения убытков, осуществление поиска способов восстановления деловой репутации.

3) угроза информационной безопасности связана с тем, что злоумышленники стремятся найти уязвимости в информационных системах, чтобы получить доступ к конфиденциальной корпоративной информации. Это приводит к экономическим потерям вследствие кражи материальных активов и проведения фальшивых транзакций. Чем больше компания применяет в своей деятельности цифровые технологии, тем сильнее должна осуществляться защита от информационных атак, то есть должна меняться система выявления, оценки и минимизации рисков и угроз. Отсутствие должной степени защиты ведёт не только к снижению деловой репутации и увеличению судебных разбирательств с клиентами компании, но и к подрыву взаимоотношений с контрагентами, росту затрат на восстановление утерянной информации.

Все угрозы указывают на недостатки, нарушения в деятельности Службы экономической безопасности предприятия. Существующие и растущие угрозы экономической безопасности, противодействие которым организацией не осуществляется или осуществляется не в полной мере, требуют незамедлительного реагирования Службы экономической безопасности, совершенствования организации его деятельности и разработки рекомендаций

по борьбе с данными угрозами.

Наличие угрозы кадровой составляющей может говорить о том, что методика проверки потенциальных сотрудников при приёме на работу в организациях выстроена неэффективно или же предварительная проверка потенциального сотрудника совсем не осуществляется. Чтобы минимизировать данную угрозу, предлагается вводить в компаниях Положение о проверке профессиональных компетенций потенциальных сотрудников.

В данном Положении разработаны требования к соискателю, которые являются существенными при выборе кандидата на вакантную должность.

Наиболее важными из них являются:

- прохождение письменного и устного тестирования перед трудоустройством, позволяющее выявить истинный уровень подготовки соискателя, его соответствие профессиональным требованиям, предъявляемым на вакантную должность;

- прохождение тестирования на полиграфе для отдельных категорий сотрудников, деятельность которых будет связана с получением важнейшей конфиденциальной информации;

- предоставление медицинских справок, подтверждающих отсутствие психических отклонений, заболеваний, алкогольной и наркотической зависимости.

Эффективность данного Положения заключается в том, что организация сможет предотвратить косвенные убытки, связанные с персоналом, которые заключаются в приёме на работу сотрудников с поддельными документами об образовании, поддельными медицинскими справками, приёме на работу сотрудников, которые ранее были пойманы на воровстве или уволены вследствие разглашения конфиденциальной информации компании.

Положительный эффект внедрения Положения состоит в том, что:

1. Действия сотрудников не противоречат коммерческим интересам компании, так как, согласно Положению, проводится тщательная проверка потенциального сотрудника и исключается возможность принятия на работу

неквалифицированного сотрудника или человека, который целенаправленно устраивается на работу, чтобы получить конфиденциальные данные и нанести серьёзный экономический ущерб (данный факт может быть выявлен путём тестирования на полиграфе для потенциальных сотрудников определённых отделов, где предоставляется доступ к конфиденциальной информации, имеющей особую важность).

2. Организация не несёт финансовых убытков вследствие действий неквалифицированных сотрудников, а также не теряет деловой имидж.

Угрозой технико-технологической составляющей является угроза поставки некачественных запчастей, оказания некачественных услуг, нарушений условий договора. Данная угроза реализовывается вследствие того, что службой экономической безопасности неэффективно и неслаженно выстроена работа с контрагентами. «Контрагенты изучаются всегда в конкретных целях и под определённым ракурсом, чтобы обезопасить предприятие от потенциально существующего риска». [5]

В качестве рекомендации по противодействию данной угрозе, а также совершенствования деятельности службы экономической безопасности предприятия, предлагается проводить детальный анализ контрагента на основе Методики проверки контрагентов, в которую будет входить система Black-list для контрагентов.

Целью внедрения данной методики является минимизация налоговых рисков, снижение угрозы поставки некачественных запчастей, оказания несоответствующих условиям договора услуг.

Порядок действий сотрудников отдела работы с контрагентами службы экономической безопасности должен включать в себя:

1. Поиск информации о деятельности контрагента по источникам, находящимся в открытом доступе с последующим формированием досье по контрагенту.

2. Проверка сведений о постановке контрагента на налоговый учёт.

3. Проверка юридического и фактического адреса нахождения

контрагента.

4. Сопоставление кодов ОКВЭД в документах с фактическими направлениями деятельности.

5. Проверка подлинности и действительности лицензий, проверка наличия или отсутствия информации о контрагенте в реестрах ВАС РФ и ФССП.

6. Изучение сайта организации, отзывов.

7. Запрос копий уставных документов, паспортных данных руководителя организации – контрагента.

8. Изучение бухгалтерской отчётности компании с целью проведения анализа платёжеспособности и финансовой устойчивости.

Система Black-list представляет собой автоматизированную совокупность данных по контрагентам, сотрудничество с которыми невозможно вследствие поставки некачественных запчастей, оказания некачественных услуг, нарушений условий договора. Суть системы заключается в том, что сотрудниками отдела по работе с контрагентами Службы экономической безопасности составляется список, состоящий из наименования организации, сведений об организации, причины внесения в список, даты внесения в список, а также включает возможную дату исключения из списка. Решение о возможности или невозможности исключения из системы Black-list принимается начальником отдела по работе с контрагентами. Данное решение зависит от причины включения в список.

