Аннотация

В условиях роста числа кибератак и финансового ущерба от них возникает необходимость в определении четкой взаимосвязи между финансовой устойчивостью предприятия и ее уровнем информационной безопасности. Целью статьи является построение модели управления финансовой устойчивостью предприятия в контексте информационной безопасности.

Результаты исследования могут заложить основу для оптимизации затрат на информационные технологии, что окажет благоприятное влияние на финансовые показатели деятельности компаний.

Ключевые слова: информационная безопасность, финансовая устойчивость, кибератака, информационный риск

Annotation

In the context of the growing number of cyber attacks and financial damage from them, there is a need to determine a clear relationship between the financial stability of the company and its level of information security. The purpose of the article is to build a model for managing the financial stability of the company in the context of information security.

The results can lay the foundation for optimizing information technology costs, which will have a positive impact on the financial indicators of companies.

Keywords: information security, financial stability, cyberattack, information risk

Модель управления финансовой устойчивостью предприятия в контексте информационной безопасности

Введение.

Эпидемия новой коронавирусной инфекции спровоцировала ускорение цифровой трансформации различных отраслей экономики. Вследствие чего компании столкнулись с проблемой масштабных кибератак. На данный момент наблюдается непрерывный рост финансовых потерь, нарушений целостности и непрерывности функционирования компаний в следствие кибератак. По данным Positive Technologies, в 2021 году треть опрошенных компаний подверглась кибератакам, в особенности, финансовый сектор, предприятия топливно-энергетического комплекса и госучреждения. По информации МИД, к концу 2021 года ущерб от киберпреступлений в России достиг $6 трлн.

Данные обстоятельства обуславливают построение компаниями эффективной системы информационной безопасности, что является одной из важнейших мер по

поддержанию и укреплению их финансового состояния, платежеспособности и финансовой устойчивости.

В условиях нестабильных условий работы и высокого уровня неопределенности, характерного для настоящего этапа развития российской экономики, управление финансовой устойчивостью должно быть направлено на обеспечение финансовой гибкости, а именно, способности компаний противостоять рискам с минимизацией затрат.

Влияние информационных рисков на финансовую устойчивость предприятия.

Информационные риски могут повлиять на финансовую стабильность предприятия через потерю деловой репутации, через утрату элементов структуры и нарушение системных связей.

Рисунок 1 иллюстрирует причинно-следственную цепочку от кибератаки до финансовой нестабильности.

Рисунок 1 – Взаимосвязь информационной безопасности и финансовой устойчивости

Однако для того, чтобы управлять финансовой стабильностью в контексте информационной безопасности необходимы точные количественные оценки потенциальных потерь от киберинцендентов.

Для оценки рисков информационной безопасности выделяют две группы показателей: показатели, представляющие собой численное выражение выгоды от внедрения средств защиты информационной безопасности, а также показатели, оценивающие объем инвестиций в информационные технологии.

Первый набор показателей рассматривает выгоды от внедрения защитных приспособлений, которые обеспечиваются за счет уменьшения величины финансового ущерба от киберинцидентов.

А) ГОП – годовые ожидаемые потери.

ГОП представляют собой потери денежных средств предприятия и рассчитываются по формуле:

$$\text{ГОП} = \text{ПУ} \cdot \text{ЕКА} \quad (1)$$

где ПУ – потенциальный ущерб от реализации единичной угрозы;

ЕКА – ожидаемое ежегодное количество атак.

Потенциальный ущерб от реализации единичной угрозы рассчитывается по формуле:

$$\text{ПУ} = \text{СИА} \cdot \text{К}_\text{р}, \quad (2)$$

где СИА – стоимость активов предприятия, относящихся к информационной безопасности;

$К_р$ – коэффициент риска потерь от реализации угроз, выраженный в долях от стоимости активов предприятия, относящихся к системе информационной безопасности.

Б) ОВИ – ожидаемая прибыль от инвестиций в обеспечение информационной безопасности.

ОВИ рассчитывается как разность между ГОП при отсутствии мер безопасности ($ГОП_0$) и ГОП при использовании защитных мер ($ГОП_с$):

$$\text{ОВИ} = \text{ГОП}_0 - \text{ГОП}_\text{с} \quad (3)$$

В) ОЧВ – ожидаемые чистые выгоды от инвестиций в обеспечение информационной безопасности.

ОЧВ составляет разность между ОВИ и затратами предприятия на реализацию средств по защите информации:

$$\text{ОЧВ}_\text{с} = \text{ОВИ}_\text{с} - \text{ЗК} = \text{ГОП}_0 - \text{ГОП}_\text{с} - \text{ЗК}, \quad (4)$$

где ЗК – затраты предприятия на реализацию средств по защите информации.

