Planowanie informacyjnej ciągłości działania – przegląd standardu NIST SP 800-34

Łukasz BŁASZCZYK, Krzysztof LIDERMAN

Instytut Teleinformatyki i Automatyki WAT,
ul. Gen. S. Kaliskiego 2, 00–908 Warszawa
lukaszblaszczyk@tlen.pl, k.liderman@ita.wat.edu.pl

STRESZCZENIE: Artykuł zawiera przegląd zaleceń amerykańskiego standardu NIST SP 800-34 z zakresu planowania informacyjnej ciągłości działania. Zostały w nim także zamieszczone informacje nt. wytworzonych w ramach pracy dyplomowej narzędzi ułatwiających zastosowanie ww. standardu w organizacji – listy kontrolnej oraz oprogramowania „Ankieter" wspomagających pracę audytora bezpieczeństwa informacji.

SŁOWA KLUCZOWE: informacyjna ciągłość działania, odtwarzanie systemów IT

1. Wstęp

Zapewnianie informacyjnej ciągłości działania jest zwykle utożsamiane tylko z wykonywaniem i przechowywaniem tzw. kopii zapasowych [5] (nazywanych także kopiami bezpieczeństwa) oraz, w razie potrzeby, odtwarzaniem z nich zasobów informacyjnych organizacji. Jest to w istocie problem znacznie bardziej skomplikowany i wymagający znacznie większej wiedzy i nakładów (organizacyjnych, finansowych, pracy ludzkiej itd.) niż zwykłe wykonywanie kopii zapasowych.

Ze względu na biznesowe znaczenie zasobów informacyjnych dla współczesnych organizacji, ich nieraz bardzo dużą objętość oraz ostre wymagania co do dostępności, zapewnianie informacyjnej ciągłości działania, jak każde skomplikowane przedsięwzięcie, wymaga dobrego planowania. Opis planowania tego typu trudno znaleźć w literaturze polskojęzycznej (patrz np. [4], [11]). Plan zapewniania ciągłości działania jest często niedocenianym przez kierownictwo organizacji dokumentem. Dopiero zewnętrzne okoliczności, takie jak: wymogi przepisów prawa, podjęcie współpracy z bardziej w tym zakresie

zaawansowanym partnerem (i próba wyrównania standardów organizacyjnych) czy katastrofa, która dotknęła organizację, są bodźcem do opracowania dokumentów regulujących zagadnienia zapewniania ciągłości działania (w tym informacyjnej) organizacji. Problem, który pojawia się w takim przypadku, to brak jednolitych, ogólnie uznanych wzorców takich dokumentów. Brakuje także (również w literaturze anglojęzycznej) jednolitej terminologii w zakresie nazewnictwa takich planów.

Pewne wytyczne co do ich zawartości można znaleźć w normach i standardach, takich jak normy PN-ISO/IEC-17799 [8], PN-ISO/IEC 24762:2010 [10], BS 25999-1[1] [2], [3] czy standard COBIT[2], ale ostateczna struktura i zawartość wytworzonej dokumentacji może się znacznie różnić w zależności od organizacji. Z wymienionych dokumentów największym uznaniem na świecie w tym zakresie cieszy się brytyjska, dwuczęściowa norma BS 25999. Jednak dla technicznej strony planowania przedsięwzięć związanych z informacyjną ciągłością działania, zdaniem autorów, lepsze są zalecenia zapisane w standardzie NIST (ang. *National Institute of Standards and Technology*) SP 800-34 *Contingency Planning Guide for Federal Information Systems* [6].

NIST jest organizacją, która m.in. opracowuje standardy opisujące wymagania, jakie należy spełnić w celu zapewnienia bezpieczeństwa systemom informacyjnym. Wymagania te są skierowane przede wszystkim do agencji rządowych USA, z wykluczeniem systemów służących bezpieczeństwu narodowemu (dla nich są formułowane inne wymagania). Dopuszczalne jest również wdrożenie zaleceń standardu w organizacjach pozarządowych, a jego wykorzystanie nie podlega ochronie praw autorskich. Co ważne, w odniesieniu do agencji rządowych USA, standard NIST SP 800-34 jest tylko uzupełnieniem zaleceń ministerstwa handlu i w związku z tym nie wolno korzystać z zaleceń standardu, które są sprzeczne z praktykami wprowadzonymi przez to ministerstwo – standard ten nie jest ani dokumentem nadrzędnym nad zaleceniami ministerstwa handlu, ani alternatywą dla takich zaleceń.

Pomimo że SP 800-34 został opracowany dla agencji rządowych USA, jest on opublikowany w sieci Internet i dostępny dla każdego[3], kto zechce się z nim zapoznać. Zdaniem autorów tego artykułu jego podstawową zaletą jest znacznie większy poziom szczegółowości opisu i „inżynierska konkretność”,

[1] W maju 2012 roku została opublikowana, na bazie BS 25999, norma ISO 22301:2012 *Societal security. Business continuity management systems. Requirements* ustanawiająca zbiór międzynarodowych wymogów dotyczących Systemu Zarządzania Ciągłością Działania.

[2] COBIT (ang. *Control Objectives for Information and Related Technology*), obecnie w wersji 5.0 – standard „ładu informatycznego” organizacji ISACA (ang. *Information Systems Audit and Control Association*).

[3] Za darmo (!), co odróżnia go od norm ISO i Polskiego Komitetu Normalizacyjnego. Dostępny pod adresem: http://csrc.nist.gov/publications/PubsSPs.html.

której często brakuje w normach ISO. Dlatego w kolejnych rozdziałach są zaprezentowane przegląd zawartości tego standardu oraz wyniki pewnych prac, dla których stanowił podstawę, a których szczegóły można znaleźć w pracy [1].

2. Przegląd zawartości rozdziałów standardu NIST SP 800-34

Dokument NIST SP 800-34 składa się z pięciu rozdziałów:

1. Wstęp.
2. Informacje organizacyjne.
3. Proces planowania strategii przywracania systemu informatycznego.
4. Przygotowanie planu przywracania systemu informatycznego.
5. Wskazówki odnośnie środków technicznych w planie przywracania systemu informatycznego.

Standard zawiera także dziewięć załączników. Dwa pierwsze załączniki zawierają przykładowe plany przywracania i przykładową analizę wrażliwości procesów biznesowych oraz szablony, które można wykorzystać przy opracowaniu własnych planów i analiz. Do kolejnych załączników należą:

1. Najczęściej zadawane pytania (FAQ).
2. Wskazówki dotyczące postępowania z personelem.
3. Środki bezpieczeństwa stosowane w planowaniu przywracania systemów.
4. Cykl życia procesu rozwoju systemu informatycznego i planów postępowania z systemem w sytuacjach awaryjnych.
5. Słownik.
6. Wyjaśnienie stosowanych skrótów.
7. Wykaz materiałów źródłowych.

W dalszej części niniejszego punktu artykułu znajduje się opis zawartości poszczególnych rozdziałów standardu NIST SP 800-34. W celu ułatwienia porównania fragmentów tego tekstu z treścią standardu, dalej zostanie zastosowana oryginalna numeracja rozdziałów. Dla odróżnienia od numeracji rozdziałów w ramach artykułu, ta numeracja i tytuły są drukowane kursywą.

1. Wstęp (ang. Introduction)

Zawiera definicje planu przywracania działania systemu informatycznego oraz odtwarzania systemu informatycznego. Opisany jest cel powstania dokumentu, jego zakres i struktura oraz do kogo jest on kierowany. Zgodnie z zamieszczonym tam opisem, standard ma wspomagać:

- ocenę systemów informatycznych,
- określenie wymagań dotyczących planu przywracania tych systemów,
- przydzielenie odpowiednich priorytetów poszczególnym działaniom.

Jednocześnie podkreślono odrębność planu przywracania od (planu) strategii zapewniającej kontynuowanie misji. Oba plany, jak i wiele innych, są częścią strategii zarządzania kryzysowego. Plan przywracania dotyczy jednak wyłącznie systemów informatycznych, które mogą wspomagać realizację procesów biznesowych, ale nie są jedynym elementem gwarantującym poprawne funkcjonowanie organizacji. W związku z tym, zastosowanie się do procedur wyszczególnionych w planie przywracania będzie skutkowało dostępnością sprawnej infrastruktury teleinformatycznej, jednak nie gwarantuje, że organizacja, w której wdrożono plan, będzie mogła realizować swoje zadania.

