# Bezpieczeństwo i optymalizacja procesów realizowanych drogą elektroniczną

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt „Programowa i strukturalna reforma systemu kształcenia na Wydziale Mat-Fiz-Inf".
Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego.

Człowiek-najlepsza inwestycja

UNIWERSYTET MARII CURIE-SKŁODOWSKIEJ
WYDZIAŁ MATEMATYKI, FIZYKI I INFORMATYKI
INSTYTUT INFORMATYKI

# Bezpieczeństwo i optymalizacja procesów realizowanych drogą elektroniczną

Bogdan Księżopolski


LUBLIN 2011

**Instytut Informatyki UMCS**
**Lublin 2011**

Bogdan Księżopolski

# BEZPIECZEŃSTWO I OPTYMALIZACJA PROCESÓW REALIZOWANYCH DROGĄ ELEKTRONICZNĄ

**Recenzent**: Zbigniew Kotulski

**Projekt okładki**: Agnieszka Kuśmierska

Praca współfinansowana ze środków Unii Europejskiej w ramach
Europejskiego Funduszu Społecznego

Publikacja bezpłatna dostępna on-line na stronach
Instytutu Informatyki UMCS: informatyka.umcs.lublin.pl

**Wydawca**
Uniwersytet Marii Curie-Skłodowskiej w Lublinie
Instytut Informatyki
pl. Marii Curie-Skłodowskiej 1, 20-031 Lublin
Redaktor serii: prof. dr hab. Paweł Mikołajczak
www: informatyka.umcs.lublin.pl
email: dyrii@hektor.umcs.lublin.pl

**Druk**
ESUS Agencja Reklamowo-Wydawnicza Tomasz Przybylak
ul. Ratajczaka 26/8
61-815 Poznań
www: www.esus.pl

ISBN: 978-83-62773-07-7

# SPIS TREŚCI



`

# PRZEDMOWA

Zaawansowane technologie teleinformatyczne dają obecnie szerokie możliwości rozwoju przemysłu lub usług świadczonych przez instytucje publiczne. Aktualnie duży nacisk kładziony jest na rozwój powszechnie dostępnych usług informacyjnych nazywanych „e-anything", czyli e-urząd (ang. e-government), e-pieniądze (ang. e-money), e-bankowość (ang. e-banking). Wspomniane procesy realizowane są głównie drogą elektroniczną, dzięki czemu można zwiększyć ich powszechność, jednocześnie zmniejszając koszty.

Wprowadzenie tych usług w praktyce wiąże się z zagwarantowaniem odpowiedniego poziomu ochrony informacji przesyłanych między uczestnikami danej usługi. Wśród technologii teleinformatycznych oraz modułów kryptograficznych są takie, dzięki którym można zadbać o różne usługi ochrony informacji np.: poufność, integralność, niezaprzeczalność, anonimowość danych. Wszelkie działania na danych w obrębie danej usługi elektronicznej zawarte są w protokołach, które je realizują. Jeżeli w protokołach zawarte są moduły kryptograficzne to mówimy o protokołach kryptograficznych.

Istotnym problemem jest określenie poziomu ochrony informacji realizowanych usług w danym protokole. Każdorazowe użycie dowolnej usługi internetowej wiąże się z wymianą informacji, co w przypadku udanego ataku stanowi dodatkowe zagrożenie dla całego procesu.

Wybór mechanizmów bezpieczeństwa, które zapewniają stosowny poziom zabezpieczeń [55], jest uzależniony między innymi od stworzonej koncepcji bezpieczeństwa. Wspomnianą koncepcję możemy utworzyć za pomocą różnych metodologii [18, 59], ale zasadniczo w każdej z nich musimy zadbać o ustalenie podobnych komponentów wpływających na ocenę ryzyka danego procesu. Wśród głównych komponentów, które są określane w procesie oceny ryzyka można wymienić: zasoby biorące udział w procesie, potencjalne zagrożenia dla zasobów, wrażliwość zasobów, skutki udanego ataku i zastosowane zabezpieczenia.

Taka analiza pozwala ustalić odpowiednie mechanizmy bezpieczeństwa, za pomocą których określane są poziomy bezpieczeństwa dla poszczególnych faz protokołu [24], który realizuje daną usługę elektroniczną. Takie podejście jest tylko częściowym rozwiązaniem, ponieważ za pomocą danej usługi elektronicznej można przesyłać informacje o różnym poziomie zagrożenia. Często przyjmowaną praktyką jest stosowanie zawyżonych środków ochrony informacji, co w dużej mierze obniża wydajność i dostępność sytemu, a także

`

wprowadza nadmiarowość systemu oraz zawyża koszty.

Wartym zbadania jest zastosowanie skalowanego bezpieczeństwa, dzięki któremu można sterować poziomem ochrony informacji w zależności od konkretnych wymogów rozważanego przypadku.

# ROZDZIAŁ 1

## PROCESY REALIZOWANE DROGĄ ELEKTRONICZNĄ

## 1.1. Społeczeństwo informacyjne

Od kilkunastu lat społeczeństwo, w jakim się znajdujemy staje się „społeczeństwem informacyjnym". Pojęcie to jest szeroko opisywane w literaturze. Przyjęto określenie, że „społeczeństwo informacyjne jest etapem w rozwoju cywilizacji, w którym społeczeństwo i gospodarka skoncentrowane są na produkcji, dystrybucji i użytkowaniu informacji; informacja i wiedza stają się podstawowymi czynnikami produkcji" [17].