Вторая группа состоит из показателей для подсчета эффективности инвестиций в информационную безопасность.

А) РИИ – рентабельность инвестиций в информационные технологии.

РИИ связывает расходы на меры защиты информации с управлением рисками для демонстрации финансовых выгод для организации. РИИ показывает отношение ОЧВ к затратам на реализацию средств по защите информации:

$$\text{РИИ} = \frac{\text{ОЧВс}}{\text{ЗК}} = \frac{\text{ГОП}_0 - \text{ГОП}_\text{с} - \text{ЗК}}{\text{ЗК}} \quad (5)$$

Также коэффициент РИИ предлагается рассчитывать на основании следующей формулы:

$$\text{РИИ} = \frac{\text{ГОП} \cdot \text{ПЭК} - \text{ЗК}}{\text{ЗК}}, \quad (6)$$

где ПЭК – показатель эффективности меры защиты информации.

ГОП также могут рассчитываться по формуле:

$$\text{ГОП} = \text{СИА} \cdot \text{ЕКА} \cdot \text{К}_\text{р} \quad (7)$$

В практике индекс РИИ нашел широкое применение в силу своей простоты для понимания и вычисления, доступности данных, необходимых для расчетов, и т.д. Главным преимуществом индекса РИИ является его направленность на оценку важнейшего показателя деятельности любой компании – прибыльности, что позволяет проводить сравнительный анализ различных проектов.

Б) ВРА – выгоды злоумышленника от реализации кибератаки.

Данный показатель позволяет оценить сложность реализации атаки злоумышленником с применением средств информационной безопасности. Другими словами, ВРА характеризует соотношение доходов атакующей стороны, которые получены путем успешной реализации атаки, над затратами, которые он несет из-за принятия подразделением по защите информации технологий отражения киберугроз.

$$\text{ВРА} = \frac{\text{ОВ} \cdot (1 - \text{ПЭК}) - (\text{ПР}_\text{а} + \text{ДР}_\text{а})}{(\text{ПР}_\text{а} + \text{ДР}_\text{а})}, \quad (8)$$

где ОВ – ожидаемая выгода от атаки (принимается равной показателю ГОП);

$\text{ПР}_\text{а}$ – постоянные расходы злоумышленника;

$\text{ДР}_\text{а}$ – дополнительные расходы злоумышленника.

Эффективная система информационной безопасности должна состоять из таких средств защиты информации, которые дают возможность максимизации рентабельности инвестиций в информационную безопасность РИИ и минимизации прибыли хакера ВРА.

Для формирования эффективной системы информационной безопасности на предприятии и рационального выбора контрмер необходимо придерживаться следующих принципов:

1. Максимизации индекса РИИ и минимизации индекса ВРА.
2. Обеспечения условий оптимальности по Парето, т.е. такого состояния системы защиты, при котором значение каждого частного критерия, описывающего ее состояние, не может быть улучшено без ухудшения положения других элементов.

Преобразуем выражения (6) и (8) к следующему виду:

$$\text{РИИ} = \frac{\text{ГОП} \cdot \text{ПЭК}}{\text{ЗК}} - 1 \quad (9)$$

$$\text{ВРА} = \frac{\text{ОВ} \cdot (1 - \text{ПЭК})}{\text{СР}} - 1 \quad (10)$$

$$\text{СР} = \text{ПР}_\text{а} + \text{ДР}_\text{а}, \quad (11)$$

где СР – суммарные постоянные и дополнительные расходы атакующей стороны.

Для простоты и удобства сравнительного исследования систем защиты информации разработан специальный критерий, отражающий требование к максимизации РИИ и минимизации ВРА для каждой i-ой угрозы (атаки):

$$\text{ВРА} = \frac{\text{ОВ} \cdot (1 - \text{ПЭК}) - (\text{ПР}_\text{а} + \text{ДР}_\text{а})}{(\text{ПР}_\text{а} + \text{ДР}_\text{а})}, \quad (12)$$

$$\sqrt{\sum_{i=1}^{n} \text{к}_i \cdot \left(\frac{\text{ВРА}_i}{\text{РИИ}_i}\right)^2} \rightarrow min, \quad (13)$$

Данный критерий позволяет учесть все атаки на информационные системы и оценить вероятность их реализации с помощью весового коэффициента $к_i$.

Значение коэффициента $к_i$ может быть определено методом экспертных оценок, либо на основе статистических данных и (или) значений, рассчитанных с помощью теории вероятностей.

На основе вышеизложенного можно сделать вывод о необходимости построения результативной системы защиты информации и рационального расходования средств организаций на средства по защите информации, которые, в свою очередь, должны соответствовать как техническим, так и экономическим критериям эффективности.