W standardzie wyodrębniono plany dla trzech typów systemów:

1. Klient-serwer.
2. Systemów telekomunikacyjnych.
3. Systemów typu mainframe.

Standard jest adresowany m.in. do kierowników odpowiedzialnych za nadzór nad procesami, których realizacja jest zależna od systemów informatycznych używanych w organizacji, inżynierów i architektów systemowych, którzy projektują, wdrażają i modyfikują systemy oraz administratorów i ludzi odpowiedzialnych za bezpieczeństwo systemów informatycznych w firmie.

2. Informacje podstawowe (ang. Background)

W tym rozdziale wyjaśniono kilka podstawowych pojęć związanych z bezpieczeństwem teleinformatycznym organizacji oraz umieszczono spis i krótkie definicje poszczególnych typów planów. Opisane jest pojęcie odporności systemu jako zdolność dostosowywania systemu do zmian sytuacji zachodzących w jego otoczeniu i przywracania jego sprawności, o ile zmiany te miałyby negatywny wpływ na jego działanie. Sam proces przygotowania planu przywracania rozpoczyna się od przygotowania polityki przywracania i przeprowadzenia analizy zależności procesów biznesowych od danego systemu teleinformatycznego. Wyniki analizy są pomocne przy nadawaniu elementom systemu priorytetów, które określają kolejność przywracania, zgodnie z zasadą minimalizacji potencjalnych strat powstałych w wyniku zajścia sytuacji awaryjnej.

Plan przywracania systemu jest częścią większej całości, jaką jest program zarządzania ryzykiem, bezpieczeństwem i przygotowaniem organizacji na sytuacje awaryjne. Z całym programem związanych jest wiele różnych planów, które należy przygotować, aby mógł on zostać sprawnie zrealizowany.

3. Proces planowania strategii przywracania systemu informatycznego (ang. Information System Contingency Planning Process)

W rozdziale trzecim opisano proces przygotowania i utrzymania planu przywracania. Całość została podzielona na siedem etapów:

1. Przygotowanie polityki organizacji odnośnie postępowania w sytuacjach awaryjnych.
2. Przeprowadzenie analizy wrażliwości zadań realizowanych przez organizację na awarie systemów informatycznych wspomagających ich wykonanie (BIA – ang. *Business Impact Analysis*).
3. Identyfikacja przydatnych środków bezpieczeństwa.
4. Przygotowanie strategii przywracania.
5. Przygotowanie planu przywracania dla systemów informatycznych.
6. Przygotowanie planu testów, szkoleń i ćwiczeń.
7. Przygotowanie planu utrzymania wdrożonych planów przywracania.

Cały proces przygotowania planu przywracania, opisany w tej części standardu, dotyczy działań jednakowych dla wszystkich rodzajów systemów informatycznych. Elementy unikatowe dla różnych architektur systemów opisano w rozdziale piątym. Rozdział trzeci zawiera opis sześciu, spośród siedmiu, wyszczególnionych wcześniej etapów. Przygotowaniu właściwego planu przywracania (etap piąty na liście) systemów informatycznych przeznaczono osobny, czwarty rozdział.

3.1. Przygotowanie dokumentu polityki odnośnie postępowania w sytuacjach awaryjnych

Przygotowanie planu przywracania systemu informatycznego należy rozpocząć od spisania dokumentu, w którym zostanie postawiony cel, jaki powinien zostać osiągnięty w wyniku realizacji procedur planu przywracania. Cel ten nadaje kierunek dalszym pracom podczas definiowania czynności do wykonania w sytuacji awaryjnej. Czynności te powinny być spójne, realizowane w odpowiedniej kolejności i dawać jasno określone skutki.

W dokumencie polityki należy też określić strukturę organizacyjną zespołu, który będzie realizował zdefiniowany plan. Konieczne jest przypisanie członkom zespołu funkcji, jakie będą pełnić oraz zakresu obowiązków. Ponadto dokument powinien zawierać wymagania dotyczące zasobów niezbędnych do realizacji planu, a także realizacji szkoleń i ćwiczeń, harmonogram utrzymania planu oraz minimalną częstość wykonywania kopii zapasowych danych przetwarzanych w systemie.

W standardzie FIPS 199 określono warunki, na podstawie których dzieli się systemy informatyczne ze względu na poziom wrażliwości procesów biznesowych realizowanych w organizacji przez nie wspieranych. Standard ten definiuje trzy klasy systemów: niskiego, średniego i wysokiego znaczenia.

Polityka przywracania musi uwzględniać klasę systemu, do którego się odnosi oraz zastosowanie środków bezpieczeństwa związanych z klasą tego systemu.

3.2. Analiza wrażliwości procesów biznesowych

W treści standardu NIST SP 800-34 ten etap został określony jako kluczowy dla przygotowania planu przywracania. Jego zadaniem jest identyfikacja elementów systemu informatycznego, misji i procesów biznesowych realizowanych w organizacji oraz zależności pomiędzy nimi. W procesie analizy pod uwagę bierze się wyłącznie procesy biznesowe wspierane przez określony system informatyczny. Należy uwzględnić wpływ niedostępności systemu na procesy wraz z dopuszczalnym czasem niedostępności[4].

Częścią analizy wrażliwości jest ocena, jakie zasoby w postaci sprzętu, oprogramowania, zapasowych danych, personelu, a nawet zaplecza lokalowego są konieczne do możliwie szybkiego przywrócenia pełnej sprawności informacyjnej organizacji.

Ostatnim etapem analizy jest przypisanie poszczególnym elementom systemu priorytetów informujących o kolejności ich przywracania po awarii. Nadany elementowi priorytet zależy od znaczenia tego elementu dla działalności organizacji i jest rezultatem oceny wyników otrzymanych we wcześniejszych etapach analizy.

W tym rozdziale są zdefiniowane także trzy parametry służące do określenia dopuszczalnego czasu niedostępności elementu systemu. Do wspomnianych parametrów należą:

- maksymalny dopuszczalny czas niedostępności (MTD – ang. *Maximum Tolerable Downtime*) – czas niedostępności usług, który zarząd organizacji jest w stanie zaakceptować;
- dopuszczalna długość czasu przywracania (RTO – ang. *Recovery Time Objective*) – maksymalny czas awarii elementu systemu, w którym niedostępność tego elementu nie wpływa negatywnie na inne zasoby systemowe;
- punkt przywrócenia systemu (RPO – ang. *Recovery Point Objective*) – określa ostatni przed awarią, możliwy do odtworzenia, stan systemu.

Zdefiniowanie wymienionych parametrów ma pomóc w wyborze środków służących przywracaniu systemu informatycznego oraz określeniu stanu, do jakiego chcemy przywrócić system, zanim sytuacja i czas pozwolą na całkowite odtworzenie systemu.

[4] Jest on określony jako maksymalny czas, w którym awaria nie będzie miała negatywnego wpływu na możliwość realizacji misji przez organizację.

3.3. Identyfikacja środków bezpieczeństwa

W rozdziale wskazano środki bezpieczeństwa, które mogą przyczynić się do zmniejszenia strat spowodowanych niedostępnością elementów sytemu informatycznego. Do wspomnianych elementów należą m.in.:

- urządzenia podtrzymywania zasilania (UPS),
- spalinowe generatory prądu,
- detektory dymu i ognia,
- czujniki wody w pomieszczeniach ze sprzętem komputerowym,
- instalacje przeciwpożarowe,
- regularnie wykonywane i właściwie przechowywane kopie zapasowe,
- odpowiednio przygotowane miejsca poza firmą, służące do przechowywania kopii zapasowych, danych w postaci nieelektronicznej oraz dokumentacji systemu.

W celu dokładnego zapoznania się z sugerowaną listą środków bezpieczeństwa, standard NIST SP 800-34 odwołuje się do dokumentu NIST SP 800-53 [7], w którym te środki są opisane, z uwzględnieniem ich przydatności dla różnych systemów, w zależności od typu i konfiguracji[5].

3.4. Opracowanie strategii przywracania

W tej części dokumentu są opisane zagadnienia dotyczące wykonania kopii zapasowych i ich przechowywania, zapewnienia zapasowych elementów systemu w razie konieczności wymiany oraz przygotowania miejsc, w których można tymczasowo skonfigurować i uruchomić system zapasowy[6].

