A. P. Batsula, A. I. Kuralenko, Y. V. Kopolovets, M. M. Sablin

Modeling of Information Security Strategic Planning Methods and Expert Assessments

Keywords: SWOT-analysis, threats, information security

The article, paper addresses problem of increasing the level of information security. As a result, a method of increasing the level of information security is developed through its modeling of strategic planning SWOT-analysis using expert assessments.

А. П. Бацула, А. И. Кураленко, Ю. В. Кополовец, М. С. Саблин

МОДЕЛИРОВАНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МЕТОДОМ СТРАТЕГИЧЕСКОГО ПЛАНИРОВАНИЯ И ЭКСПЕРТНЫХ ОЦЕНОК

В настоящее время стабильная работа организации зависит от множества параметров, начиная от корректного подбора персонала и заканчивая разработкой эффективной стратегии работы предприятия, которая содержит в себе множество составляющих. Одной из таких составляющих является информационная безопасность (ИБ). Для оценки и обеспечения требуемого уровня информационной безопасности необходимо разработать эффективную модель ИБ [1], которая должна учитывать все возможные изменения ситуации во внешней и внутренней среде организации. На основании такой модели можно будет обеспечить высокий уровень эффективности ИБ в организации, а также построить долгосрочную стратегию ИБ.

В данной работе предлагается в качестве метода моделирования ИБ использовать SWOT-анализ и метод экспертных оценок [2]. SWOT – метод стратегического моделирования, используемый для оценки факторов и явлений, влияющих на объект. Все факторы и явления объединяются в четыре критерия:

- сильные стороны (Strengths) – преимущества деятельности;
- слабости (Weaknesses) – недостатки деятельности;
- возможности (Opportunities) – факторы внешней среды, использование которых создаст преимущества для этой деятельности;
- угрозы (Threats) – факторы, которые могут потенциально затруднить деятельность.

SWOT-анализ позволяет установить связь между данными составляющими, для чего их необходимо выделить[3].

Приведем пример построения списка категорий SWOT-анализа (таблица 1).

Таблица 1. Списки категорий SWOT-анализа

Сильные стороны: - наличие сертифицированных средств защиты информации; - подбор высококвалифицированного персонала.	Слабые стороны: - отсутствие опыта применения на практике доступных технологий; - отсутствие системы контроля управления доступом.
Возможности: - повышение квалификации персонала; - закупка нового оборудования.	Угрозы: - возможен съем информации по техническим каналам утечки данных; - подкуп сотрудников.

Общая методология проведения анализа, применяемая на практике, состоит в следующем:

· составление списков перечисленных категорий SWOT-анализа;

· построение матрицы SWOT (таблица 2);

· построение матрицы оценки критериев (таблицы 3, 4).

Таблица 2. Матрица SWOT

	Возможности (1…n)	Угрозы (1…n)
Сильные стороны (1…n)	«СИВ»	«СИУ»
Слабые стороны (1…n)	«СЛВ»	«СЛУ»

В результате построения матрицы образуются четыре поля:

· сильные стороны и возможности;

· сильные стороны и угрозы;

· слабые стороны и возможности;

· слабые стороны и угрозы.

Для разработки эффективной стратегии информационной безопасности организации необходимо рассматривать все возможные парные комбинации данных полей.

Если в результате рассмотрения были выбраны пары из поля «Сильные стороны и возможности», разработка стратегии должна учитывать использование сильных сторон организации для того, чтобы получить отдачу от возможностей, которые появились во внешней среде. Для пар из поля «Сильные стороны и угрозы» стратегия предполагает использования сильных сторон для противодействия угрозам. Для пар из поля «Слабые стороны и возможности» стратегия описывает компенсацию слабых сторон организации за счет появившейся во внешней среде возможности. Для пар из поля «Слабые стороны и угрозы» стратегия должна содержать в себе метод или способ устранения слабой стороны организации и устранения угрозы.

Чтобы оценить такой критерий, как «Возможности», строится матрица, которая позиционирует каждую отдельно взятую возможность (таблица 3).

Таблица 3. Матрица оценки критерия «Возможности»

	Сильное влияние	Умеренное влияние	Малое влияние
Высокая вероятность	«ВС»	«ВУ»	«ВМ»
Средняя вероятность	«СС»	«СУ»	«СМ»
Малая вероятность	«НС»	«НУ»	«НМ»

В результате построения матриц возможности, попадающие в поля, имеющие наибольшую значимость, такие как «ВС», «ВУ» и «СС», рекомендуются к обязательному использованию, остальные возможности, попадающие в поля «СУ», «НУ» и «НМ», не обязательны для использования.

Аналогично составляется и матрица для оценки угроз (таблица 4).