Приведенные в данной работе экономические метрики информационных рисков дают возможность максимизации рентабельности инвестиций в информационную безопасность РИИ и минимизации финансового ущерба.

Модель управления финансовой устойчивостью предприятия с учетом его информационной безопасности.

Обобщая вышесказанное, разработаем модель управления финансовой устойчивостью предприятия в контексте информационной безопасности (рис. 2).

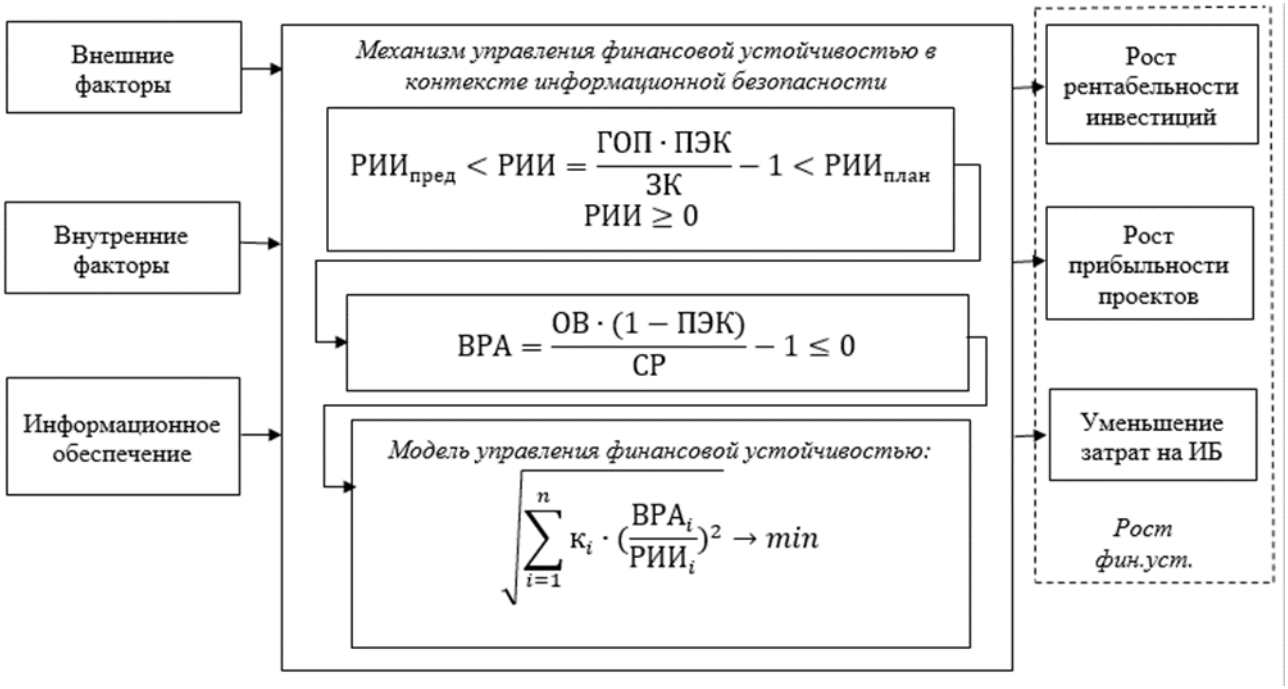

Рисунок 2 – Модель управления финансовой устойчивостью предприятия в контексте информационной безопасности

Формирование и реализация данной методики включает в себя из следующих основных этапов:

1. выявление структурных компонентов финансовой устойчивости предприятия, обоснование причинно-следственных связей между ними;
2. формирование системы показателей для оценки финансовой устойчивости предприятия;
3. управление значениями показателей для обеспечения оптимального уровня финансовой устойчивости предприятия.

Первым этапом является определение структурных компонентов финансовой устойчивости предприятия.

Этот этап содержит в себе теоретическое обоснование предлагаемой модели, точнее, обоснование разработанной системы показателей оценки финансовой устойчивости предприятия. Данный этап был реализован ранее, в процессе исследования термина «финансовая устойчивость предприятия» и выявления основных признаков этого понятия, раскрывающих его экономическую сущность. По итогу исследование показало, что структурную основу финансовой устойчивости предприятия лучше всего рассматривать как комплекс трех важнейших ее составляющих: финансовой стабильности, финансового потенциала, финансовой гибкости. Последнее имеет огромное значение. Финансовая гибкость представляет собой характеристику адаптационных способностей (одна из

важных способностей предприятия– киберустойчивость) функционирования предприятия в условиях нестабильной внешней среды.

Вторым этапом является формирование системы показателей для оценки финансовой устойчивости предприятия.