Zakładając, że informacja jest głównym czynnikiem produkcji możemy mówić o nowej gospodarce opartej na zastosowaniu wiedzy. Jednym z kluczowych elementów, który kreuje obraz społeczeństwa informacyjnego jest postęp technologiczny. Rozwój technologiczny przebiega wokół głównych nurtów badań naukowych, od których zależą dalsze przemiany, są to między innymi: sprzęt, oprogramowanie i teleinformatyka.

W budowanie społeczeństwa informacyjnego zaangażowane jest wiele państw Europy. Powstaje wiele planów oraz inicjatyw, które opisują przeobrażenia oraz założenia dla społeczeństwa informacyjnego. W 2002 roku powstała inicjatywa „eEurope 2005: An information society for all" [79], która bazuje na dwóch głównych grupach aktywności. Pierwsza obejmuje nowoczesne elektroniczne formy usług dla społeczeństwa (e-government, e-learning, e-health) oraz dynamiczne środowiska dla e-biznesu. Druga mówi o infrastrukturze teleinformatycznej oraz zagadnieniach bezpieczeństwa.

Podobne strategie zostały utworzone dla Polski. Jest nim między innymi „Strategia informatyzacji Rzeczypospolitej Polskiej - ePolska" [62]. Zostały wyodrębnione obszary, w obrębie których projekty mogą zostać zrealizowane. Są to:

- powszechny dostęp do treści i usług udostępnianych elektronicznie;
- tworzenie wartościowej oferty treści i usług;
- zapewnienie warunków ich efektywnego wykorzystania.

Wyodrębniono również projekty, które są krytyczne dla informatyzacji Polski; są to:

- szerokopasmowy dostęp do Internetu w każdej szkole (infrastruktur dostępu, bezpieczeństwo sieci);
- „Wrota Polski" (zintegrowana platforma usług administracji publicznej dla społeczeństwa informacyjnego);
- promocja Polski w Internecie;
- powszechna edukacja informatyczna.

Część projektów zostało już zrealizowanych, niektóre są w trakcie realizacji. Do takich projektów można zaliczyć projekt eTEN, którego głównym celem jest niwelowanie różnic w poziomie rozwoju państw członkowskich Unii Europejskiej (http://kbn.gov.pl/eten/), projekt IDA-II polegający głównie na wspieraniu implementacji sieci sektorowych w obszarach priorytetowych dla Unii Europejskiej (http://bip.mswia.gov.pl/), projekt eContent mający na celu

stymulowanie rozwoju i wdrażania europejskich zasobów cyfrowych w sieciach globalnych (http://cordis.lu/econtent/). Warto zwrócić uwagę, że również zagadnienia związane z bezpieczeństwem informacji uwzględnione są w projektach rządowych.

## 1.2. Rodzaje usług elektronicznych

W społeczeństwie informacyjnym administracja publiczna oraz inne usługi publiczne zmieniają klasyczną formę przekazywania informacji na formę elektroniczną. Korzyści płynące ze stosowania drogi elektronicznej są znaczne: oszczędność czasu, znaczne usprawnienie przepływu dokumentów, obniżenie kosztów. Aktualnie prowadzone są badania nad różnymi sferami administracji publicznej, można tutaj wymienić: elektroniczną służbę zdrowia (e-health) [4], elektroniczne państwo (e-government) [1, 40], elektroniczne nauczanie (e-learning) [7] i handel elektroniczny (e-commerce) [24]. Każda z wymienionych dziedzin aktywności zawiera w sobie wiele problemów i rozwiązań szczegółowych, których praktyczna realizacja sama w sobie jest złożonym zagadnieniem.

Przykładowym projektem, który realizowany jest w obrębie elektronicznego państwa (e-państwo, e-government), jest elektroniczne głosowanie (e-voting). Dzięki takiej usłudze wyborcy mogliby oddawać swoje głosy za pośrednictwem sieci Internet, co spowodowałoby między innymi większą frekwencję wyborczą i zmniejszyłoby możliwości fałszerstw. Innym realizowanym projektem jest elektroniczne wypełnianie zeznań podatkowych (e-tax-filling), które pozwala między innymi na zaoszczędzenie czasu przez podatnika, zmniejszenie kosztów przez urząd oraz usprawnienie ewidencji.

Do inicjatyw e-państwa można zaliczyć również uzyskiwanie dokumentów państwowych (np. dowód osobisty, prawo jazdy), odnawianie już uzyskanych dokumentów, udostępnianie informacji dotyczącej funkcjonowania urzędów państwowych oraz szczególnie ważną dla państwa polskiego elektroniczną formę przetargu, zgodną z ustawą o zamówieniach publicznych[14].

W obrębie grupy elektronicznego nauczania (e-learning) zawierają się projekty realizujące zagadnienia zdalnej edukacji. Wśród nich wymienić można wirtualne uniwersytety np. British Open University (http://www.open.ac.uk/), Polski Uniwersytet Wirtualny (http://www.puw.pl/), dzięki, którym można studiować za pośrednictwem sieci Internet. Realizowane są również zdalne szkoły średnie (e-college), które mogą zastąpić klasyczną formę nauczania. Oprócz pełnych programów edukacyjnych realizowane są projekty wspomagające nauczanie, czyli np. elektroniczne kursy po ukończeniu studiów (postgraduate courses), akademie specjalistyczne (the Globe Wide Network Academy in Denmark). Warto wspomnieć, że dzięki powyższym projektom wiele osób może rozpocząć kształcenie, przykładem są osoby niepełnosprawne lub pracujące, które nie mogą uczestniczyć w klasycznej formie zajęć.