Strategia przywracania powinna określać następujące składowe:

- minimalną częstość wykonywania kopii zapasowych,
- zasoby danych, z których kopie należy wykonać,
- format, w jakim będą zapisywane nośniki z danymi zapasowymi.

Jeżeli dopuszcza się przechowywanie takich danych poza siedzibą organizacji, należy określić sposób transportu nośników tych danych do miejsca składowania. Cały proces kopiowania danych, ich opisu i przygotowania do transportu odbywa się w siedzibie organizacji. Jednostka przechowująca kopie zapasowe jest odpowiedzialna jedynie za ich składowanie oraz dostarczenie, w razie potrzeby we wskazane miejsce.

[5] Ze sformułowań znajdujących się na początku paragrafu 3.3, dotyczącego środków bezpieczeństwa, można wnioskować, że ich zastosowanie nie jest obligatoryjne i ich użycie należy rozważyć w kontekście kosztów poniesionych na montaż i eksploatację oraz ewentualnych korzyści z tego płynących.

[6] W sytuacji, gdy lokalizacja, w której dotychczas pracował system, w wyniku katastrofy lub awarii stała się niedostępna lub nie spełnia wymogów koniecznych do dalszego funkcjonowania systemu.

Przed podjęciem decyzji o składowaniu danych poza organizacją i wybraniu miejsca składowania zaleca się rozważenie kilku czynników:

- kosztów;
- wielkości prawdopodobieństwa, że obszar, na którym znajduje się składnica danych zostanie dotknięty tą samą katastrofą, przed której skutkami staramy się zabezpieczyć dany system (wybór odpowiedniego położenia geograficznego zapasowego magazynu danych)[7];
- warunków (temperatura, wilgotność, środki ochrony technicznej w miejscu składowania), w jakich składowane są nośniki;
- bezpieczeństwa składowanych nośników z danymi, w tym metod transportu, zaufania do personelu mającego dostęp do nośników itp.

Standard przewiduje trzy sposoby zapewnienia potrzebnych do odtworzenia systemu elementów zapasowych:

1. Umowy z dostawcami sprzętu – powinny jasno określać czas, w jakim dostawca zobowiązuje się dostarczyć potrzebny sprzęt lub oprogramowanie, określać priorytet takiego zamówienia nad zamówieniami „regularnymi", nie związanymi z sytuacjami awaryjnymi oraz kolejność, w jakiej będą realizowane zamówienia organizacji, gdyby skutki awarii lub katastrofy dotknęły więcej niż jednego z klientów tego samego dostawcy.
2. Własne zapasy sprzętu przechowywane poza głównym miejscem instalacji chronionego systemu. Z jednej strony daje to możliwość prawie natychmiastowej wymiany uszkodzonych elementów, z drugiej – wymaga ponoszenia wydatków na sprzęt, który być może nigdy nie zostanie użyty, zanim konieczna będzie jego wymiana w związku z rozwojem technologii.
3. Użycie podobnego sprzętu, który wykorzystywany jest na co dzień do innych celów przez inną jednostkę tej samej organizacji.

Strategia przywracania powinna zawierać także wytyczne co do zapasowych lokalizacji, w których można uruchomić tymczasowo system. Organizacja może takie miejsce przygotować samodzielnie w celu użycia go w sytuacji awaryjnej. Inną możliwością jest uzyskanie dostępu do takiego miejsca w sytuacji awaryjnej dzięki zawarciu wzajemnego porozumienia z inną jednostką tej samej organizacji, organizacją zewnętrzną lub wynajęcie odpowiedniego obiektu.

Pod względem stopnia przygotowania lokalizacji zapasowej dla systemu, dzielą się one na tzw. „zimne", „ciepłe" i „gorące". Lokalizacja „zimna" jest to pusty obiekt o odpowiedniej powierzchni i infrastrukturze technicznej, takiej jak źródła zasilania, łącza telekomunikacyjne czy środki ochrony technicznej, w którym można zainstalować i skonfigurować system informatyczny.

[7] Nie może to być jednak zbyt odległy teren, bo zapasowe dane trzeba dostarczyć w określonym czasie zespołowi zajmującemu się przywracaniem systemu.

Lokalizacja „ciepła” jest to częściowo wyposażona powierzchnia biurowa, w której na stałe znajdują się elementy systemu (który ma być przywracany w razie awarii), odpowiednie oprogramowanie i sprzęt telekomunikacyjny. Natomiast lokalizacja „gorąca” jest to lokalizacja, która zawiera zainstalowany i skonfigurowany system wraz z całą wymaganą do jego funkcjonowania infrastrukturą i personelem.

Jeśli zapasowa przestrzeń jest wynajmowana od wyspecjalizowanego dostawcy, wówczas wszystkie wymagania dotyczące wynajmowanej lokalizacji i dostępu do niej muszą być dokładnie sprecyzowane w umowie. Dotyczy to m.in. wymagań dotyczących bezpieczeństwa, dostępnego sprzętu komputerowego i telekomunikacyjnego, ilości czasu, w którym można przeprowadzać testy oraz czasu użytkowania powierzchni w trakcie zaistnienia właściwej sytuacji awaryjnej. W warunkach umowy należy także uwzględnić sytuację, gdy z tej samej powierzchni oferowanej przez dostawcę zmuszona jest skorzystać w tym samym czasie więcej niż jedna organizacja – w standardzie NIST SP 800-34 przewiduje się sytuację, w której wynajmujący podpisze umowę z kilkoma organizacjami. Dopuszcza się także możliwość podpisania wzajemnej umowy z innymi organizacjami, które użytkują takie same lub podobne systemy, zobowiązującej do użyczenia zasobów swojego systemu na czas trwania awarii ich własnych systemów. Należy pamiętać, aby przy definiowaniu warunków takiej umowy nie dopuścić do możliwości przeciążenia własnego systemu, który będzie musiał przez pewien czas realizować funkcje obcej organizacji[8].

Oprócz kwestii technicznych i umów związanych z dostępem do środków technicznych wspomagających realizację planu przywracania, standard NIST SP 800-34 zaleca, aby w strategii przywracania zaplanowane były koszty związane z realizacją planu. Niedopuszczalna jest sytuacja, gdy koszty realizacji przygotowanego planu przywracania przekraczają możliwości finansowe przedsiębiorstwa, ponieważ czyni to plan bezużytecznym, a organizacja staje się bezradna w sytuacji awaryjnej. Koszty przedstawione w strategii przywracania powinny uwzględniać wszelkie wydatki, począwszy od kosztów zapasowego sprzętu i oprogramowania, kosztów przygotowania kopii zapasowych danych, kosztów transportu i wynagrodzeń dla członków zespołów kryzysowych, aż do kosztów testów, szkoleń i ćwiczeń.

Według standardu NIST SP 800-34 ostatnim elementem strategii przywracania jest wyznaczenie zespołów, które będą realizować opracowany plan przywracania w sytuacji awaryjnej oraz przypisanie tym zespołom właściwych zadań. Zaproponowano funkcje, jakie poszczególne zespoły

[8] W standardzie NIST SP 800-34 określono zestaw elementów, których zdefiniowanie w umowach wzajemnych lub umowach z dostawcami sprzętu i firmami wynajmującymi powierzchnie alternatywne zostało określone jako absolutne minimum.

powinny spełniać (np. zespół kierowniczy, zespół odzyskiwania baz danych, systemów operacyjnych, zespół testowy, zespół odpowiedzialny za transport, zespół kontaktów z mediami, zespół prawny itd.). Nie ma jednak wymogu, aby strategia przywracania każdego systemu uwzględniała każdy z takich zespołów. Wybór, które z zespołów będą powołane, zależy od struktury organizacji oraz wrażliwości procesów biznesowych na awarię systemu (zgodnie ze standardem FIPS 199), którego plan przywracania dotyczy.

Członkowie poszczególnych zespołów powinni być dobierani według swoich codziennych obowiązków, aby w pracy w zespole „kryzysowym" mogli wykorzystać swoją wiedzę i doświadczenie. Liczność zespołów powinna być dobrana tak, aby zespół był w stanie wykonać swoje zadanie, nawet jeśli nie wszyscy jego członkowie mogliby dotrzeć na miejsce akcji.

