ОБЩАЯ КОНЦЕПЦИЯ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ФИРМЫ

НИКОЛАЕНКОВА Д.А. , студ.; рук. БАЛЛОД Б.А., ктн, доц.(ИГЭУ)

Предлагается общая концепция мониторинга информационной безопасности предприятия, которая совершенствует традиционный алгоритм управления рисками информационной безопасности путем исследования их динамики. Концепция реализована в ЗАО «Ивановоискож».

На сегодняшний день многие фирмы неизбежно сталкиваются с проблемой необходимости защиты ценного информационного ресурса предприятия (ЦИР). Традиционно защита ЦИР сводится к покупке и внедрению дорогостоящих средств защиты, что отрицательно влияет на бюджет организации и в то же время не обеспечивает обнаружения и предотвращения совершения противоправных действий по отношению к ЦИР.

Также в большинстве случаев на предприятиях не проводится мониторинг угроз ЦИР, прироста ЦИР и эволюции его уязвимостей. Данное обстоятельство приводит к увеличению вероятностей реализации угроз и уязвимостей ЦИР, увеличивает общий вероятный ущерб предприятию и потенциально грозит сокращению общей прибыли.

Вопрос решается при помощи использования общей концепции мониторинга информационной безопасности фирмы, которую можно представить следующими положениями:

1. Определение составляющих ЦИР и их категорирование по величине возможного ущерба *Sj* ЦИР (или стоимости ЦИР) с учетом нарушения требований доступности, целостности и конфиденциальности, где *j* – порядковый номер категории ЦИР.

2. Определение вероятности реализации возможных угроз *Pi* и степени уязвимости ЦИР *Pij* в условиях действующей системы защиты (СЗ) ЦИР, где *i* – порядковый номер угрозы.

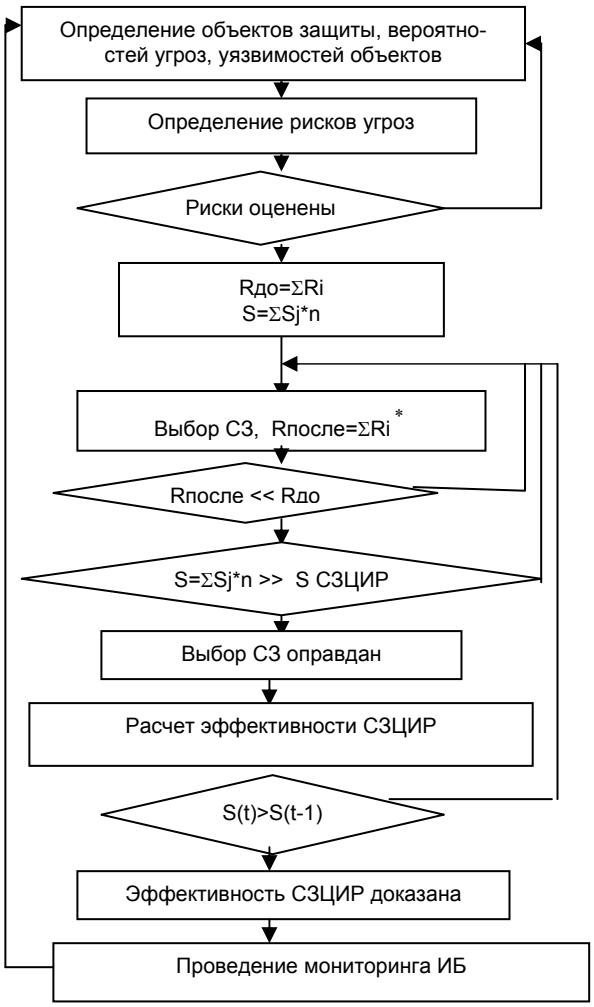
3. Определение рисков угроз категориям ЦИР: $Ri = Pi*Pij*Sj$. Определение суммарного риска: $Rдо = \Sigma Ri$. Определение величины общего возможного ущерба $S = \Sigma Sj*n$ по определенной шкале измерения, где *n* – количество ЦИР в *j*-й категории.

4. Выбор средств защиты, которые могут быть направлены на отражение угроз, уменьшение степени уязвимости ЦИР и снижение ущерба. Определение суммарного риска после выбора СЗЦИР: $Rпосле = \Sigma Ri$. Соотнесение *S* со стоимостью СЗЦИР (*CZ*). При выполнении неравенств $Rпосле < Rдо$ и $S > CZ$ выбор СЗЦИР оправдывается.

5. Оценка эффективности СЗЦИР с учетом эволюции ЦИР: $S(t) = S(t–1) – RS(t) – CZ(t) + \Delta S(t)$, где S(t–1) – стоимость ЦИР в момент времени *t–1*; $RS(t)$ – ущерб от реализованных угроз в период времени с *t–1* по *t*; $CZ(t)$ – стоимость СЗЦИР, приобретенных и функционировавших в период времени с *t–1* по *t*; $\Delta S(t)$ – прирост стоимости ЦИР в период времени с *t–1* по *t*. Для оценки эффективности СЗЦИР необходимо сравнить $S(t)$ и $S(t–1)$, при $S(t) > S(t–1)$ СЗЦИР является эффективной. В противном случае необходимо вернуться к шагу 4 данного алгоритма.

7. Проведение мониторинга угроз ЦИР, прироста ЦИР и эволюции его уязвимостей для обновления данных шагов 2 и 3 данного алгоритма. Алгоритм управления рисками представлен на рисунке.

Алгоритм концепции мониторинга ИБ



Алгоритм концепции мониторинга ИБ

Таким образом, использование общей концепции мониторинга информационной безопасности фирмы позволяет совершенствовать алгоритм управления рисками информационной безопасности предприятия.