`

Do następnych inicjatyw można zaliczyć zagadnienia związane z opieką medyczną, które funkcjonują pod nazwą e-health. Wśród tych zagadnień można znaleźć projekty, które realizują zdalne wizyty lekarskie (e-visit). Jest to szczególnie ważne, gdy pacjent nie może dotrzeć do placówki zdrowia. Duże możliwości w dziedzinie opieki lekarskiej dają zdalne konsultacje ze specjalistami (Clinical Decision Support), którzy za pośrednictwem sieci Internet mogą stawiać diagnozy lekarskie. W obrębie opisywanej grupy realizowane są również projekty wspomagające edukację medyczną pacjentów (consumer education), komunikację między pacjentem a lekarzem (physician/consumer communication) czy administracji placówkami medycznymi (administrative efficiencies).

Elektroniczny handel (e-commerce) jest następną inicjatywą, która w dzisiejszych czasach rozwija się nadzwyczaj szybko. Wśród najpopularniejszych rozwiązań można wyróżnić: aukcje internetowe, serwisy ogłoszeniowe, sklepy internetowe, pasaże handlowe, rynki elektroniczne i wirtualne giełdy. Handel elektroniczny ma wiele zalet, co stanowi podstawę jego gwałtownego rozwoju. Do nich można zaliczyć między innymi: elastyczność, interaktywność, dostępność i oszczędzanie kosztów.

# Rozdział 2

## Podstawy bezpieczeństwa informacji

## 2.1. Modele komunikacji

Urządzenia sieciowe połączone są ze sobą za pomocą mediów sieciowych, przez które dane w postaci pakietów są wymieniane [11]. Wprawdzie media sieciowe służą do przesyłania danych z jednego miejsca do drugiego, to same nie biorą udziału w procesie komunikacyjnym. Sprowadza się to do faktu, że za pomocą samych mediów sieciowych dane nie są w żaden sposób przetwarzane, a operacje wykonywane są głównie za pomocą oprogramowania. Wspomniane oprogramowanie wykorzystuje do wymiany danych różne modele komunikacyjne, wśród nich do najpopularniejszych można zaliczyć model klient-server oraz peer-to-peer (P2P).

Model klient-serwer jest aktualnie modelem komunikacyjnym najbardziej powszechnym w sieciach komputerowych. Określenie klient i serwer odnosi się do dwóch programów biorących udział w wymianie informacji. Oprogramowanie rozpoczynające połączenie nazwane jest klientem, a program czekający biernie na żądanie połączenia serwerem.

Oprogramowanie bazujące na opisywanym modelu zazwyczaj ma następujące cechy [11]:

1. Klient
   - jest dowolnym programem użytkowym, realizowany jest tymczasowo (w razie potrzeby komunikacji z serwerem), ale wykonuje również obliczenia lokalne;
   - jest wywołany bezpośrednio przez użytkownika, a czas wykonania obejmuje tylko jedną sesję;
   - działa lokalnie na komputerze osobistym użytkownika;
   - aktywnie inicjuje kontakt z serwerem;
   - w razie potrzeby może kontaktować się z wieloma serwerami, jednak jednocześnie aktywnie komunikuje się tylko z jednym serwerem;
   - nie wymaga specjalnego sprzętu ani wyrafinowanego systemu operacyjnego.

2. Serwer
   - jest specjalizowanym, uprzywilejowanym programem, którego zadaniem jest świadczenie konkretnej usługi, a który może obsługiwać jednocześnie wielu klientów;
   - jest uruchamiany automatycznie przy uruchamianiu systemu i działa przez wiele kolejnych sesji;
   - działa na publicznie dostępnym komputerze (a nie na komputerze osobistym użytkownika);
   - czeka biernie na zgłoszenia od dowolnych klientów;
   - przyjmuje połączenia od dowolnych odległych klientów, ale spełnia jedną konkretną usługę;
   - wymaga wydajnego sprzętu i zaawansowanego systemu operacyjnego.

Do zastosowań modelu klient-serwer można zaliczyć np.: systemy WWW (HTTP), pocztę elektroniczną (SMTP), wymianę danych (FTP), współdzielenie plików (NFS), itd.

Model P2P jest modelem komunikacyjnym, który w odróżnieniu od scentralizowanego modelu klient-serwer bazuje na bezpośredniej wymianie danych między stronami biorącymi udział w komunikacji [69]. Architektura P2P jest zwróceniem się w stronę zdecentralizowanych systemów, w jej obrębie można wymienić trzy rodzaje:

- autonomiczne P2P – brak centralnego serwera;
- P2P zorientowane na użytkownika – serwer lub serwery dysponują katalogiem użytkowników;
- P2P zorientowane na dane – serwer lub serwery przechowują indeks dostępnych w systemie zasobów.

Aplikacje P2P sprawdzają się najlepiej, gdy:

- centralizacja zasobów nie jest możliwa lub nie jest pożądana;
- wymaga się bardzo wysokiej skalowalności;
- związki pomiędzy węzłami są krótkotrwałe i *ad-hoc;*
- zasoby są rozproszone;
- wymagana jest duża odporność na awarie.

Zastosowanie aplikacji bazujących na modelu P2P to głównie współdzielenie plików; do nich zaliczamy aplikacje takie jak TORENT. Innymi są rozproszone obliczenia, rozproszone usługi, rozproszone repozytorium danych i komunikatory.