3.5. Plan testów, szkoleń i ćwiczeń

Samo przygotowanie planu przywracania nie gwarantuje jego skuteczności. Standard zaleca okresowe testy planu, szkolenia personelu i ćwiczenia w przeprowadzaniu planu. Po każdym takim przedsięwzięciu należy udokumentować wyniki i na ich podstawie wprowadzić ewentualne zmiany w planie przywracania. Wprowadzając zmiany w planie przywracania, zawsze należy uwzględnić zmiany w systemie, a także zmiany organizacyjne, jakie zaszły od opracowania planu lub od ostatniego przeprowadzonego ćwiczenia/testu.

Testowanie planu przywracania ma na celu wykrycie jego niedostatków. Należy przetestować procedury przywracania dotyczące każdego z elementów systemu. W standardzie NIST SP 800-34 wymieniono procedury, które trzeba umieścić w planie testów: powiadamianie, odzyskiwanie systemu z kopii zapasowych, sprawdzenie wydajności systemu pracującego na sprzęcie zapasowym, przywrócenie normalnego działania systemu. Plan testów powinien zawierać datę przeprowadzenia każdego z testów oraz listę uczestników biorących udział w testach.

W trakcie szkoleń personel zespołów (kryzysowych) zdobywa wiedzę o swoich obowiązkach w realizacji planu przywracania oraz nabywa umiejętności niezbędne do skutecznego przeprowadzenia tego planu. W NIST SP 800-34 zaleca się szkolenia przynajmniej raz w roku.

W standardzie sugeruje się dwa rodzaje ćwiczeń – teoretyczne i praktyczne. Ćwiczenie teoretyczne ogranicza się do dyskusji członków zespołów kryzysowych, sprawdzenia znajomości obowiązków i procedur zapisanych w planie przywracania. Takie dyskusje zawsze są prowadzone w odniesieniu do przedstawionego na początku ćwiczenia scenariusza sytuacji awaryjnej. W trakcie ćwiczeń praktycznych uczestnicy wykonują swoje zadania w sztucznym środowisku, ale tak jakby sytuacja awaryjna rzeczywiście miała

miejsce. Zakres takich ćwiczeń należy dobrać odpowiednio do stopnia zależności funkcjonowania firmy od sprawności danego systemu. Zakres ten może obejmować tylko niektóre elementy planu, jak np. procedury powiadamiania, kontakt z dostawcami i przywracanie systemu z kopii zapasowych, lub możne obejmować pełny plan, łącznie z relokacją całego systemu w miejsce zapasowe.

3.6. Utrzymanie planu przywracania

Plan przywracania powinien być regularnie aktualizowany, żeby odzwierciedlał rzeczywisty stan, strukturę i potrzeby systemu, którego dotyczy i organizacji, w której jest wdrożony. Należy sprawdzać aktualność m.in.: wymagań bezpieczeństwa, procedur technicznych, wymagań na sprzęt (typ, ilość), danych kontaktowych członków zespołów kryzysowych i osób kontaktowych ze strony firm zewnętrznych wspierających w jakikolwiek sposób proces przywracania (np. dostawcy sprzętu).

Plan przywracania zawiera dane personalne oraz może zawierać informacje wrażliwe. Dlatego należy zwrócić szczególną uwagę na sposób dystrybucji i przechowywania planu. Plan powinien zostać udostępniony wyłącznie osobom upoważnionym zgodnie z zasadą „wiedzy koniecznej". Dodatkowo należy utworzyć spis osób, które otrzymały egzemplarz planu.

4. Opracowanie dokumentu planu przywracania systemu informatycznego (ang. Information System Contingency Plan Development)

W czwartym rozdziale NIST SP 800-34 zostało opisanych pięć elementów, każdy w osobnym podrozdziale, składających się na właściwy plan przywracania.

4.1. Informacje pomocnicze

Ta część dokumentu jest wstępem przedstawiającym założenia planu przywracania i zawiera informacje, które mają ułatwić posługiwanie się nim. Można się z niej dowiedzieć „co zawiera plan" oraz jakie inne uzupełniające plany są z nim powiązane.

W części ogólnej wskazuje się, jakich rezultatów oczekuje się po wykonaniu tego planu oraz podaje zakres dokumentu i założenia, jakie zostały przyjęte podczas jego tworzenia. Zakres jest określany poziomem wpływu awarii systemu, którego dotyczy plan, na działanie organizacji (zgodnie ze standardem FIPS 199) wraz z przyjętym dopuszczalnym czasem wykonania procedury przywracania (RTO). W części opisującej założenia planu należy także zamieścić listę sytuacji, w których nie należy stosować danego planu. Przykładowe założenia i listę sytuacji zamieszczono w dodatku A standardu NIST SP 800-34.

Druga część informuje, że w kolejnych rozdziałach znajdują się następujące informacje:

- opis przywracanego systemu (architektura, umiejscowienie, rysunki techniczne z elementami składowymi systemu),
- opis trzech faz składających się na plan przywracania (aktywacja i powiadamianie, odzyskiwanie, przywrócenie wszystkich funkcji),
- zarys struktury zespołów kryzysowych i ich odpowiedzialności, a także sposób koordynacji pracy poszczególnych zespołów.

4.2. Faza aktywacji planu i powiadamiania

Celem tej fazy jest powiadomienie członków zespołów kryzysowych o zaistniałej sytuacji i ocena skutków awarii. Inicjuje się ją po wystąpieniu awarii lub wykryciu zdarzeń mogących do awarii doprowadzić. Dla każdego systemu definiuje się kryteria aktywacji planu, które powinny być opisane w polityce przywracania. Zespół dokonujący oceny sytuacji określa, jakie czynności należy podjąć i na tej podstawie zapada decyzja, które z zespołów kryzysowych będą potrzebne do przywrócenia działania systemu.

W tej części planu precyzuje się sposoby informowania personelu zespołów kryzysowych w standardowych godzinach pracy oraz poza nimi. Uwzględnia się też sytuację, gdy któryś z potrzebnych zespołów (lub jego członków) nie odpowiada na wezwanie. Plan przywracania zawiera listę członków poszczególnych zespołów, z uwzględnieniem ich stanowiska w zespole i wszelkich informacji kontaktowych.

Standard NIST SP 800-34 określa, jakie informacje powinny się znaleźć w wysłanym komunikacie, ale konkretny zestaw tych informacji jest dobierany odpowiednio do zaistniałej sytuacji awaryjnej. Oprócz członków wybranych zespołów kryzysowych, powiadomienia powinny być też wysłane do osób kontaktowych ze współpracujących firm zewnętrznych (np. klientów lub partnerów biznesowych), jeśli tylko awaria opisywanego systemu może mieć negatywny wpływ na działanie ich systemów.

Ocena sytuacji dokonywana na początku procesu aktywacji ma pomóc w podjęciu właściwej decyzji co do dalszego działania – podstawą jest określenie charakteru awarii i jej rozmiaru. Procedury służące ocenie sytuacji należy przygotować indywidualnie dla każdego systemu, jednak standard NIST SP 800-34 wyszczególnia, jakie elementy należy uwzględnić jako absolutne minimum procesu oceny.

Do wspomnianych elementów należą:

- przyczyna awarii,
- możliwość pojawienia się dodatkowych uszkodzeń,
- stan infrastruktury technicznej,
- stan funkcjonalny urządzeń systemu,
- rodzaj powstałych uszkodzeń,
- elementy wymagające wymiany,
- oszacowanie czasu potrzebnego na przywrócenie pełnego działania.

4.3. Faza odzyskiwania

W fazie odzyskiwania wykonuje się podstawowe procedury spisane w planie. Celem jest przywrócenie działania systemu (dopuszcza się przywrócenie w lokalizacji zapasowej) oraz usunięcie uszkodzeń. Standard zaleca, aby do tej fazy przypisać wyłącznie działania o wysokim priorytecie.

Kolejność odzyskiwania poszczególnych funkcji systemu powinna być ułożona z uwzględnieniem priorytetów tych funkcji oraz ich maksymalnego dopuszczalnego czasu niedostępności (MTD). Jeśli przywracanie systemu ma odbyć się w lokalizacji zapasowej, wówczas w planie należy wskazać zespół lub konkretne osoby, które będą odpowiedzialne za zorganizowanie transportu elementów systemu i/lub zakup elementów brakujących.

