Таким образом, общая структура механизма управления инновационной деятельностью предприятия должна раскрываться в соответствии с особенностями конкретной предметной области, сферы деятельности организации, конкретными характеристиками управляемой системы, в том числе материально–техническими, кадровыми, финансовыми, информационными, научно–методическими условиями ее функционирования.

При этом многообразие свойств, содержания и вариантов реализации того или иного организационно–экономического механизма управления определяется большим количеством взаимодействующих субъектов управления и их целями, объектами целенаправленного воздействия, реализующими функции управления, средств и механизмов управления.

Литература

1. Даль В.И. Большая российская энциклопедия. Электронная версия— М.- 2016. http://slovardalja.net/ 25.01.2022.
2. Лопатин В. В. Толковый словарь современного русского языка. – М.: Эксмо, 2013. – 928 с.
3. Дуболазова Ю.А. Инновационный механизм – важнейшее направление реализации эффективного развития промышленного предприятия /Ю.А. Дуболазова //Международный журнал. - 2017. - № 04 (58) - С. 86-88.

Нестеренко Е.В., 1 курс (КарУ им. академика Е.А. Букетова)
Научный руководитель - к.э.н., доцент, профессор кафедры менеджмента Дарибеков С.С.

УГРОЗЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ МАЛОГО И СРЕДНЕГО БИЗНЕСА В СОВРЕМЕННЫХ УСЛОВИЯХ

В современном мире с его стремительно меняющейся картиной мира и постоянно растущим уровнем конкуренции невозможно оставаться на прежнем уровне. Это означает, что для поддержания своего положения в конкурентной борьбе необходимо постоянно совершенствовать и развивать свои навыки, компетенции и опыт, а также внедрять новые подходы и технологии. В рамках цифровизации в первую очередь речь идет о новых способах взаимодействия людей, компаний и государства.

Стремительное цифровое развитие оказывает существенное влияние на деятельность малого и среднего бизнеса (МСБ).

Понятие «экономической безопасности предприятия» первоначально рассматривалось как защита информации, то есть оно тесно увязывалось с процессами информатизации деятельности предприятия. В настоящее время термин утратил свое первоначальное значение, поскольку под этим понятием стали рассматривать совокупность мер, направленных на обеспечение

экономической устойчивости предприятия в условиях нестабильной внешней среды и угроз со стороны конкурентов, партнеров, государства.

Анализ угроз позволяет выявить их существенность и оценить степень уязвимости предприятия и его отдельных подсистем.

Одним из распространенных подходов к классификации угроз экономической безопасности предприятий является функциональный. Малаховская М.В. предлагает следующую их группировку:

- физические угрозы (кражи, нападения, взломы, рэкет, проникновения на территорию предприятия и т.д.);
- информационные угрозы (копирование, уничтожение или подмена информации, взлом корпоративных сетей, заражение «вирусами», блокирование работы серверов путем провоцирования искусственной перегрузки и т.д.);
- экономические угрозы (недобросовестная конкуренция, промышленный шпионаж, неправомерное использование «административного ресурса» и т.д.);
- юридические угрозы (заведомо неверное оформление договоров и иных документов, подлоги, рейдерство, предвзятые проверки контролирующих органов и т.д.) [1].

По мере того как происходит развитие информационных технологий, происходят и изменения в действиях злоумышленников, с деятельностью которых связаны не только цифровые, но и физические угрозы экономической безопасности предприятия.

Киберпреступления в современном мире становятся одними из наиболее опасных и трудно выявляемых. Согласно данным Комитета по правовой статистике и специальным учётам Республики Казахстан, в 2021 г. число уголовных правонарушений в сфере информатизации и связи увеличилось на 6% по сравнению с 2020г. При этом наибольшая доля приходится на неправомерный доступ к информации, в информационную систему или информационно-коммуникационную сеть (ст.205) и составляет 70% от всех киберпреступлений [2].

С учетом расширения и усиления процессов цифровизации число и серьезность киберпреступлений в будущем будет возрастать. Это создаст новые и трансформирует существующие угрозы экономической безопасности предприятий МСБ. В связи с этим, задачей менеджмента становится создание и развитие на предприятиях специализированных подразделений по противодействию угрозам информационной безопасности, исходящим как от собственного персонала, так и из внешней среды. Это требует значительных расходов. Так, по данным исследовательской компании Astute Analytica, затраты на информационную безопасность в мире в ближайшие годы будут увеличиваться в среднем на 13,4% ежегодно. Ожидается, к 2027 году расходы

на нее в глобальном масштабе достигнут $345 млрд против $162 млрд в 2021 году (рисунок 1).

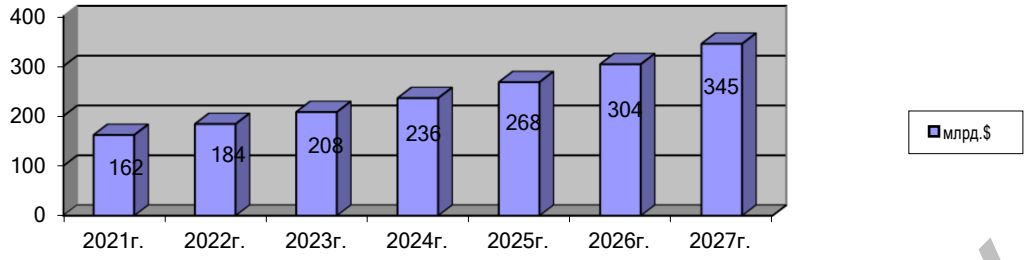

Рисунок 1. Ожидаемые затраты на информационную безопасность в мире 2021-2027гг.

П р и м е ч а н и е – источник [3]

Очевидно, что небольшие предприятия, которые не обладают достаточными ресурсами, не смогут самостоятельно эффективно противодействовать киберугрозам.

Происходит «размывание границ» отдельных типов угроз. Все они становятся в той или иной мере цифровыми, что является следствием проникновением цифровых технологий во все бизнес-процессы и процессы управления предприятий.

Цифровизация дает возможность повышения информационной открытости предприятия, следовательно – его уязвимости для вредоносного воздействия. МСБ по своей природе во многом становится цифровым. Это связано с широким распространением цифровых платформ [4]. В ряде отраслей это приводит к коренному изменению бизнес-моделей.

Таким образом, в условиях быстрорастущей цифровизации социально-экономической системы, происходят существенные изменения в организации обеспечения экономической безопасности предприятий.

Литература

1. Малаховская М.В. Экономическая безопасность: государство, регион, предприятие: монография. Димитровград, 2017. 143 с.

2. Комитет по правовой статистике и специальным учётам Генеральной прокуратуры Республики Казахстан [Электронный ресурс]. — Режим доступа: https://qamqor.gov.kz (Дата обращения: 9.02.2022).

3. DailyComm [Электронный ресурс]. — Режим доступа: https://www.dailycomm.ru (Дата обращения: 9.02.2022).

4. Грибанов Ю.И., Репин Н.В., Руденко М.Н. Развитие информационной инфраструктуры управления предприятием на основе ИТ-аутсорсинга: монография. М.: Креативная экономика, 2019. 220 с.