Innym elementem związanym z komunikacją sieciową jest zagadnienie trasowania ruchu sieciowego (routing), czyli wyznaczania tras datagramów (pakietów) [11]. Oprogramowanie odpowiedzialne za trasowanie pakietów powinno zajmować się nie tylko znajdowaniem tras, ale wybieraniem tej optymalnej. Charakterystyka tras wymienianych pakietów w dużej mierze zależy od używanej aplikacji. Dla aplikacji sieciowych, które wymieniają dane w czasie rzeczywistym, istotnym elementem jest zadbanie o jak najmniejszą niestabilność wymienianych danych. Inaczej jest w sytuacji, gdy główną funkcją aplikacji jest wymiana dużych plików danych, czyli np. grafiki, oraz innych danych multimedialnych. Wówczas kluczowym problemem jest zagwarantowanie odpowiednio dużej przepustowości sieci.

Zarysowane wyżej zagadnienie jest istotnym problemem informatycznym zarówno dla samego procesu komunikacji, jak i dla zagadnień związanych z ochroną informacji. Jednak wykracza ono poza ramy książki, dlatego nie będzie szczegółowo rozważane w dalszej części.

`

## 2.2. Zagrożenia procesów elektronicznych

Analizując zagrożenia występujące w procesach elektronicznych widzimy, że bezpieczeństwo informacji jest kluczowym zagadnieniem dla ich poprawnego funkcjonowania [48]. Aktualnie w procesach realizowanych drogą elektroniczną główną rolę pełnią aplikacje typu klient-serwer; przykładem są aplikacje bazujące na WWW. Bezpieczeństwo takich usług sieciowych ma trzy newralgiczne elementy. Składają się na nie [22]:

- bezpieczeństwo po stronie klienta;
- bezpieczeństwo wymiany danych;
- bezpieczeństwo po stronie serwera.

Szczegółowa analiza wspomnianych zagadnień jest bardzo złożona. Zajmuje się nimi wiele organizacji tworząc odpowiednie normy, które wyznaczają praktyczne standardy bezpieczeństwa, np. [35, 44, 78, 91, 92]. Warto zwrócić uwagę na niektóre zagadnienia związane z zapewnieniem bezpieczeństwa, zwłaszcza takie, które można stosunkowo łatwo wprowadzić np. we wcześniej wspomnianych systemach administracji publicznej.

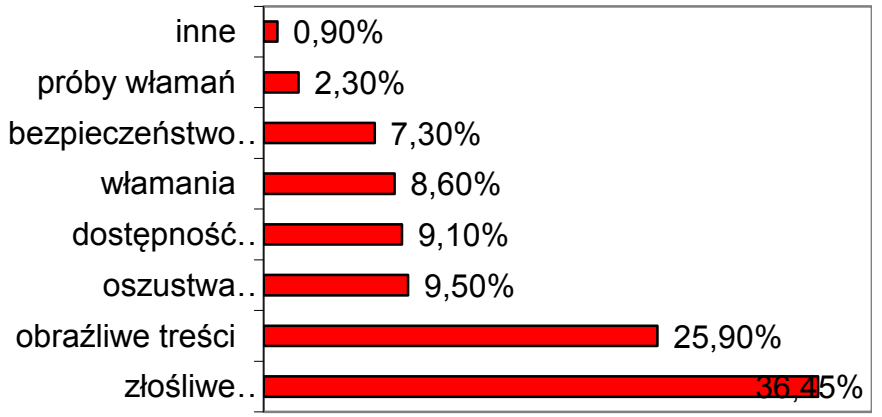
Bezpieczeństwo klienta opisuje zabezpieczenia po stronie użytkownika systemów informatycznych. Istotnym elementem jest prawidłowe zabezpieczenie systemów operacyjnych oraz aplikacji, z których klienci usług elektronicznego korzystają. W tym celu należy zadbać między innymi o najnowsze uaktualnienia systemów, aplikacji oraz baz wirusów programu antywirusowego. Warto również zaopatrzyć się w osobistą „zaporę ogniową", która pomaga uchronić komputery klienckie przed niepożądanym ruchem z sieci. Zazwyczaj mniejszą rolę przywiązuje się do komputerów klienta niż serwera. Powoduje to, że są one celem wielu ataków.

Ochrona informacji przekazywanych między klientem a serwerem jest kolejnym istotnym składnikiem bezpieczeństwa. Informacje przekazywane przez Internet są narażone na wiele zagrożeń [8]. Szczegółowe usługi ochrony informacji zostały przedstawione w rozdziale 2. Korzystając z aplikacji posiadających zaimplementowane moduły kryptograficzne można zapewnić odpowiedni poziom bezpieczeństwa. Głównie używane moduły kryptograficzne to: podpis cyfrowy (elektroniczny), szyfrowanie, schemat podziału sekretu i inne protokoły kryptograficzne, a także funkcje kryptograficzne.

Ochrona danych zgromadzonych na serwerze oraz zabezpieczenie samego serwera to kolejne zagadnienie ochrony informacji. Serwer, jako komputer udostępniający określone usługi, posiadający dostęp do wielu informacji, jest ogniwem mocno zagrożonym. Bezpieczeństwo serwerów sieciowych powinno stać na najwyższym poziomie. Chcąc sprostać takim wymaganiom należy tworzyć zabezpieczenia infrastruktury systemu, bazując na wprowadzonych normach dotyczących ochrony informacji [35].

### 2.2.1. Krytyczne zagrożenia

Ataki na infrastrukturę teleinformatyczną mają różny charakter oraz różne natężenie [9, 10] (rys. 2.1). Informacje dotyczące zagadnień związanych z naruszeniem ochrony informacji w Internecie są rejestrowane przez organizacje zrzeszające zespoły reagujące i zespoły bezpieczeństwa. Do nich zaliczamy CERT Polska (ang. Computer Emergency Response Team).