Plan przywracania powinien zawierać dokładne procedury, a efekt ich wykonania powinien być jasno określony dla systemu lub jego elementów[9]. Ułatwia to decyzję o zakończeniu realizacji jednego etapu odzyskiwania i przejściu do następnego. Poszczególne procedury powinny być przypisane do wcześniej określonych zespołów kryzysowych i powinny zawierać opisy co najmniej następujących działań:

- zapewnienia uprawnień do dostępu na teren objęty awarią;
- powiadomienia o awarii partnerów biznesowych, których systemy są połączone z systemem uszkodzonym lub są zależne od jego działania;
- zapewnienia odpowiedniego sprzętu i przestrzeni biurowej;
- zapewnienia i instalacji komponentów przywracanego systemu;
- zapewnienia dostępu do kopii zapasowych danych;
- przywrócenia systemu operacyjnego i aplikacji potrzebnych do działania systemu;
- przywrócenia danych systemu do określonego stanu;
- testowania działania systemu wraz z testami zabezpieczeń;
- podłączenia systemu do sieci komputerowej lub zewnętrznego systemu.

[9] Procedury powinny być spisane w konwencji „krok-po-kroku” i nie mogą pozostawiać miejsca na jakiekolwiek niejasności lub przypuszczenia.

4.4. Faza przywracania

Faza przywracania jest to ostatnia część planu przywracania, w której zdefiniowane są czynności mające na celu przetestowanie i zatwierdzenie (dopuszczenie do działania) funkcji przywróconego systemu. Na tym etapie wszystkie procedury odzyskiwania są zakończone, a system działa według zasad sprzed awarii. Przeprowadzony proces przywracania zatwierdza się, gdy zostaną spełnione następujące warunki:

1. System przywrócony działa poprawnie i jest odpowiednio zabezpieczony[10].
2. Wykonano testowanie danych i oceniono, że bazy danych systemu oraz same dane zostały przywrócone poprawnie do ostatniego sprzed awarii, możliwego do odzyskania stanu.
3. Wykonano testowanie funkcji systemu i stwierdzono, że system działa poprawnie i wszystkie swoje zadania realizuje bez błędów.

Po zatwierdzeniu wykonania planu przywracania można przeprowadzić jego dezaktywację. Polega ona na przywróceniu systemu do pracy w jego normalnych warunkach i przygotowaniu się na ewentualne następne sytuacje awaryjne. W trakcie dezaktywacji należy powiadomić użytkowników, według wcześniej określonych procedur, o zakończeniu prac przy przywracaniu funkcji systemu. Trzeba uprzątnąć obszar, na którym były prowadzone prace i rozmontować wszelkie tymczasowe instalacje w lokalizacjach zapasowych oraz zwrócić dokumentację i instrukcje użyte w trakcie realizacji działań w miejsca ich stałego przechowywania. Jeśli w organizacji kopie zapasowe danych przechowuje się poza jej siedzibą, to należy wykorzystane nośniki danych przewieźć z powrotem w miejsce ich składowania.

Po ustąpieniu sytuacji awaryjnej należy sporządzić pełną kopię zapasową odtworzonego systemu, na wypadek wystąpienia awarii w przyszłości. Wszystkie zdarzenia, jakie wystąpiły w trakcie realizacji planu przywracania – przedsięwzięte działania, napotkane problemy itp., powinny zostać udokumentowane i przeanalizowane, a wnioski uwzględnione przy opracowaniu aktualizacji planu przywracania systemu.

4.5. Załączniki do planu przywracania

Ostatnim elementem planu przywracania są załączniki zawierające informacje, które nie znalazły się w treści dokumentu właściwego. Do omawianych załączników należą m.in.:

1. Dane kontaktowe członków zespołów kryzysowych.
2. Dane kontaktowe dostawców i innych kontrahentów, z którymi współpracę przewiduje plan przywracania.

[10] Systemy o identycznych zadaniach powinny pracować jednocześnie w kilku, co najmniej dwóch, oddzielnych lokalizacjach, aż do momentu uzyskania takiego potwierdzenia.

3. Wyniki analizy wrażliwości procesów biznesowych organizacji (BIA).
4. Dokładna treść procedur odzyskiwania.
5. Dokładna treść procedur przeprowadzania testów.
6. Lista niezbędnego sprzętu, elementów systemu, oprogramowania itp.
7. Procedury umożliwiające działanie systemu, przynajmniej w ograniczonym zakresie, podczas wykonywania procedur przywracania.
8. Procedury testowania i utrzymania planu.
9. Informacje o połączeniach (wymianie danych) systemu z innymi systemami.
10. Wszystkie aktualne umowy zawarte z dostawcami i innymi organizacjami, mające zapewnić realizację planu przywracania.

5. *Uwagi dotyczące rozwiązań technicznych (ang. Technical Contingency Planning Considerations)*

W ostatnim rozdziale standardu NIST SP 800-34 opisane są rozwiązania techniczne, które można zastosować w systemach w zależności od ich architektury. Pierwsza część rozdziału opisuje rozwiązania oraz wymagania wspólne dla wszystkich architektur systemów (rodzajów), natomiast każda z kolejnych części odnosi się już do rozwiązań dla konkretnego rodzaju systemu.

Dla każdego systemu należy określić częstość tworzenia kopii zapasowych oraz ich rodzaj, konieczność składowania tych samych danych w kilku miejscach, typ lokalizacji zapasowej dla systemu. Punktem wyjściowym do podjęcia tych decyzji jest analiza BIA. Kopie tych samych danych zaleca się przechowywać na kilku nośnikach jednocześnie, co zapobiega utracie danych w przypadku uszkodzenia jednego z nich, a dane powinny być chronione przed nieuprawnionym dostępem[11].

Standard NIST SP 800-34 określa trzy podstawowe typy kopii zapasowych danych systemu:

1. Kopia pełna – zawiera dokładne odwzorowanie danych (których kopiowanie jest wymagane) z nośnika źródłowego.
2. Kopia przyrostowa – zawiera dane, które zostały utworzone lub uległy zmianie od wykonania ostatniej kopii zapasowej.
3. Kopia różnicowa – zawiera dane utworzone lub zmienione od wykonania ostatniej pełnej kopii zapasowej systemu.

Przy wyborze typu kopii zapasowej danych należy wziąć pod uwagę różne czynniki – w standardzie są wyspecyfikowane m.in.: ilość danych do skopiowania, oprogramowanie używane do kopiowania, wymagany czas życia nośników z kopiami, sposób i miejsce składowania kopii, sposób ich opisu itp.

[11] Jednym z zalecanych sposobów jest szyfrowanie danych. Wiąże się ono jednak z dodatkowymi trudnościami dotyczącymi odpowiedniego zarządzania kluczami szyfrującymi – ich tworzeniem i przechowywaniem oraz zapewnieniem ich dostępności, gdy zajdzie taka potrzeba.

Oprócz samych danych, ochronie powinny podlegać również inne zasoby systemu – jego niesprawność, a co za tym idzie, brak dostępu do danych, może być spowodowana awarią np. jednego z jego elementów sprzętowych systemu[12]. Zabezpieczyć należy też oprogramowanie instalacyjne aplikacji używanych w systemie oraz ich licencje (warunki, numery itp.). Odnośnie do środków ochrony technicznej zaleca się wykorzystanie rozwiązań zgodnych ze standardem NIST SP 800-53.

Jeśli organizacja zdecyduje się na wykorzystanie alternatywnych lokalizacji, to przy wyborze konkretnego obiektu należy kierować się takimi czynnikami, jak położenie, godziny pracy (jeśli obiekt jest zarządzany przez zewnętrzną firmę), ograniczenia dotyczące przechowywania danych (np. dostępna powierzchnia)[13]. Dopuszcza się wykorzystanie dla jednego systemu kilku typów lokalizacji, ze względu na zróżnicowany poziom istotności różnych funkcji realizowanych przez ten system.

Standard NIST SP 800-34 zawiera także opis koncepcji „wysokiej dostępności" systemu (HA – ang. *High Availability*). Jest to rozwiązanie (kosztowne!) oparte na eksploatacji systemu zawierającego nadmiarowe elementy sprzętowe oraz programowe, które mogą przejmować realizację zadania w razie awarii elementu podstawowego.