Итак, оценка эффективности применения методики проверки контрагента с применением системы Black-list состоит в том, что:

1. Организация не несёт финансовых потерь из-за дебиторской задолженности контрагента.

2. Тщательная проверка контрагента по методике исключает возможность нанесения ущерба деловой репутации организации.

3. Организация значительно уменьшает затраты времени и финансовых средств путём уменьшения случаев судебных разбирательств (в том числе по возмещению ущербов) и их издержек.

4. Снижается время на проверку контрагента, потому что методика предполагает комплексное изучение деятельности контрагента, где большая часть информации получается из открытых источников в сети Интернет. Финансовые вложения и дополнительная рабочая сила не требуются.

Функция информационной безопасности, как правило, недооценивается компаниями. Тем не менее, незаконное владение информацией даёт возможность злоумышленникам получить доступ к коммерческой конфиденциальной информации, возможность производить незаконный оборот финансовых средств, что может обернуться для предприятия банкротством или большими убытками. Чтобы этого избежать, Служба безопасности разрабатывает комплекс мер, направленный на создание и внедрение защитных средств и систем для защиты от угроз, которые предварительно планируются мошенниками.

Одной из угроз информационной составляющей экономической безопасности во многих организациях является угроза, связанная с противоправными действиями третьих лиц, наносящими ущерб информационной безопасности предприятия. Также нередко злоумышленники пользуются уязвимостями информационных ресурсов с целью завладения конфиденциальной информацией.

Рекомендацией по противодействию данным угрозам может выступать разработка и внедрение собственной многофункциональной антифрод – системы в крупных компаниях под контролем сотрудников отдела информационной безопасности Службы экономической безопасности совместно с IT-департаментами, которая позволила бы выявлять и предотвращать противоправные действия мошенников и операции.

Антифрод – система проводит мониторинг мошеннических операций, проверяя каждый платёж в режиме реального времени и блокируя те, которые считает подозрительными.

Основные функции антифрод-системы:

1) система способна отсеивать тех, кто нечестно пользуется материальными активами компании в виде бонусов или скидок, например

регистрирует каждый раз новые аккаунты, с целью получения привилегий;

2) система способна защищать личные аккаунты клиентов компании от взлома, например, в качестве защиты от внешнего фрода система способна сгенерировать одноразовые пароли для личных аккаунтов путём подтверждения через SMS;

3) система проверяет подозрительных покупателей с помощью современной технологии 3-D Secure, которая обеспечивает безопасность платежей в сети Интернет. С помощью этой технологии можно идентифицировать подлинность держателя карты и снизить риск мошенничества с использованием банковской карты;

4) система определяет транзакции украденных карт пользователей и регистрации учетных записей нежелательными клиентами.

Эффективность внедрения многофункциональной антифрод – системы состоит в том, что:

1. Исключаются подозрительные сделки и транзакции, так как система их мгновенно блокирует.

2. Уменьшаются финансовые затраты на осуществление поиска мошенников, а также возмещения финансовых средств и восстановление аккаунтов клиентам компании.

3. Значительно снижается количество судебных разбирательств. Компания не теряет своих клиентов и исключается возможность подрыва деловой репутации.

На сегодняшний день тема организации службы безопасности является особенно актуальной вследствие возрастающих кризисных явлений в экономике, недобросовестной конкуренции. Для обеспечения эффективности работы Службы экономической безопасности необходимо правильно определить структуру данной службы, исходя из приоритетных целей и задач организации, а именно численность персонала, участвующего в работе службы, ресурсов технического и материального обеспечения. Эффективность предложенных рекомендаций высока, так как их внедрение позволит исключать сотрудничество

с ненадёжными поставщиками, принимать на работу только квалифицированных сотрудников с хорошей репутацией, а также значительно снизить угрозу информационной безопасности, связанную с мошенничеством.

Список литературы

1. Бондина, Е. А. Формирование структуры экономической безопасности на предприятиях / Е. А. Бондина, С. Е. Чинахова. — Текст : непосредственный // Молодой ученый. — 2017. — № 13 (147). — С. 253-257. — URL: https://moluch.ru/archive/147/41283/ (дата обращения: 25.10.2020).

2. Киселева, И.А. Экономическая безопасность предприятия: особенности, виды, критерии оценки / И.А. Киселева, Н.Е. Симонович, И.С. Косенко // Вестник Воронежского государственного университета инженерных технологий. — 2018. — № 2. — С. 415-423. — ISSN 2226-910X. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/journal/issue/309853 (дата обращения: 26.09.2020). — Режим доступа: для авториз. пользователей.).

3. Сергеев, А. А. Экономическая безопасность предприятия : учебник и практикум для вузов / А. А. Сергеев. — Москва : Издательство Юрайт, 2020. — 273 с. — (Высшее образование). — ISBN 978-5-534-10645-9. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/455598 (дата обращения: 28.10.2020).

4. Сергеева И.А. // Комплексная система обеспечения экономической безопасности предприятия : учебное пособие / Федеральное государственное бюджетное образовательное учреждение высшего образования «Пензенский государственный университет» (ПГУ). - Пенза : Изд-во ПГУ, 2017.

5. Шульц, В. Л. Безопасность предпринимательской деятельности : учебник для вузов / В. Л. Шульц, А. В. Юрченко, А. Д. Рудченко ; под редакцией В. Л. Шульца. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 585 с. — (Высшее образование). — ISBN 978-5-534-12368-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/447405 (дата обращения: 27.09.2020).