Система показателей состоит из взаимосвязанных величин, всесторонне отображающих состояние и развитие данного субъекта. Традиционные индикаторы: платёжеспособность, сбалансированность денежных потоков, ликвидность, а также экономические метрики информационной безопасности: ГОП, ОВИ, ОЧВ, РИИ, ВРА, все эти компоненты составляют систему показателей для оценки финансовой устойчивости.

Методологическими требованиями и принципы используют при формировании системы показателей оценки финансовой устойчивости предприятия. Таким образом, выбор показателей основывался на проверке их соответствия следующим основным критериям:

– уместность;

– сопоставимость;

– содержательная взаимосвязь и взаимодополняемость;

– преимущественное использование относительных величин;

– однозначно трактуемый способ расчета;

– возможность проверки и прозрачность;

– эффективность трудозатрат (простота расчетов);

– своевременность и регулярность поступления исходной информации в виде объективных данных бухгалтерской отчетности;

Отличает эту систему показателей то, что она сформирована с учетом не только общих методических требований и принципов, но и полученных результатов исследования теоретических основ финансовой устойчивости предприятия, в частности выделенных и дополненных ее признаков и обоснования структурного содержания, а именно выявленного влияния информационной безопасности на финансовую устойчивость.

Таким образом, положительная динамика указанных показателей будет о росте финансовой устойчивости предприятия с точки зрения приращения прибыльности проектов, рентабельности инвестиций, сокращения затрат на информационную безопасность и финансового ущерба от кибератак, способных генерировать будущие доходы.

Третий этап — это управление значениями показателей для обеспечения оптимального уровня финансовой устойчивости предприятия.

Оценка финансовой устойчивости предприятия должна проводиться регулярно, так как оперативная разработка и реализация управленческих решений позволит достичь и сохранить целевой уровень финансовой устойчивости. Поэтому особую значимость имеет последний, третий этап, заключающийся в интеграции предложенной методики оценки финансовой устойчивости в систему управления финансовой устойчивостью предприятия.

Выводы.

В заключение стоит отметить, что разработанная модель управления финансовой устойчивостью предприятия характеризуется следующими преимуществами:

1. Основу методики составляет не набор, а система показателей оценки финансовой устойчивости предприятия. Эти показатели не противоречат, не дублируют друг друга, не оставляют пробелов в оценке финансовой устойчивости предприятия. Наоборот, в совокупности они обеспечивают формирование целостной картины финансовой устойчивости.
2. Наиболее важным достоинством методики является включение не только статических, но и динамических показателей оценки финансовой гибкости, финансового потенциала, характеризующих способность предприятия в условиях изменяющейся среды бизнеса соблюдать заданную целевую траекторию своего развития.
3. Предложенная методика может быть легко адаптирована к специфике деятельности конкретного предприятия. Оптимальные (нормативные) значения частных показателей оценки финансовой устойчивости самостоятельно устанавливаются руководством компании исходя из экономической стратегии ее развития, финансовой политики, а также с учетом отраслевой специфики бизнеса.

Библиографический список:

1. Шеремет А. Д., Козельцева Е. А. Финансовый анализ: Учебно-методическое пособие. — М.: Экономический факультет МГУ им. М. В. Ломоносова, 2020.
2. Щевьёва В. А., Попов А. В. Влияние инновационной деятельности предприятия на его финансовую устойчивость // Экономика и бизнес: теория и практика, 2018 [Электронный ресурс] // Режим доступа: https://cyberleninka.ru/article/n/vliyanieinnovatsionnoy-deyatelnosti-predpriyatiya-na-egofinansovuyu-ustoychivost/viewer (Дата обращения: 24.05.2022)

3. Потери организаций от киберпреступности // Информационный портал Tadviser [Электронный ресурс] // Режим доступа: https://www.tadviser.ru/index.php/Статья:Потери_организаций_от_киберпреступности (Дата обращения: 04.06.2022)
4. Исследование «Финансовые киберугрозы в 2018 году» // Лаборатория Касперского [Электронный ресурс] // Режим доступа: https://www.kaspersky.ru/about/press-releases/2017_damage-from-cyberattacks (Дата обращения: 07.06.2022)
5. Демарчук, В. В. Перспективы и направления реализации проектов «интеллектуальных» месторождений нефти и газа // Молодой ученый. — 2014. — № 19 (78). — С. 284-289. — Режим доступа: https://moluch.ru/archive/78/13523/ (Дата обращения: 07.06.2022)
6. Старицкая А.К., Романова В.И. Взлом — дело дорогое. Как хакеры экономят на атаках // Новостной портал 360 [Электронный ресурс] // Режим доступа: https://360tv.ru/news/tekst/vzlom-delo-dorogoe/ (Дата обращения: 09.07.2022)