

УДК 338:004.056.5(467)

## **ЦИФРОВАЯ ЗРЕЛОСТЬ И СНИЖЕНИЕ РИСКОВ УТЕЧЕК ИНФОРМАЦИИ КАК ФАКТОР УСТОЙЧИВОГО РАЗВИТИЯ НАЦИОНАЛЬНОЙ ЭКОНОМИКИ**

**Яскевич Д. А., магистрант,**

**Мрочко А. А., магистрант**

*Научный руководитель – канд. экон. наук, доцент Лебедева С. О.*

*Белорусский государственный экономический университет*

*Минск, Республика Беларусь*

**Аннотация.** Исследуются экономические последствия утечек информации в условиях цифровизации с применением факторной модели ущерба и методика SIRI. Реализованный подход снижает риски и формирует стратегии цифровой трансформации организаций.

**Ключевые слова:** цифровая трансформация, цифровая зрелость, утечки информации, экономический ущерб, риски.

В условиях цифровизации устойчивое развитие национальной экономики во многом определяется способностью организаций к цифровой трансформации. Она охватывает не только внедрение технологий, но и переосмысление бизнес-моделей, организационных структур и процессов управления, формируя основу для повышения конкурентоспособности и устойчивости хозяйственной системы в целом.

Ключевым индикатором готовности организаций к таким изменениям выступает цифровая зрелость – способность системно использовать цифровые инструменты для повышения эффективности, гибкости и снижения рисков, включая утечки информации. Высокий уровень цифровой зрелости означает переход от отдельных инициатив к комплексной стратегии, охватывающей процессы, технологии и человеческий капитал. Это обеспечивает рост производительности и снижение уязвимости, что в совокупности укрепляет устойчивость национальной экономики.

Среди инструментов оценки цифровой зрелости особое место занимает методика Smart Industry Readiness Index (SIRI). Она позволяет не только выявлять уязвимости организаций по трем ключевым измерениям (процессы, технологии и организация), но и формировать ре-

комендации по их устранению [1]. При этом особое внимание уделяется информационной безопасности, поскольку именно она определяет устойчивость бизнеса и его способность минимизировать риски.

Одним из наиболее значимых рисков цифровой трансформации остаются утечки информации. Масштаб проблемы подтверждают усредненные показатели: по данным IBM (2023), средняя стоимость инцидента достигает 4,455 млн долл. США в год, а ущерб на одну запись (минимальную учетную единицу информации, потеря или компрометация которой учитывается при расчете стоимости утечки) – 165 долл. США [2]. Даже относительно небольшие утечки способны привести к серьезным финансовым и репутационным потерям, подрывая устойчивость организаций и, в совокупности, национальной экономики.

Реализация рекомендаций, основанных на методике SIRI, демонстрирует, что устранение уязвимостей в управлении данными и процессами обеспечивает значимый эффект. Так, в организации Pepperl+Fuchs цифровизация и внедрение инструментов планирования повысили производительность на 5–10 % и укрепили устойчивость цепочки поставок почти на 50 %, в том числе за счет повышения прозрачности и управляемости потоков данных. Аналогичные результаты достигнуты в Haier, где использование платформы COSMOPlat в сочетании с технологиями 5G и edge computing увеличило точность выявления дефектов на 15 % и эффективность контроля качества на 20%, одновременно снизив риски утечек информации благодаря автоматизации и анализу данных в реальном времени.

Для того чтобы наглядно показать, каким образом цифровая зрелость и реализуемые меры влияют на снижение ущерба от утечек информации, была предложена авторская мультипликативная модель:

$$C = R \cdot V \cdot P \quad (1)$$

где  $C$  – совокупный ущерб от утечки информации (долл. США);

$R$  – количество записей, которые могут быть скомпрометированы (ед.);

$V$  – доля записей, реально подверженных риску утечки (%);

$P$  – стоимость ущерба на одну запись (долл. США).

В табл. 1 показаны значения факторов модели ущерба в базовом периоде и после реализации рекомендаций, основанных на методике SIRI.

Таблица 1 – Анализ динамики факторов модели ущерба до и после внедрения рекомендаций

Показатель	Базовый период	Отчетный период	Абс. откл.	Отн. откл. (%)
R (шт.)	27 000	25 000	–2 000	–7,41
V (%)	100	70	–30	–30
P (долл. США)	165	100	–65	–39,39
C (тыс. долл. США)	4 455	1 750	–2 705	–60,72

*Примечание.* Источник: собственная разработка на основе [2].