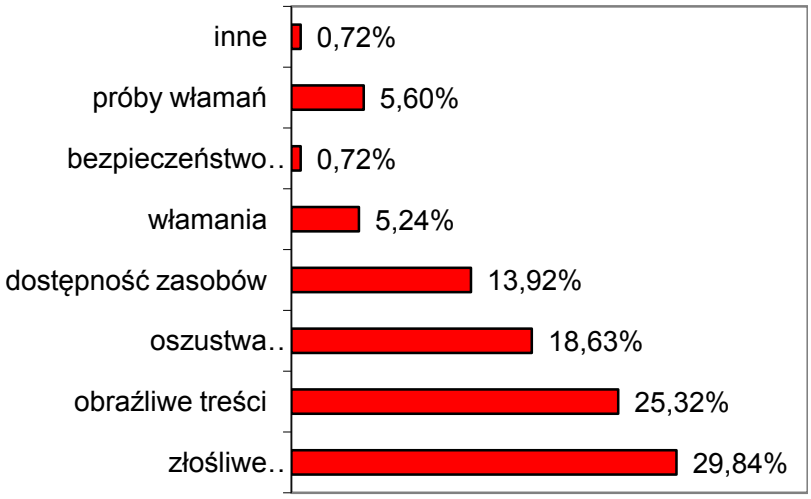

Rys. 2.1 Rozkład procentowy typów incydentów w roku 2003 (bez kategorii „gromadzenie informacji") [9].

Według raportu CERT przedstawiającego analizy incydentów naruszających bezpieczeństwo teleinformatyczne w roku 2003 [9] najbardziej powszechnym nadużyciem jest „gromadzenie informacji", czyli głównie *skanowanie.* Według CERT Polska liczba tego typu incydentów nie przedstawia realnego zagrożenia dla infrastruktury sieciowej, ponieważ nie świadczy to wyłącznie o przygotowywaniu przyszłych ataków, ale jest następstwem wcześniej udanych ataków na sieci i komputery. Na rys. 2.1 przedstawiono rozkład procentowy typów incydentu bez kategorii „gromadzenie informacji", gdyż ta grupa nadużyć utrudnia analizę pozostałych zagrożeń.

Główne typy odnotowanych incydentów przedstawione na rys. 2.1, pokazują różnorodność możliwych nadużyć w Internecie. Incydenty towarzyszące procesom realizującym usługi elektroniczne można podzielić na dwie grupy: incydenty zagrażające klientom oraz incydenty zagrażające podmiotom świadczącym usługi (serwerom). Analizując bezpieczeństwo usług elektronicznych jako pewnego procesu warto zauważyć, że krytyczne zagrożenie procesu leży w dużym stopniu po stronie serwera usług, a w mniejszym po stronie klienta.

W roku 2003 nadużycia zanotowane przez CERT Polska [9] wskazują, że najpowszechniejszym zagrożeniem poprawności użycia usług elektronicznych jest „złośliwe oprogramowanie". Zaliczamy do nich głównie robaki sieciowe,

wirusy oraz konie trojańskie. Innymi, powszechnie stosowanymi nadużyciami są „niechciane lub obraźliwe treści", czyli spam. Wspomniane ataki nie stanowią jednak dużego zagrożenia dla procesów usług elektronicznych (np. handlu elektronicznego - e-commerce), ponieważ ich szkodliwość dla klienta jest dosyć niska, a zapobieganie stosunkowo proste.




Rys. 2.2 Rozkład procentowy typów incydentów w roku 2004 (bez kategorii „gromadzenie informacji") [10].

Oprócz incydentów mało szkodliwych należy również zauważyć groźne nadużycia. W ich skład wchodzą „włamania" (włamania na konto uprzywilejowane lub zwykłe), „oszustwa komputerowe" (nieuprawnione wykorzystanie zasobów, naruszenie praw autorskich, podszycie się), „bezpieczeństwo informacji" (nieuprawniony dostęp do informacji).

W roku 2005 CERT Polska przedstawił analizę incydentów naruszających bezpieczeństwo teleinformatyczne w roku 2004 [10]. Na rys. 2.2 przedstawiono rozkład procentowy zanotowanych incydentów na infrastrukturę teleinformatyczną. Z powodów przedstawionych wcześniej, również to zestawienie przedstawiono bez grupy incydentów „gromadzenie informacji".

Porównując procentowy udział incydentów zanotowanych w roku 2003 i 2004 można zauważyć, że główne różnice są w grupach incydentów określanych jako „oszustwa komputerowe" oraz „bezpieczeństwo informacji". W roku 2004 dwukrotnie wzrosły „oszustwa komputerowe", czyli nieuprawnione wykorzystanie zasobów, naruszenie praw autorskich, kradzież tożsamości i podszycie się. W stosunku do roku 2003 blisko dziesięciokrotnie zmalała grupa incydentów zawartych w grupie „bezpieczeństwo informacji", czyli nieuprawniony dostęp do informacji i nieuprawniona zmiana informacji. Incydenty w pozostałych grupach były zanotowane w podobnej liczbie w latach 2003 - 2004.

Przykładem ilustrującym potencjalne zagrożenie dla procesów elektronicznych może być atak składający się z zestawienia wymienionych incydentów. Pierwszym krokiem może być zdobycie uprawnień uprzywilejowanych („włamanie") w pewnym systemie operacyjnym komputera klienckiego. Drugi krok może polegać na nieuprzywilejowanym dostępie do informacji („bezpieczeństwo informacji"). Ostatecznym krokiem może być podszycie („oszustwo komputerowe"), za pomocą którego można zdalnie wysłać poufne informacje zdobyte w kroku drugim jako całkiem inna osoba. Powszechność takiego rodzaju ataków jest stosunkowa niska, nie mniej jednak konsekwencje są bardzo wysokie.