Таблица 4. Матрица оценки критерия «Угрозы»

	Разрушение	Критическое состояние	Тяжелое состояние	«Легкие ушибы»
Высокая вероятность	«ВР»	«ВК»	«ВТ»	«ВЛ»
Средняя вероятность	«СР»	«СК»	«СТ»	«СЛ»
Малая вероятность	«НР»	«НК»	«НТ»	«МЛ»

Угрозы, представляющие наибольшую опасность для организации, относятся к полям «ВР», «ВК» и «СР» и требуют немедленного принятия мер по их устранению. Угрозы, которые относятся к полям «ВТ», «СК» и «НР», также должны быть устранены в первую очередь. Угрозы, попавшие в поля «НК», «СТ» и «ВЛ», должны быть нейтрализованы в порядке приоритета.

Как и любая методология, SWOT-анализ имеет свои преимущества и недостатки. К преимуществам относятся:

· простота концепции SWOT-анализа;

· возможность определить актуальные угрозы ИБ, зная данные о уязвимостях и мерах защиты;

· возможности обобщить и сопоставить информацию совершенно разного характера;

· четкая классификация по определенным критериям;

· свободный выбор анализируемых элементов в зависимости от поставленных целей;

· возможность адаптировать концепцию к объекту исследования любого уровня и на любом этапе обследования объекта.

К недостаткам этого метода относятся:

· результаты данного неформализованного метода представляются в виде качественного описания, что затрудняет его использование в процессе мониторинга;

· SWOT-анализ представляет собой лишь один из способов систематизировать уже существующие знания. Если эти знания неверны или их слишком мало, то и результаты анализа будут иметь небольшую ценность;

· оценка возможностей и угроз — это всего лишь оценка с определенной долей вероятности. Возможен вариант, когда ожидания будут завышены, а угрозы недооценены, так как SWOT-анализ не учитывает возможные риски.

В результате изучения недостатков SWOT-анализа был сделан вывод, что большинство из них носит довольно субъективный характер, потому что при проведении SWOT-анализа используются мнение и компетентность людей, проводящих данный анализ.

Для устранения субъективизма целесообразно использовать метод экспертных оценок. Метод экспертных оценок — это метод организации работы со специалистами-экспертами и обработки мнений экспертов, выраженных в количественной и/или качественной форме с целью подготовки информации для принятия решений лицами, принимающими решения. Для проведения экспертизы создают рабочую группу, которая и организует деятельность экспертов, объединенных (формально или по существу) в экспертную группу (подробно о методе экспертных оценок сказано в [4, 5]).

Для того чтобы показать применимость SWOT на практике, так как аналогия стратегического планирования и информационной безопасности требует серьезного обоснования, проведем сравнение методологии SWOT со следующими классическими работами [6, 7].

В этих работах особое место занимают вопросы теоретических основ обеспечения ИБ. В них рассматриваются обобщенные модели ИБ, в которых делается попытка одновременно охватить все возможные факторы, влияющие на систему защиты.

Авторы работ приводят обобщенную модель системы защиты информации. В ней защищенность информации определяется рядом показателей, которые, в свою очередь, определяются параметрами системы и внешней среды. Вся совокупность параметров, определяющих значения показателей защищенности информации, в общем случае разделяется на три вида:

· управляемые параметры, то есть такие, значения которых полностью формируются системой защиты информации;

· параметры, недоступные для такого однозначного и прямого управления, — как параметры первого вида, но на которые система защиты может оказывать некоторое воздействие;

· параметры внешней среды, на которые система защиты информации никаким образом воздействовать не может.

Анализ обобщенной модели представлен в [7]. Приведенная модель в принципе позволяет решать все задачи моделирования систем и процессов защиты информации. Однако чтобы воспользоваться этой обобщенной моделью, должны быть известны функциональные зависимости значений показателей защищенности от всех параметров и зависимость самих параметров от объемов ресурсов, вкладываемых в обеспечиваемые ими процессы.

Недостатком модели является слабая проработка формальных сторон модели, так как на практике из-за отсутствия необходимых статистических данных не удается вывести формальные выражения, связывающие блоки модели. Следовательно, рассмотренная модель может применяться только в совокупности с неформальными методами анализа и прогнозирования. Далее сравним SWOT и обобщенную модель, о которой говорилось ранее.

Таблица 5. Сравнение методологии SWOT и обобщенной модели

Критерии сравнения	SWOT-анализ	Обобщенная модель
Простота, трудоемкость	Метод очень прост, но для реализации должны использоваться либо хорошие статистические данные, либо компетентные эксперты	Метод содержит расчет, для которого должны быть известны значения показателей защищенности или статистические данные либо для проведения которого должны быть использованы компетентные эксперты
Применимость	Возможно построение модели ИБ, а также определение актуальных угроз	Возможно построение модели ИБ, определение уязвимостей системы
Входные данные	Используются внутренние и внешние параметры, возможности, угрозы	Параметры системы и внешней среды (множество параметров внешней среды, оказывающих влияние на функционирование системы; множество ресурсов системы, участвующих в обработке защищаемой информации; множество внутренних параметров системы, которыми можно управлять непосредственно в процессе обработки защищаемых данных; множество внутренних параметров системы, не поддающихся непосредственному управлению, но поддающихся воздействию; множество средств и ресурсов текущего управления; множество средств и ресурсов воздействия; множество общих ресурсов управления)
Выходные данные	Определяются угрозы и возможности (меры), которые должны быть реализованы в первую очередь для достижения результата	Множество показателей защищенности (уязвимости) информации, возможность определить основные меры