Данные таблицы отражают усредненный эффект применения методики SIRI для выявления и устранения уязвимостей в управлении данными. Сопоставление базового и фактического периодов показывает, что совокупный ущерб от утечек информации может быть сокращен более чем на 60 % за счет уменьшения объема затронутых записей, снижения их уязвимости и сокращения средней стоимости ущерба на запись.

Для уточнения вклада каждого из факторов в итоговое снижение совокупного ущерба проведем факторный анализ методом абсолютных разниц. Таким образом, уменьшение ущерба произошло вследствие:

– изменения количества записей, которые могут быть скомпрометированы;

$$C_{\Delta R} = (25000 - 27000) \cdot 100\% \cdot 165 = -330000 \text{ (долл. США)} \quad (2)$$

– изменения доли записей, реально подверженных риску утечки;

$$C_{\Delta V} = 25000 \cdot (70\% - 100\%) \cdot 165 = -1237500 \text{ (долл. США)} \quad (3)$$

– изменения стоимости ущерба на одну запись;

$$C_{\Delta P} = 25000 \cdot 70\% \cdot (100 - 165) = -1137500 \text{ (долл. США)} \quad (4)$$

Совокупный ущерб от утечки информации:

$$C = -330000 - 1237500 - 1137500 = -2705000 \text{ (долл. США)} \quad (5)$$

Совокупный ущерб от утечек информации сократился с 4,455 млн долл. США в базовом периоде до 1,75 млн долл. США после внедрения рекомендаций по методике SIRI, что соответствует снижению на 2,705 млн долл. США (-60,7 %). Данный результат обеспечен за счет: уменьшения числа потенциально скомпрометированных записей на 7,41 % (330 тыс. долл. США), сокращения их уязвимости на 30 п. п. (1,2375 млн долл. США) и снижения средней стоимости ущерба на запись на 39,39 % (1,1375 млн долл. США).

Сокращение количества потенциально скомпрометированных записей стало результатом внедрения практик управления жизненным циклом данных и инструментов Attack Surface Management (ASM), что позволило ограничить объем информации, вовлекаемой в инциденты, и снизить совокупный ущерб на 330 тыс. долл. США.

Уменьшение доли данных, подверженных риску утечки, обеспечила интеграция DevSecOps-подхода, систем управления уязвимостями и threat intelligence, что сократило доступность информации для компрометации и дало наибольший эффект – экономии в 1,2375 млн долл. США.

Применение Security AI, автоматизации и регулярного тестирования планов реагирования на инциденты позволило ускорить обнаружение и локализацию утечек, снизить затраты на уведомления и расследования, что уменьшило среднюю стоимость ущерба на запись и обеспечило экономию порядка 1,1375 млн долл. США. Эти результаты демонстрируют, что повышение цифровой зрелости в целом оказывает комплексное воздействие, тем самым не только снижая вероятность инцидентов, но и уменьшая их экономические последствия.

Проведенное исследование подтвердило, что использование факторной модели позволяет не только количественно оценить совокупный ущерб от утечек информации, но и определить вклад отдельных факторов в его сокращение. Сравнительный анализ показал: комплексное воздействие на объем вовлекаемых данных, уровень их уязвимости и стоимость ущерба на запись обеспечивает снижение совокупных потерь более чем на 60 %. Наибольший эффект дало уменьшение доли уязвимых данных (1,2375 млн долл. США), далее снижение стоимости ущерба на запись (1,1375 млн долл. США) и сокращение объема вовлекаемой информации (0,33 млн долл. США).

Ключевое значение имеет применение методики SIRI, которая выступает универсальным инструментом оценки цифровой зрелости

и позволяет увязать ее уровень с экономическими результатами в сфере информационной безопасности. Внедрение практик DevSecOps, управления уязвимостями, автоматизации реагирования и использования Security AI демонстрирует, что рост цифровой зрелости напрямую снижает риски и финансовые последствия инцидентов.

Таким образом, методология SIRI может рассматриваться не только как средство диагностики цифровой зрелости организаций, но и как основа для формирования стратегий цифровой трансформации. Их реализация способствует укреплению устойчивости и конкурентоспособности организаций, что в совокупности повышает устойчивость национальной экономики в условиях цифровизации.

### **Список использованных источников**

1. The Global Smart Industry Readiness Index Initiative: Manufacturing Transformation Insights Report 2022 : white paper / World Economic Forum ; in collab. with Singapore Economic Development Board. – Geneva : World Economic Forum, 2022. – 37 p.

2. Cost of a Data Breach Report 2023 : research study / IBM Security ; conducted by Ponemon Institute. – Armonk, NY : IBM Corp., 2023. – 52 p.