Dalsza część rozdziału piątego zawiera opisy i rozwiązania dotyczące konkretnych architektur sprzętowych. W przypadku architektury klient-serwer podkreślone zostało znaczenie ochrony danych – dostępności, integralności i poufności danych zarówno po stronie klienta, jak i serwera. Podczas opracowywania planu przywracania dla tego typu systemu należy rozważyć następujące zagadnienia:

- wybór miejsca przechowywania danych zapasowych[14];
- ustandaryzowanie (ujednolicenie) rozwiązań stosowanych w organizacji odnośnie do sprzętu, oprogramowania, urządzeń peryferyjnych[15];
- udokumentowanie konfiguracji systemu i danych o dostawcach, które to informacje mogą być przydatne w trakcie aktywacji planu;
- zgodność rozwiązań z planu przywracania z polityką bezpieczeństwa i środkami bezpieczeństwa systemu (cel – ochrona przed wyciekiem informacji wrażliwych podczas awarii systemu lub w procesie jego przywracania).

[12] Przyczyną awarii systemu może być np. zanik zasilania.

[13] Należy przy tym pamiętać, że wybrany lub własny obiekt zapasowy musi być wyposażony zgodnie ze stopniem ważności hostowanego systemu dla działalności organizacji i wymaganym typem lokalizacji („zimna", „ciepła", „gorąca").

[14] Standard NIST SP 800-34 zaleca dla tej architektury przechowywanie kopii zapasowych danych poza siedzibą główną organizacji.

[15] Zapewnienie kompatybilności urządzeń usprawni proces przywracania i może pomóc w sytuacji braku elementu zapasowego dla przywracanego systemu.

Oprócz powyższych, standard sugeruje uwzględnienie kilku zagadnień dotyczących osobno strony klienta i strony serwera. Dla komputerów klienckich są to następujące zagadnienia:

- ograniczenie przechowywania danych bezpośrednio na komputerach użytkowników – wrażliwe dane powinny być zapisywane na centralnych serwerach, na których przeprowadzana jest regularna archiwizacja;
- zautomatyzowanie procesu tworzenia kopii zapasowych – zainstalowanie oprogramowania, które automatycznie, zgodnie z ustalonym harmonogramem, tworzy kopie zapasowe danych zapisanych w określonym miejscu (folderze);
- poinformowanie użytkowników o folderach, których zawartość jest kopiowana i w razie potrzeby będzie możliwa do odzyskania.

Z kolei dla strony serwerowej systemu należy rozważyć następujące zagadnienia:

- standaryzację sprzętu, oprogramowania i urządzeń peryferyjnych – zapewnia to niższe koszty przywracania, ponieważ zasoby mogą być współdzielone pomiędzy systemami;
- udokumentowanie architektury serwera i konfiguracji jego poszczególnych elementów;
- zgodność zastosowanych rozwiązań z polityką bezpieczeństwa w zakresie bezpieczeństwa sieci i zastosowanie podobnych środków i procedur bezpieczeństwa w celu ochrony danych wrażliwych;
- koordynację zastosowanych rozwiązań z procedurami stosowanymi w przypadku wykrycia incydentu bezpieczeństwa teleinformatycznego.

Jako konkretne rozwiązania do zastosowania w systemie, standard NIST SP 800-34 wymienia stosowanie szyfrowania danych na komputerach klienckich oraz szyfrowanie nośników z danymi zapasowymi, które są przechowywane poza organizacją macierzystą. Pośród sposobów przechowywania kopii zapasowych danych wymienione zostały płyty DVD, dyski sieciowe, zewnętrzne dyski twarde i przechowywanie kopii danych w sieci Internet (usługa komercyjna). Jeśli organizacja posiada wiele serwerów, zalecane jest, aby system przechowywania danych zapasowych z tych serwerów był jeden, wspólny dla wszystkich. Ułatwia to zarządzanie kopiami zapasowymi z danymi. W przypadku gdy organizacja posiada wiele danych, które należy zabezpieczyć, i są one przesyłane w sieci, dobrym rozwiązaniem jest utworzenie osobnej sieci wyłącznie do transferu danych zapasowych. Dzięki temu działalność organizacji nie jest zakłócona przez przeciążenie sieci, z której korzystają pracownicy.

Plan przywracania systemów telekomunikacyjnych powinien uwzględniać te same zagadnienia, które zostały opisane dla architektury klient-serwer, ale bez elementów wyszczególnionych osobno dla klienta i serwera. Ponadto należy zadbać o:

- aktualność schematów fizycznej i logicznej struktury sieci telekomunikacyjnej wraz z urządzeniami spinającymi sieci w całość, adresacją IP, serwerami DNS itp.;
- udokumentowanie konfiguracji urządzeń sieciowych (w celu ułatwienia szybkiej ponownej konfiguracji) oraz danych kontaktowych kontrahentów odpowiedzialnych za dostarczenie elementów systemu w razie awarii;
- zgodność zaplanowanych rozwiązań z polityką bezpieczeństwa sieci.

Z powodu różnic w rozległości i prawach administrowania, sieci LAN i WAN wymagają różnych rozwiązań przygotowanych w planie przywracania. Sieci typu LAN są mniejsze niż sieci WAN i zwykle są całkowicie zarządzane przez pracowników organizacji, w której sieć jest użytkowana. W takiej sieci należy zidentyfikować wszystkie punkty, których uszkodzenie (uszkodzenie okablowania, interferencje elektromagnetyczne i fal radiowych oraz uszkodzenia np. przez wodę lub ogień itp.) lub awaria może wywołać negatywne skutki dla organizacji. Należy, na podstawie wcześniej przeprowadzonej analizy BIA, określić, jakie funkcje są pełnione przez wszystkie urządzenia sieciowe spinające tę sieć w całość i odpowiednio do ich znaczenia przygotować środki zapewniające możliwość korzystania z sieci, nawet jeśli jeden z takich elementów ulegnie awarii.

W sytuacji krytycznej dopuszcza się wykorzystanie przygotowanych wcześniej zdalnych połączeń do wewnętrznej sieci organizacji[16]. Zdalny dostęp do wewnętrznej sieci organizacji należy odpowiednio zabezpieczyć, np. zadbać o odpowiednią weryfikację użytkowników, szyfrowanie danych itp. Także sieci bezprzewodowe mogą być używane podczas przeprowadzania procedur przywracania, jeśli kablowa struktura sieci została uszkodzona. W takim przypadku należy przedsięwziąć szczególne środki ostrożności (przynajmniej zadbać o szyfrowanie danych), transmisja bezprzewodowa jest bowiem łatwa do przechwycenia.

Dla sieci WAN należy uwzględnić wymienione wcześniej elementy (dla architektury klient-serwer i sieci LAN). Dodatkowo należy zadbać o bezpieczeństwo łączy pomiędzy systemami. Kryterium, jakie należy przyjąć przy podejmowaniu decyzji dotyczącej wyboru rozwiązań, jest rodzaj danych przesyłanych w sieci WAN. Jeśli nie są one krytyczne dla funkcjonowania

[16] Aby uzyskać dostęp do jej pełnych zasobów, jeśli np. obszar, na którym znajduje się siedziba organizacji jest niedostępny z powodu wystąpienia na nim katastrofy, a zasoby znajdujące się wewnątrz sieci są potrzebne do przywrócenia sprawności systemów i umożliwienia dalszego działania organizacji.

organizacji, to również poziom zabezpieczeń nie musi być najwyższej klasy. Zwykle należy rozważyć konieczność wystąpienia następujących czynników:

- zapewnienia nadmiarowych łączy w sieci WAN, na wypadek uszkodzenia jednego z nich;
- zawarcia umowy z kilkoma operatorami sieciowymi na dostarczanie usług[17];
- wprowadzenia nadmiarowości użytych urządzeń sieciowych w strukturze sieci, co zabezpiecza sprawność sieci, jeśli jeden z elementów przestanie działać (dodatkowo równoważy obciążenie na poszczególnych łączach sieci).

Ostatnią architekturą systemu opisaną w standardzie NIST SP 800-34 jest architektura typu mainframe. Jest to architektura scentralizowana – wszystkie dane są przechowywane w jednym miejscu. Z tego powodu głównymi problemami, z punktu widzenia ochrony systemu, są dostępność jednostki centralnej systemu i tworzenie kopii zapasowych danych. Należy:

- przechowywać kopie bezpieczeństwa danych poza siedzibą organizacji, w miejscu na tyle odległym, aby zminimalizować prawdopodobieństwo oddziaływania skutków tej samej awarii lub katastrofy na obie lokalizacje;
- odpowiednio dokumentować konfigurację systemu i dane kontaktowe dostawców;
- zapewniać zgodność planu przywracania z polityką bezpieczeństwa opracowaną dla sieci organizacji oraz ze środkami bezpieczeństwa wdrożonymi dla systemu.

