**Информационная безопасность как процесс управления рисками**

Е.В. Комлева, Кольский научный центр РАН, Д.В. Баранов

**Введение**

Большинство предприятий тратят на безопасность продукта своей деятельности определенный фиксированный процент прибыли. Часть вложенных на безопасность средств в этот продукт не возвращается в виде прибыли. Можно видеть, что безопасность это не продукт, а процесс. Поэтому для решения подобной проблемы можно посмотреть на безопасность как на управление рисками. Цель управления рисками заключается в балансе рисков для деятельности предприятия, снижая потенциальные угрозы. Необходимость в методе управления рисками, который бы позволил точно и надежно измерять параметры безопасности продукта и получать максимальную отдачу средств, вложенных на его безопасность, по-прежнему велика [1].

**Компоненты информационной безопасности.**

Информационная безопасности включает три компонента: требования, политику и механизмы. Требования определяют цели безопасности. Они отвечают на вопрос, – «Что вы ожидаете от вашей безопасности?». Политика определяет значение безопасности. Она отвечает на вопрос, - «Какие шаги вы должны предпринять в достижении целей поставленных выше?». Механизмы предопределяют политику. Они отвечают на вопрос, - «Какие инструменты, процедуры и другие пути вы используете, чтобы гарантировать то, что шаги предопределенные выше будут выполнены?» [2].

Управление рисками Многие лидирующие предприятия и индустриальные сектора видят управление рисками как новый подход к управлению информационной безопасностью. Управление рисками должно помочь им в количественном определении вероятности опасности, оценить степень возможных убытков и взвесить затраты на безопасность против их ожидаемой эффективности [3].

Управление рисками должно дать ответ на следующие вопросы:

1 На сколько улучшилась безопасность предприятия в текущем году?

2 Что предприятие получило за деньги, потраченные на безопасность?

3 На какой уровень безопасности предприятие должно ориентироваться?

Для ответа на эти вопросы требуется строгое определение параметров безопасности и структуры управления рисками.

Можно выделить четыре наиболее важных момента в управлении рисками предприятия:

1 Недолговечность информационного актива. Предприятия и большинство промышленных отраслей понимают, что эффективность их работы зависит от информации. Каждый известный случай критического искажения, повреждения или разрушения информации усиливает их опасения по этому пункту.

2 Доказуемая безопасность. Так как параметры безопасности не всегда имеют оценку, предприятия не способны измерить стабильность или эффективность при выборе различных средств безопасности. Следовательно, количество средств, которое можно потратить на улучшение безопасности не известно.

3 Обоснование стоимости. Повышение стоимости решений и средств безопасности приводит к тому, что проекты информационной безопасности конкурируют с другими инфраструктурными проектами предприятия. Прибыльно-стоимостной анализ и расчет средств возвращаемых в инвестиции становятся стандартными требованиями для любых проектов по информационной безопасности.

4 Ответственность. С ростом предприятий их зависимость от рисков информационной безопасности возрастает. Необходим надежный механизм для управления этими рисками. Для оценивания информационной безопасности прибыльно-стоимостного анализа и расчета 58 средств возвращаемых в инвестиции не достаточно. До сих пор нет метода, позволяющего наиболее достоверно статистически представить параметры информационной безопасности.

A. Что измерять В решениях требующих баланса стоимости контрмер против стоимости риска, важным моментом является точность пунктов любых сделанных измерений [4].

Любой руководитель предприятия в оценивании безопасности желает получить ответы на такие вопросы как:

• Насколько предприятие информационно безопасно?

• Получило ли прибыль предприятие с введением системы оценивания рисков в этом году по сравнению с прошлым?

• Какую выбрать стратегию информационной безопасности?

• Правильное ли количество денег тратится на информационную безопасность?

• Существуют ли альтернативы управления рисками?

В отличие от экономических оценок, где всегда имеются исходные данные, оценивание информационной безопасности почти всегда приходится начинать с нуля. Это, как правило, слабо структурированная задача с постоянно изменяющимися параметрами.

B. Данные для оценивания Какие данные должны быть собраны? Все данные, которые могут быть измерены или имеют какую-то размерность.

Список измеряемых параметров может включать:

• Опасные дефекты приложений, связанные со стадией разработки.

• Уязвимость сети, даже если обнаруживается только при сканировании, а также • Отношение числа пользовательских сессий к числу подозрительных действий.

• Взлом пароля с использованием автоматизированных средств.

• Попытки внедрения инфицированных объектов в систему безопасности.

• Обновление используемых или стоимость новых более защищенных приложений.

• Сканирование сети на входящую и исходящую информацию.

• Затраты при отказе средств защиты.

Конечно, это не полный список. Каждое предприятие должно выбирать свой собственный уровень достаточности информационной безопасности. И на этом фоне проводить сбор данных для дальнейшего оценивания. Так как реальные угрозы почти всегда внутри предприятия, то достаточный уровень безопасности обычно определяется тем, кто контролирует внутренние информационные показатели.

C. Модель данных Решения, связанные с вопросами оценивания безопасности, часто принимаются в условиях неопределенности. В таких условиях всегда существует недостаток данных. Стандартным подходом в построении модели является использование экспертного мнения для дополнения данных. Далее с появлением новых данных мы можем обновлять, модернизировать или калибровать модель, а также возможно полное замещение экспертного мнения.

D. Отчеты по оцениванию информационной безопасности Какие отчеты должны быть представлены при проведении оценивания информационной безопасности?

Некоторые могут включать:

• Временной анализ тенденций.

59 • Представление полученных параметров и финансовый анализ.

• Уменьшенные либо принятые риски.

Основная проблема оценивания информационной безопасности заключается в отсутствии полноты данных [5]. Но полнота информации может складываться из тех фактов, которые предоставляют, например, антивирусные программы, файлы отчетов, системы сканирования и отчеты по безопасности от сотрудников. Таким образом, необходимы критерии оценивания и методы анализа.

Заключение С усложнением информационных технологий предприятия сталкиваются все с более сложными информационными рисками. Если бы была возможность обнаружить и определить уязвимость безопасности в процессе создания продукта деятельности, то оправданы ли будут затраты на разработку таких методов?

Многие предприятия тонут в потоке данных. В большинстве случаев, имеющееся количество фактов, позволяет получать необходимую информацию по оцениванию информационной безопасности. Но проблема в том, что не всегда и не все могут получать эту информацию. Решением этой задачи является механизм, который позволит анализировать факты и, выделяя необходимую информацию оценивать ее, преобразуя в знания о безопасности.

**Список литературы**

1. Geer D., Hoo K., Jaquith A. Information Security: Why the Future Belongs to the Quants / IEEE Security & Privacy Vol. 1, No. 4; July/August 2003, pp. 24-32.

2. Bishop M. What Is Computer Security? / IEEE Security & Privacy Vol. 1, No. 1; January/February 2003, pp. 67-69.

3. Boehm B., Turner R. Using Risk to Balance Agile and Plan-Driven Methods / IEEE Computer Vol. 36, No. 6; June 2003, pp. 57-66.

4. Geer D. Risk Management Is Still Where the Money Is / IEEE Computer Vol. 36, No. 12; December 2003, pp. 129-131.

5. Gliedman C. Managing IT Risk with Portfolio Management Thinking / CIO (Analyst Corner),www.cio.com/analyst/012502\_giga.html.