Serwer usług (np. typu e-commerce) jest elementem krytycznym całego procesu. Głównym powodem takiego stwierdzenia jest fakt, że większość usług nie może być poprawnie zrealizowana bez pośrednictwa różnych serwerów sieciowych. Nadużyciami, które mogą być istotnym zagrożeniem dla serwerów sieciowych, są „włamania", „oszustwa komputerowe", „bezpieczeństwo informacji" oraz „dostępność zasobów" (ataki blokujące DoS oraz DDoS). Wymienione ataki mają miejsce z podobną częstotliwością, zagrożenia są podobne jak w przypadku opisywanym dla klienta z tą różnicą, że informacje przechowywane na serwerach są zazwyczaj krytyczne dla całego systemu usługi realizowanej drogą elektroniczną.

Wśród wspomnianych incydentów warto wyróżnić grupę określaną przez CERT jako „dostępność zasobów". Ataki te polegają na blokowaniu serwerów (np. rozproszony atak odmowy usługi, DDoS), ich szczególne niebezpieczeństwo polega na tym, że ich powstrzymanie jest szczególnie trudne, a czasami praktycznie niemożliwe do wykonania. W tym wypadku nadużycia niegroźne dla pojedynczego klienta (np. bombardowanie spamem), może doprowadzić do dużych strat dla dostawcy usług elektronicznych, powstałych w wyniku uniemożliwienia pracy serwera.

## 2.3. Bezpieczeństwo procesów realizowanych drogą elektroniczną

### 2.3.1. Usługi ochrony informacji

W praktyce realizacja procesów przeprowadzanych drogą elektroniczną niesie ze sobą spełnienie wielu uwarunkowań technicznych, formalnych i prawnych. Projektując systemy musimy zadbać o realizację różnych usług bezpieczeństwa [55, 63, 83]. Wśród nich możemy wymienić między innymi: integralność danych, niezaprzeczalność zdarzenia, niezaprzeczalność nadawcy oraz odbiorcy, poufność danych, autoryzację stron, zarządzanie przywilejami, anonimowość sieciową, anonimowość nadawcy oraz odbiorcy, dostępność do usług i zasobów, wzajemne zaufanie uczestników, zaufanie przez trzecią stronę, bezpieczne przechowywanie danych, rozliczalność sieciową oraz rozliczalność protokołu i usług. Każda usługa bezpieczeństwa posiada własną charakterystykę. Usługi te zostały w sposób skrótowy przedstawione w tab. 2.1.

`

Usługa integralności danych gwarantuje, że informacje odbierane są w takiej postaci, w jakiej zostały wysłane, bez wstawiania i modyfikacji, powtórzeń, zmian kolejności. Istotnym elementem, który zapewniany jest przez opisywaną usługę jest ochrona przesyłanych danych przed zniszczeniem.

Usługę niezaprzeczalności możemy zaliczyć do jednej z trzech kategorii: do takich, które stwierdzają niezaprzeczalność nadawcy, odbiorcy lub wystąpienia samego zdarzenia. Usługa ta polega na pozbawieniu możliwości zaprzeczenia faktu wysłania danych przez strony protokołu oraz możliwości wyparcia się faktu wymiany danych przez konkretne strony protokołu (samego faktu komunikacji).

Usługa poufności zapobiega ujawnieniu jakichkolwiek danych wymienianych pomiędzy stronami protokołu. Ilość danych wymienianych w sposób poufny w danym protokole zależy od jego wymogów. Poufne mogą być tylko konkretne komunikaty, a nawet odpowiednie fragmenty komunikatów.

Tab. 2.1 Charakterystyka usług bezpieczeństwa.

| **Grupa usług** | **nazwa usługi** | **charakterystyka** |
|---|---|---|
| Integralność | *integralność danych* | niemożliwa modyfikacja danych |
| Niezaprzeczalność | *niezaprzeczalność zdarzenia* | jednoznaczność przesłania wiadomości |
| | *niezaprzeczalność nadawcy* | jednoznaczność tożsamości nadawcy |
| | *niezaprzeczalność odbiorcy* | jednoznaczność tożsamości odbiorcy |
| Poufność | *poufność danych* | dostęp do danych tylko przez uprawnione osoby |
| Uwierzytelnienie i autoryzacja | *autoryzacja stron* | możliwość udziału w protokole tylko po weryfikacji tożsamości |
| Przywileje | *zarządzanie przywilejami* | różnorodność praw dostępu w zależności od funkcji w protokole |
| Anonimowość | *anonimowość nadawcy* | nieznana tożsamość nadawcy wiadomości (bez anonimowości sieciowej) |
| | *anonimowość odbiorcy* | nieznana tożsamość odbiorcy wiadomości (bez anonimowości sieciowej) |
| | *anonimowość sieciowa* | ukrycie faktu wymiany danych (ukrycie przepływu informacji, ukrycie ruchu sieciowego) |
| Dostępność | *dostępność do usług i* | możliwość skorzystanie z usług |

| | | |
|---|---|---|
| | *zasobów* | i zasobów w dowolnym momencie |
| Publiczne zaufanie | *wzajemne zaufanie uczestników* | możliwość publicznej weryfikacji przeprowadzonego kroku protokołu wśród uczestników protokołu |
| | *zaufanie przez trzecią stroną* | możliwość weryfikacji przeprowadzonego kroku protokołu za pośrednictwem trzeciej strony |
| Przechowywanie danych | *bezpieczne przechowywanie danych* | poufne oraz trwałe przechowywanie wymienianych danych |
| Rozliczalność | *rozliczalność sieciowa* | zdarzenia w sieci są rejestrowane |
| | *rozliczalność protokołu/usługi* | kroki protokołu (dostęp do usługi) są rejestrowane |

Najwyższy poziom poufności zabezpiecza wszelkie dane wymieniane przez strony protokołu.