Scentralizowany charakter systemu powoduje, że awaria jednego, głównego elementu będzie jednoznaczna z awarią całego systemu. Jego ochrona sprowadza się zatem głównie do zabezpieczenia działania tego właśnie, jednego elementu. Należy więc zadbać o zapasowe, długoterminowe źródło zasilania i UPS-y dla zabezpieczenia systemu przed wahaniami napięcia. Dane składowane w jednostce centralnej powinny być powielane i składowane na różnych nośnikach jednocześnie. Należy też wziąć pod uwagę przygotowanie systemu zapasowego w „ciepłej” lub „gorącej” lokalizacji zastępczej.

3. Lista kontrolna zgodności ze standardem

Na podstawie treści rozdziału piątego standardu NIST SP 800-34 (patrz punkt 2 niniejszego artykułu), w którym znajduje się opis zagadnień, jakie należy wziąć pod uwagę podczas pracy nad przygotowaniem planu

[17] W tym przypadku należy się upewnić, że sieci wybranych operatorów nie mają ani jednego wspólnego punktu.

przywracania, została opracowana lista pytań kontrolnych wspomagających ocenę zgodności opracowania i wdrożenia planu zapewniania ciągłości działania z zaleceniami tego standardu[18]. Fragment takiej ankiety (listy kontrolnej) jest pokazany na rysunku 1. Pełna lista, zawierająca 157 pytań, jest zamieszczona w załączniku do pracy [1].

1. Analiza wpływu awarii systemu na realizację procesów biznesowych (BIA)

Pytania kontrolne:

1. Czy przeprowadzono analizę wpływu awarii systemu na możliwości operacyjne organizacji?
   □ **TAK** □ **NIE** □ **NIE DOTYCZY** □ **UWAGI**

Jeżeli odpowiedź na pytanie 1 brzmi „TAK", to proszę odpowiedzieć na pytania 2-16.

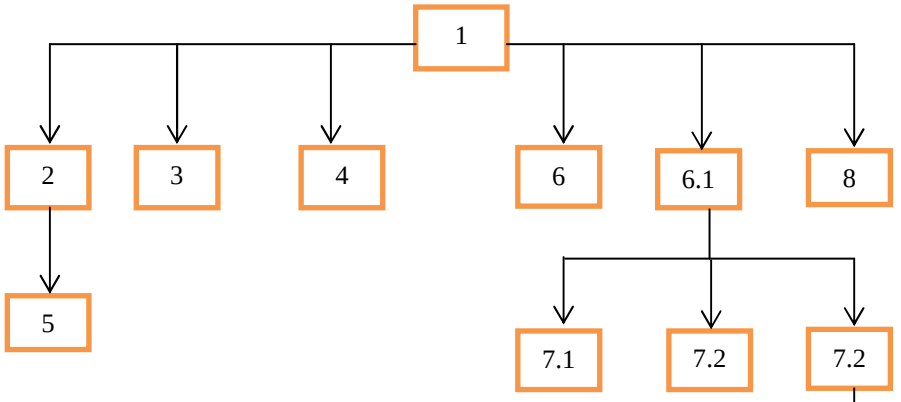
2. Czy jednoznacznie zidentyfikowano poszczególne elementy systemu?
   □ **TAK** □ **NIE** □ **NIE DOTYCZY** □ **UWAGI**
3. Czy jednoznacznie zidentyfikowano niezbędne zadania działalności biznesowej, w których wykorzystuje się system lub jego komponenty?
   □ **TAK** □ **NIE** □ **NIE DOTYCZY** □ **UWAGI**
4. Czy określono skutki braku możliwości realizacji poszczególnych zadań?
   □ **TAK** □ **NIE** □ **NIE DOTYCZY** □ **UWAGI**
5. Czy określono zależność zidentyfikowanych zadań od poszczególnych elementów systemu?
   □ **TAK** □ **NIE** □ **NIE DOTYCZY** □ **UWAGI**
6. Czy określono dopuszczalny czas braku możliwości realizacji dla każdego z zadań?
   □ **TAK** □ **NIE** □ **NIE DOTYCZY** □ **UWAGI**
7. Czy dla każdego z elementów systemu określono czas, po jakim ten element musi ponownie działać?
   □ **TAK** □ **NIE** □ **NIE DOTYCZY** □ **UWAGI**
8. Czy zdefiniowano zasoby potrzebne do przywrócenia sprawności operacyjnej organizacji (np. personel, sprzęt, oprogramowanie)?
   □ **TAK** □ **NIE** □ **NIE DOTYCZY** □ **UWAGI**
9. Czy określono priorytety przywracania poszczególnych elementów lub funkcji systemu?
   □ **TAK** □ **NIE** □ **NIE DOTYCZY** □ **UWAGI**

Rys. 1. Przykładowy fragment listy kontrolnej

[18] Wyjątek stanowią pytania dotyczące analizy wpływu awarii systemu na realizację procesów biznesowych (BIA), które opracowano na podstawie rozdziału 3.2. W rozdziale piątym znajduje się bowiem wyłącznie uzasadnienie przeprowadzenia analizy BIA, natomiast opis elementów składowych takiej analizy zamieszczono właśnie w rozdziale 3.2.

Pytania w tej ankiecie mają charakter zamknięty, tzn. że osoba odpowiadająca na pytania nie ma swobody wypowiedzi i musi się ograniczyć do wyboru odpowiedzi spośród zbioru podanego pod każdym pytaniem. Podczas opracowywania pytań starano się, żeby były one możliwie proste i pozwalały na udzielenie jednoznacznej odpowiedzi. Dlatego na każde z pytań można odpowiedzieć „Tak", „Nie" lub „Nie dotyczy". Na wypadek jednak, gdyby pojawiły się jakieś wątpliwości podczas wypełniania ankiety lub trudno byłoby odnieść wybrane pytanie do badanego systemu, dodano czwartą odpowiedź: „Uwagi". Wybranie tej odpowiedzi oznacza, że ankietowany ma wątpliwości dotyczące pytania i że osoba prowadząca ankietowanie powinna (najczęściej w bezpośredniej rozmowie) te wątpliwości wyjaśnić tak, aby możliwe było udzielenie jednoznacznej odpowiedzi.

Pytania w ankiecie zostały podzielone na zakresy tematyczne (kategorie) odpowiadające poszczególnym podrozdziałom rozdziału piątego standardu. Pomiędzy niektórymi kategoriami istnieją zależności, które należy uwzględnić podczas korzystania z ankiety w procesie oceny. Niektóre z tych zależności są wprost narzucone w treści standardu, inne wynikają z zagadnień poruszanych w pytaniach. Na rysunku 2 przedstawiono schemat korzystania z listy kontrolnej. Ilustruje on zależności pomiędzy kategoriami pytań oraz wskazuje kolejność, w jakiej należy poddawać ocenie poszczególne zagadnienia dotyczące systemu.



LLegenda:

1 – Analiza BIA.
2 – Bezpieczeństwo danych, integralność, kopie zapasowe.
3 – Ochrona zasobów systemu.
4 – Wybór środków bezpieczeństwa.
5 – Wybór miejsca przechowywania kopii zapasowych i uruchomienia systemu zapasowego.
6 – Systemy klient-serwer.
6.1 – Architektura klient-serwer.
7.1 – Systemy telekomunikacyjne.
7.2 – Sieci LAN.
7.3 – Sieci WAN.
8 – Systemy mainframe.

Rys. 2. Schemat korzystania z ankiety na potrzeby audytu zgodności

Numery na diagramie odpowiadają numerom zagadnień w ankiecie, np. numer „1” oznacza analizę BIA. Jest to punkt wyjściowy dla każdego innego zagadnienia, ponieważ podczas tej analizy identyfikuje się elementy systemu, które należy uwzględnić w planie przywracania ze względu na ich znaczenie dla utrzymania informacyjnej ciągłości działania organizacji. Sensowne wydaje się również przeprowadzenie analizy kategorii drugiej, dotyczącej m.in. sporządzania kopii zapasowych przed przystąpieniem do analizy kategorii piątej, w której mowa jest o miejscu przechowywania kopii zapasowych. Jeśli w organizacji nie robi się kopii zapasowych, to pytania o miejsce ich przechowywania można z góry odrzucić. Z drugiej jednak strony w kategorii piątej znajdują się też pytania nie związane z kategorią drugą, dlatego zachowanie wskazanej kolejności nie jest obligatoryjne. Należy to potraktować jako sugestię w celu usprawnienia pracy z ankietą.

