Zalecenia wymienionej normy, dotyczące metod oceny bezpieczeństwa w zależności od poziomu integralności zabezpieczeń, są podane w tabeli 3.22.

Tabela 3.22. Metody oceny bezpieczeństwa a poziomy integralności

Lp.	Metoda lub technika	SIL 1	SIL 2	SIL 3	SIL 4
1	Kwestionariusze ocen	R	R	R	R
2	Tablice decyzyjne i tablice prawdy	R	R	R	R
3	Miary złożoności programów	R	R	R	R
4	Diagramy przyczynowo-skutkowe (CCD)	R	R	R	R
4a	Analiza drzewa zdarzeń (ETA)	R	R	R	R
5	Analiza drzewa błędów (FTA)	R	R	WR	WR
6	Analiza rodzajów i skutków uszkodzeń (FMEA)	R	R	WR	WR
7	Analiza hazardu i gotowości systemu (HAZOP)	R	R	WR	WR
8	Modele Markowa	R	R	R	WR
9	Schematy blokowe niezawodności	R	R	R	R
10	Symulacja (Monte Carlo)	R	R	R	R

R – rekomendowane, WR – wysoce rekomendowane.

3.5. Zmniejszanie wartości ryzyka[63]

Możliwe reakcje na ryzyko (ang. *risk treatment*) to:

- unikanie ryzyka,
- kontrolowanie ryzyka,
- transfer ryzyka,
- retencja (zatrzymanie) ryzyka.

Wymieniona kolejność jest umotywowana pogarszającym się wskaźnikiem nakładów czasu, wysiłku i kosztów do uzyskanych efektów kolejnych rozwiązań. Unikanie ryzyka[64] pozwala na pełne uwolnienie własnych zasobów bądź procesów od tego ryzyka.

Jeżeli możliwości unikania ryzyka zostały wyczerpane, należy podjąć próbę kontrolowania ryzyka przez:

- *prewencję*, czyli oddziaływanie na możliwość realizacji zagrożenia (przez kontrolowanie podatności);

[63] Inne stosowane w literaturze nazwy tego procesu to *redukcja*, *minimalizowanie* oraz *łagodzenie.*

[64] Na przykład odcięcie pracownikom dostępu do Internetu pozwala na uniknięcie ryzyka m.in. dostępu do agresywnych stron WWW. Podobnie, przejście na system typu Unix pozwala na uniknięcie ataku kodów i programów złośliwych utworzonych dla systemów Windows.

– *minimalizowanie* szkód/strat, czyli oddziaływanie na skutek realizacji zagrożenia; celem jest zmniejszanie wielkości strat w przypadku wykorzystania podatności przez zagrożenie, co oznacza, że działania minimalizujące powinny być opisane w planach odtwarzania ciągłości działania odpowiedniego szczebla (patrz podrozdz. 4.3); oddziaływanie to zwykle sprowadza się do realizacji odpowiednich procedur szybkiego przywracania poprawnego działania systemów teleinformatycznych.

Wobec ryzyka położonego bliżej lewego górnego rogu mapy ryzyka (niskie prawdopodobieństwo zdarzenia, lecz katastrofalny skutek – porównaj rys. 3.10) działania będą najskuteczniejsze i najwydajniejsze w zakresie zmniejszanie PML – zwykle znacznie łatwiej będzie zmniejszyć PML o 1/3 (np. z 3 mln do 2 mln PLN) niż prawdopodobieństwo realizacji zagrożenia zmniejszyć na przykład z 3% do 2%. Powodowane jest to m.in. tym, że są to najczęściej tzw. zdarzenia (zagrożenia) rzadkie, często związane z czynnikami naturalnymi (trzęsienie ziemi, powódź, huragan), na które zwykle nie mamy wpływu.

Z kolei ryzyko leżące blisko prawego dolnego rogu (częste, lecz mało dotkliwe lub dające się dobrze opanować zdarzenia) wymagają zwykle działań zmniejszających prawdopodobieństwo realizacji zagrożenia (oddziaływania na sposób realizacji), gdyż próba zmniejszenia każdej jednostkowej szkody, na przykład z 1000 PLN do 700 PLN, będzie mało skuteczna i jednocześnie bardzo kosztowna. Przykładem takiej mało skutecznej próby zmniejszenia jednostkowej szkody może być rezygnacja ze stosowania oprogramowania antywirusowego na rzecz procedur naprawczych po wykonanym ataku kodu lub programu złośliwego.

Gdy organizacja wyczerpała możliwości kontrolowania ryzyka i jeśli tzw. ryzyko rezydentne (ang. *residual risks*), czyli poziom ryzyka, które pozostało po zastosowaniu wcześniej wspomnianych technik je zmniejszających, jest nadal zbyt wysoki, należy rozważyć przekazanie (transfer) takiego ryzyka lub jego części.

Podstawową zasadą transferu jest dokonywanie go na podmiot, który potrafi ryzykiem zarządzać lepiej niż podmiot, który chce się ryzyka pozbyć. Do form przekazywania ryzyka należy:

– outsourcing tych funkcji organizacji, które są obarczone ryzykiem niewspółmiernie wysokim do wartości dodanej przez te funkcje[65];
– pozostawienie funkcji (procesów, majątku trwałego) w organizacji, a wyprowadzenie samego ryzyka poza organizację – często odbywa się to przez współuczestniczenie partnera zewnętrznego w ryzyku[66];
– ubezpieczenie ryzyka.

[65] Na przykład oddanie w outsourcing administrowania systemami teleinformatycznymi organizacji lub utworzenie centrum zapasowego przetwarzania danych nie przez wybudowanie go z własnych środków finansowych organizacji, lecz skorzystanie z usługi kolokacji lub hostingu.

[66] Na przykład partycypacja finansowa wynajętej firmy ochraniającej obiekty w szkodach kradzieżowych, obowiązek kontrolowania i finansowania ryzyka awarii sprzętu komputerowego przez producenta lub serwisanta itp.