Usługa autoryzacji (identyfikacji i uwierzytelnienia) polega na zagwarantowaniu wiarygodnej identyfikacji stron protokołu (potwierdzeniu, że każda ze stron jest tą, za którą się podaje). Rozszerzona na wymieniane informacje (nazywana wówczas usługą autentyczności) pozwala zapewnić autentyczność informacji wymienianych pomiędzy stronami protokołu.

Zarządzanie przywilejami polega na przydzieleniu odpowiednich uprawnień stronom protokołu. Jest to poprzedzone wcześniejszą ich identyfikacją i uwierzytelnieniem. Dzięki tej usłudze można zarządzać dostępem do danych i możliwymi funkcjami pełnionymi przez strony w protokole.

Usługa anonimowości pełni trzy główne funkcje. Pierwsza (anonimowość nadawcy) polega na ukryciu tożsamości nadawcy, bez uwzględnienia anonimowości sieciowej. Druga (anonimowość odbiorcy) zapewnia ukrycie tożsamości odbiorcy, również bez anonimowości sieciowej. Trzecia (anonimowość sieciowa) zapewnia ukrycie samego faktu wymiany danych. Anonimowość sieciowa jest zwykle realizowana przez ukrycie ruchu sieciowego (np. poprzez ukrycie go w sztucznie generowanym ruchu pakietów danych).

Usługa dostępności polega na tym, że osoby uprawnione będą miały możliwość korzystania z zasobów oferowanych przez system w dowolnym momencie przewidzianym w protokole. Zagwarantowanie tej usługi jest szczególnie istotne, ponieważ gdy system nie jest dostępny dla użytkowników, to traci swoją funkcjonalność, co prowadzi do blokady dowolnych operacji na nim.

Usługa publicznego zaufania pozwala na powszechną weryfikację

`

przeprowadzonego kroku protokołu. Istnieje możliwość weryfikacji przy udziale uczestników danego protokołu lub za pośrednictwem zaufanej trzeciej strony.

Usługa przechowywania danych polega na poufnym i trwałym przechowywaniu wymienianych danych. Informacje wymagane w protokole są używane w różnych jego krokach, dlatego istotnym elementem jest ich poufne i trwałe przechowywanie.

Tab. 2.2 Relacje między usługami ochrony informacji (N – neutralny, Z – zawiera, W - wyklucza).

| usługa \ relacje | I | Au | MP | NR | NA | PT | C | AN | SS | AV |
|---|---|---|---|---|---|---|---|---|---|---|
| Integralność (I) | N | | | | | | | | | |
| Autoryzacja (Au) | Z | N | | | | | | | | |
| Przywileje (MP) | Z | Z | | | | | | | | |
| Niezaprzeczalność (NR) | Z | Z | Z | N | | | | | | |
| Rozliczalność (A) | Z | Z | Z | Z | N | | | | | |
| Publiczne zaufanie (PT) | Z | Z | Z | Z | Z | N | | | | |
| Poufność(C) | | | | | | | N | | | |
| Anonimowość (AN) | | | | | W | | | N | | |
| Bezpieczne przechowywanie danych (SS) | | | | | | | | | N | |
| Dostępność (AV) | | | | | | | | | | N |

Wśród usług rozliczalności można wyróżnić rozliczalność sieciową oraz rozliczalność protokołu lub usługi. Rozliczalność polega na gromadzeniu informacji na temat zdarzeń oraz operacji przeprowadzanych w sieci lub podczas kroków protokołu. Dzięki posiadaniu takiego dziennika istnieje możliwość sprawdzenia czynności wykonanych przez klienta danej usługi, a w przypadku ewentualnego nadużycia - ustalenie sprawcy wykroczenia.

Usługi bezpieczeństwa są połączone ze sobą pewnymi zależnościami. Wśród nich można wymienić takie usługi, które mogą zawierać się w sobie, wykluczać się wzajemnie oraz pełnić funkcje neutralne względem siebie (opcjonalne). Usługi, które zawierają się w sobie powodują, że zastosowanie w systemie jednej pociąga za sobą użycie innych. Usługi wykluczające to takie, których jednoczesne użycie jest niemożliwe do zrealizowania. Usługi neutralne są stosowane dowolnie i nie są uzależnione od innych usług ochrony informacji. Wszystkie wspomniane relacje mogą być zastosowane jednocześnie do pojedynczej usługi bezpieczeństwa lub zastosowane wybiórczo. W tab. 2.2 przedstawiono zestawienie usług oraz ich wzajemne relacje; neutralność oznaczona jest przez literę „N”, usługi wykluczające przez „W”, a usługi zawierające się przez „Z”.

Podstawową usługą bezpieczeństwa jest integralność danych. Autoryzacja (danych) gwarantuje integralność, a dodatkowo dba o uwierzytelnienie danej strony protokołu. Przywileje gwarantują integralność oraz autoryzację, a dodatkowo pozwalają przydzielić odpowiednie prawa stronom protokołu. Niezaprzeczalność zapewnia realizację wcześniej wymienionych usług, a dodatkowo dba o jednoznaczność tożsamości stron wykonujących działania na danych oraz jednoznaczność samego faktu wykonania akcji. Rozliczalność zawiera wszystkie wspomniane wcześniej usługi oraz gwarantuje możliwość sprawdzenia wykonanych wcześniej działań. Publiczne zaufanie oprócz wymienionych usług pozwala na wykonanie publicznej weryfikacji wykonanej akcji w danym protokole.