Oprócz zależności wynikających z treści pytań, istnieją też zależności pomiędzy kategoriami pytań narzucone przez treść standardu NIST SP 800-34. Podczas oceny systemu telekomunikacyjnego organizacji (kategoria 7), należy także odpowiedzieć na pytania z kategorii 6.1, opisującej zagadnienia ogólne architektury klient-serwer. Z kolei pytania dotyczące sieci LAN (kategoria 7.2) mogą być wykorzystane w dwóch sytuacjach: podczas oceny wdrożenia zabezpieczeń zapewniających informacyjną ciągłość działania w odniesieniu do samej sieci LAN lub w odniesieniu do sieci WAN jako uzupełnienie pytań kategorii 7.3. W drugim przypadku pytania dotyczące sieci LAN powinny być potraktowane jako pytania o badaną sieć WAN. Ocenę zagadnień opisywanych przez pytania, których kategorie według algorytmu nie są ze sobą powiązane można przeprowadzać niezależnie od siebie, w dowolnej kolejności, a nawet współbieżnie (np. przez różnych ankieterów).

Należy zaznaczyć, że NIST SP 800-34 jest standardem amerykańskim i znajdują się w nim odwołania do innych amerykańskich oficjalnych dokumentów, w tym standardów. Przykładem jest standard FIPS 199, do którego co jakiś czas odwołują się autorzy standardu NIST SP 800-34. W ankiecie odwołania do tego typu dokumentów zamieniono na odwołanie do „odpowiednich przepisów prawa”. Ma to uczynić ankietę bardziej uniwersalną, którą można wykorzystać bez względu na kraj, w którym działa organizacja podlegająca ocenie.

4. Narzędzie wspomagające ocenę wdrożenia zaleceń standardu NIST SP 800-34

W celu usprawnienia procesu oceny zgodności, o którym mowa w tym artykule, opracowane zostało specjalne narzędzie programowe „Ankieter”. Jest

to aplikacja internetowa w architekturze klient-serwer, napisana w języku C# z wykorzystaniem technologii ASP.NET4. Podczas pracy nad programem korzystano ze środowiska programistycznego Visual Studio 2010 Ultimate oraz serwera baz danych Microsoft SQL Server 2008 Express Edition[19]. Testy funkcjonalne oprogramowania zostały przeprowadzone bezpośrednio w środowisku deweloperskim. Przeprowadzono również testową instalację programu wraz z bazą danych na serwerze zewnętrznym w celu rzetelnego przygotowania instrukcji ich instalacji do celów użytkowych. Jako serwera aplikacji użyto serwera IIS w wersji 7.5, natomiast bazę danych zainstalowano także w tym przypadku na serwerze SQL Server 2008 Express Edition.

Narzędzie umożliwia dwa sposoby prezentacji wyników ankiet. Pierwszym jest wyświetlenie w postaci tabeli (patrz rysunek 3) pytań wraz z udzielonymi odpowiedziami. Prezentowane wyniki są podzielone według przynależności pytań do kategorii, przy czym użytkownik sam decyduje, wyniki których kategorii chce zobaczyć. Możliwe jest jednoczesne wyświetlenie odpowiedzi kilku kategorii pytań.

Rys. 3. Program „Ankieter" – przykład prezentacji wyników ankietowania

Drugim sposobem prezentacji wyników jest podsumowanie w postaci wykresu słupkowego. Na wykresie każdy słupek odpowiada jednej z możliwych

[19] Jest to darmowy i domyślny serwer dla środowiska VS2010.

odpowiedzi występujących w ankiecie. Wysokość słupka określa ilość pytań, na które udzielono odpowiedzi reprezentowanej przez dany słupek. W przeciwieństwie do metody pierwszej, jednoczesne wybranie kilku kategorii pytań nie powoduje wyświetlenia wykresów dla każdej kategorii z osobna, lecz powoduje sumowanie odpowiedzi ze wszystkich wybranych kategorii i wyświetlenie wyniku na wspólnym wykresie.

Narzędzie ma wbudowane funkcje podstawowe, tj. zapis i przeglądanie udzielonych odpowiedzi na pytania zawarte w elektronicznej ankiecie oraz funkcje zarządcze, takie jak: przydział osoby odpowiedzialnej za opracowanie wniosków z przeprowadzanego ankietowania, przydział ekspertów zajmujących się zadanymi zakresami tematycznymi w ramach zespołu, rejestracja nowych użytkowników narzędzia itd.

5. Podsumowanie

Standard NIST SP 800-34 zawiera propozycję (dla administracji rządowej USA jest to zalecenie) struktury oraz zawartości pewnego dokumentu – planu zapewniania informacyjnej ciągłości działania. W standardzie tym są zdefiniowane i opisane poszczególne etapy takiego przedsięwzięcia (przygotowanie polityki, analiza BIA itd.) oraz wskazane te jego elementy, które powinny być w takim dokumencie zamieszczone. Nie jest to jednak instrukcja, lecz przewodnik wskazujący kierunek, w jakim należy podążać podczas przygotowywania wspomnianego planu. Konkretne rozwiązania techniczne podane w NIST SP 800-34 należy traktować jako przykład, a nie pełną listę możliwości.

W treści standardu dość często znajdują się odniesienia do innych dokumentów, w szczególności do standardów FIPS 199 i NIST SP 800-53. Prace nad planem zapewniania informacyjnej ciągłości działania wymagają również znajomości tych standardów (lub odpowiednich dokumentów krajowych). Pomagają one dobrać odpowiednie rozwiązania tak, aby plan zapewniania informacyjnej ciągłości działania był dobrze opracowany – informacja (i pośrednio system ją przetwarzający i przechowujący) zabezpieczona, ale bez ponoszenia niepotrzebnych kosztów i zgodnie z prawem miejscowym.

Opracowana na podstawie NIST SP 800-34 lista pytań kontrolnych (patrz punkt 3 artykułu) i narzędzie „Ankieter” (patrz punkt 4 artykułu) mogą być przydatne w przedsięwzięciach z zakresu audytu bezpieczeństwa informacyjnego, gdy np. należy ocenić przygotowanie organizacji na katastrofy oddziałujące m.in. na zasoby informacyjne.

Literatura

[1] BŁASZCZYK Ł., *Projekt narzędzia do wspomagania oceny zgodności stosowanych praktyk odtwarzania z wytycznymi standardu NIST SP 800-34*, praca dyplomowa, WAT, Warszawa, 2013.

[2] BS 25999-1: 2006: *Business continuity management. Code of practice*.

[3] BS 25999-2: 2007: *Specification for business continuity management*.

[4] LIDERMAN K., *Bezpieczeństwo informacyjne*, WN PWN, Warszawa, 2012.

[5] NELSON S., *Profesjonalne tworzenie kopii zapasowych i odzyskiwanie danych.* Helion S.A., Gliwice, 2012.

[6] NIST Special Publication 800-34. Rev.1: *Contingency Planning Guide for Federal Information Systems*, May 2010.

[7] NIST Special Publication 800-53: *Recommended Security Controls for Federal Information Systems and Organizations*, 2010.

[8] PN-ISO/IEC-17799:2005: *Technika informatyczna – Praktyczne zasady zarządzania bezpieczeństwem informacji*.

[9] PN-ISO/IEC 27001:2007: *Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania*.

[10] PN-ISO/IEC 24762:2010: *Technika informatyczna – Techniki bezpieczeństwa – Wytyczne dla usług odtwarzania techniki teleinformatycznej po katastrofie*.

[11] ZASKÓRSKI P. (red.), *Zarządzanie organizacją w warunkach ryzyka utraty informacyjnej ciągłości działania*, WAT, Warszawa, 2011.

Contingency planning – NIST SP 800-34 standard review

ABSRACT: The paper is a survey on USA standard NIST SP 800-34 “Contingency Planning Guide for Federal Information Systems”. It also includes some information about tools (developed within an engineering dissertation) supporting a practical application of the standard in an enterprise – a control list and the computer program “Ankieter” for supporting information security auditor.

KEYWORDS: contingency planning, IT recovery

Praca wpłynęła do redakcji: 15.03.2013