

Недооцененные риски организаций в современном мире

Научный руководитель – Фешина Стелла Сергеевна

Колпакова Анна Владимировна

Студент (бакалавр)

Финансовый университет, Факультет анализа рисков и экономической безопасности,

Анализ рисков и экономическая безопасность, Москва, Россия

E-mail: sunnypig@yandex.ru

В современном мире как никогда актуальна фраза Натана Ротшильда: «Кто владеет информацией, тот владеет миром». Информация является одним из основных ресурсов производства, а также наименее защищенным из них. Информационные риски - это большая угроза деятельности и существованию компаний. Среди них взломы облачных хранилищ [1], DDoS-атаки, кибератаки криптомайнеров [2] и, самое важное, недостаточные знания персонала компании об информационной безопасности и устройстве информационных систем. Около 84% компаний недооценивают риски, связанные с человеческим фактором по статистике антивирусной компании ESET. [3]

Следующим аспектом исследования является риск нелояльности персонала, а также возможности борьбы с ним. Каждый человек индивидуален, и при приеме на работу никто не знает, как сложатся отношения нового сотрудника с коллективом и будет ли он доволен своей работой. Как показывает мировой опыт, нелояльный персонал - неисчерпаемая база злоумышленников. [4] Угрозой благополучию компании в данном случае становится риск воровства, например, товаров из магазина или денег из банка, а также при увольнении сотрудника риск кражи баз данных и информации о клиентах с целью передачи конкурентам. Из-за таких действий бывшего сотрудника компания может потерять не только часть клиентской базы и репутацию на рынке, но и деньги.

Третьей значимой проблемой становится полная остановка производства. Предприятия часто обращаются в страховые компании с целью застраховать имущество, однако редко кто задумывается приобрести страховку от остановки производства в случае поломки оборудования, в то время как убытки от этого исчисляются миллионами или даже миллиардами рублей, потерями предприятием своего места на рынке и части клиентской базы.

Последним, но не менее важным риском, освещенным в данной статье, является риск кражи интеллектуальной собственности. Хищение интеллектуальной собственности - один из самых древних методов ведения недобросовестной конкуренции. [5] Опасность состоит в том, что компания-разработчик ноу-хау несет огромные убытки в случае кражи его конкурентами. Кроме того, на данный момент в России не существует готового страхового продукта, чтобы компенсировать потери в случае хищения.

В ходе работы была изучена статистика наступления вышеуказанных рисков, их ключевые составляющие, оказывающие наибольшее влияние на последствия, а также возможные пути решения данных проблем.

Проведенное исследование показало, что компаниям ещё предстоит улучшать систему информационной безопасности, налаживать обратную связь с персоналом, чтобы лучше понимать атмосферу в коллективе, работать над обеспечением резервных путей ведения

деятельности в случае остановки производства, и, кроме того, разрабатывать способы защиты интеллектуальной собственности.

- 2.
- 3.

Источники и литература

- 1) Е. Юдина. Топ-12 угроз облачной безопасности по версии Cloud Security Alliance. 10.05.2016 <https://iaas-blog.it-grad.ru/bezopasnost/top-12-ugroz-oblachnoj-bezopasnosti-po-versii-cloud-security-alliance/>
- 2) Статья по отчету компании Check Point Software Technologies Ltd. Компании недооценивают риск угрозы криптомайнеров. 11.02.2019 <https://www.plusworld.ru/daily/c-at-security-and-id/post-422495/>
- 3) А. Панасенко. 84% компаний недооценивают риски, связанные с человеческим фактором. 06.07.2017 <https://www.anti-malware.ru/news/2017-07-06/23357>
- 4) Л. А. Агатова, Г. Л. Смолян, Г. Н. Солнцева. Нелояльность персонала как угроза безопасности организации. Труды ИСА РАН 2007. Т. 31
- 5) В. В. Галкин. Хищение интеллектуальной собственности. 31.01. 2012 <http://vadim-galkin.ru/business-basics/unfair-competition/theft/>