Расчет вероятности угроз и уязвимостей	Только экспертным путем	Только экспертным путем

Сравнение методологии SWOT-анализа с обобщенной моделью ИБ (таблица 5) показывает, что SWOT-анализ позволяет получить на выходе результаты, аналогичные обобщенной модели, но затребовав куда меньше входных параметров и затратив меньше времени. Так, например, для того чтобы определить результаты матрицы оценки критерия «Угрозы», надо произвести куда меньше расчетов, чем в обобщенной модели. С другой стороны, знание большего числа входных параметров, если это возможно, в результате даст большую точность модели, поэтому выбор модели зависит от конкретной цели, времени и ресурсов моделирования.

Минусом обоих методов является отсутствие необходимых входных статистических данных, поэтому эффективность обоих методов будет зависеть от компетентности и умений экспертов, занимающихся моделированием.

В целом SWOT-анализ может применяться для построения моделей и систем защиты, о чем говорится в работах [8, 9].

СПИСОК ЛИТЕРАТУРЫ:

1. *Петренко С. А., Симонов С. В.* Управление информационными рисками. Экономически оправданная безопасность. М.: Компания АйТи. ДМК Пресс, 2004. — 384 с.
2. *Домарев В. В.* Безопасность информационных технологий. Системный подход. К.: ООО «ТИД ДС», 2004. — 992 с.
3. *Виханский О. С.* Стратегическое управление: Учебник. 2-е изд. М.: Гадарики, 2000. — 296 с.
4. *Панкова Л. А., Петровский А. М., Шнейдерман Н. В.* Организация экспертизы и анализ экспертной информации. М.: Наука, 1984. — 214 с.
5. *Бешелев С. Д.* Математико-статистические методы экспертных оценок. М.: Статистика, 1974. — 159 с.
6. *Малюк А. А.* Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. пособие для вузов. М.: Горячая линия-Телеком, 2004. — 280 с.
7. *Герасименко В. А.* Основы защиты информации. М.: Изд-во МИФИ, 1997. — 537 с.
8. *Мицель А. А., Шелупанов А. А., Ерохин С. С.* Модель стратегического анализа информационной безопасности // Доклады ТУСУР. 2007. № 2 (16). С. 3441.
9. *Кураленко А. И., Бацула А. П.,* Построение системы обеспечения безопасности информации методом стратегического планирования. Труды Северо-Кавказского филиала Московского технического университета связи и информатики. Ростов-на-Дону.: ПЦ «Университет» СКФ МТУСИ, 2013. С. 319—321.

REFERENCES:

1. *Petrenko A. S., Simonov S. V.* Upravlenie informacionnymi riskami. Economicheski oprafdannaya bezopasnost'. M. Kompania AiTi, DMK Press, 2004. — 384 p.
2. *Domarev V. V.* Bezopasnost' informacionyh tehnologiy. Sistemnyi podhod. K.: "TTI DS" Ltd, 2004. — 992 p.
3. *Vihanskyi O. S.* Strategicheskoe upravlenie: Uchebnik. 2-e izd. M: Gadariki, 2000.
4. *Pankova L. A., Petrovskyi A. M., Sheiderman N. V.* Organizachia ekspertizy b analiz expertnoi informachii. M.: Nauka, 1984. — 214 p.
5. *Beshelev S. D.* Matematiko-statisticheskie metody expertnyh ocenok. M.: Statistika, 1974. — 159 p.
6. *Maluk A. A.* Informacionnaya bezopasnost': konceptual"nye I metodologicheskie osnovy zachity informacii. Ucheb. posobie dly vuzov. M: Goryachaya liniya — Telekom, 2004. — 280 p.
7. *Gerasimenko V. A.* Osnovy zachity informacii. M.: Izd-vo MIFI, 1997. — 537 p.
8. *Micel' A. A., Shelupanov A. A., Erohin S. S.* Model' strategicheskogo analiza informacionnoi bezopasnosti. Jurnal «Doklady TUSUR». 2007. №2 (16). P. 34—41.
9. *Kuralenko A. I., Batsula A. P.* Postroenie sistemy obespecheniya bezopasnosti informacii metodom strategicheskogo planirovaniya. Trudy Severo-Kavkazskogo filiala Moskovskogo tehnicheskogo universiteta I svyazi I informatiki. Rostov-na-Donu.: PC «Universitet» SKF MTUSI, 2013. P. 319—321.