Prawie wszystkie usługi zawarte w tab. 2.2 są realizowane niezależnie, czyli są neutralne. Wyjątkiem jest usługa ”przywileje”, która jest powiązana z usługą „integralność” oraz „autoryzacja”.

W tab. 2.2 zaznaczone są dwie usługi bezpieczeństwa, które się wzajemnie wykluczają. Są to „anonimowość” oraz „rozliczalność”.

### 2.3.2. Mechanizmy ochrony informacji

Wymogi systemu, które są określone za pomocą usług bezpieczeństwa, realizowane są przez wybrane elementy bezpieczeństwa. Do tego celu możemy użyć np. mechanizmów przedstawionych w pracach [26, 53, 70]. Duża grupa mechanizmów zabezpieczeń bazuje na infrastrukturze klucza publicznego (PKI) [55, 70]. Architektura (infrastruktura) klucza publicznego może wykorzystywać różne modele zaufania, scentralizowany (ścisła hierarchia) oraz model rozproszonego zaufania [93]. Najbardziej rozpowszechnionym modelem jest model scentralizowany, czyli taki, w którym wszelka weryfikacja działań odbywa się poprzez główne centrum certyfikacji, które pełni role zaufanej trzeciej strony i podlegającą mu hierarchię urzędów certyfikacji. Model rozproszonego zaufania polega na tym, że weryfikacja jest ustalana między niezależnymi (równorzędnymi) centrami certyfikacji lub miedzy uczestnikami protokołu. Wśród mechanizmów zapewniających bezpieczeństwo informacji należy wymienić moduły kryptograficzne, które w odróżnieniu od usług bazujących na PKI, nie bazują na centrach certyfikacji, tylko są niezależnymi mechanizmami, na przykład mechanizm bezpiecznego podziału sekretu [53].

#### Mechanizmy bazujące na PKI (głównie scentralizowany model zaufania)

PKI jest strukturą urzędów certyfikacji wraz z ich wzajemnym podporządkowaniem (sposobem dziedziczeniem zaufania) oraz funkcjami, które one pełnią i usługami, które realizują. Główne usługi zostały przedstawione poniżej.

**Rejestracja**

Uczestnik protokołu chcący wziąć udział w procesie elektronicznym musi wcześniej zarejestrować się w centrum certyfikacji należącym do określonego

`

PKI. Po pozytywnej weryfikacji tworzona jest unikalna para kluczy publiczny/prywatny, która jednoznacznie przynależy do danego uczestnika protokołu. Klucze generowane są po stronie użytkownika lub w centrum certyfikacji, jest to uzależnione od wymogów protokołu. W skład tego mechanizmu wchodzi inicjalizująca prośba o rejestrację oraz formularz rejestracyjny zależny od konkretnego centrum certyfikacji. Dla potrzeb konkretnych aplikacji centrum certyfikacji można utworzyć wykorzystując, np., bibliotekę openSSL [67] lub openTSA [68]. Są to biblioteki objęte otwartymi licencjami. Przykładowe zastosowanie wspomnianych bibliotek zawarte jest w dodatku A oraz pracy [51]. Szczegółowy opis wymagań, które muszą zostać spełnione przy tworzeniu centrum certyfikacji zawarty jest w międzynarodowych standardach [16, 17]. Do najpopularniejszych centrów certyfikacji w Polsce należą: Signet (http://www.signet.pl/), Sigillum (http://www.sigillum.pl/), Certum (http://www.certum.pl/).

**Podpis cyfrowy**

Podpisując cyfrowo wiadomość uzyskujemy jej integralność oraz niezaprzeczalność. Proces autoryzacji również wspierany jest przez ten mechanizm. Mechanizm polega na wykorzystaniu kryptografii asymetrycznej, szyfrowaniu lub deszyfrowaniu odpowiednim kluczem, prywatnym lub publicznym. Do wykonania podpisów cyfrowych najczęściej używane są algorytmy bazujące na kryptosystemach: RSA, ElGamal, ECDSA [71, 76]. Wszystkie są opisane przez międzynarodowe normy [36].

**Szyfrowanie**

Szyfrowanie jest podstawowym kryptograficznym mechanizmem, który wykorzystywany jest do uzyskania poufności informacji. W skład funkcji szyfrujących wchodzą takie, które szyfrują i deszyfrują dane. Algorytmy kryptograficzne używane do szyfrowania danych można podzielić na dwie główne grupy algorytmów, czyli symetryczne (z kluczem prywatnym) oraz asymetryczne (kluczem publicznym). Wśród współczesnych algorytmów symetrycznych można wymienić [71] rodzinę algorytmu DES, FEAL, IDEA, RC6, Rijndael, Serpent. Do współczesnych algorytmów asymetrycznych zaliczamy kryptosystemy [71]: RSA (kryptosystem oparty na problemie faktoryzacji dużych liczb), Marklego-Hellmana (kryptosystem oparty na problemie plecakowym), McEliece'a (kryptosystem oparty na algorytmie wielomianowym), ElGamal (kryptosystem oparty na problemie logarytmu dyskretnego). Wymienione algorytmy opisano w międzynarodowych normach [36, 37].

**Znakowanie czasem**

Do dokumentu, który został podpisany cyfrowo dołączana jest informacja na temat daty i czasu jego podpisania (utworzenia), dzięki czemu jest on jednoznacznie określony względem czasu. Główne funkcje wchodzące w skład opisywanego mechanizmu to: akceptacja żądania znakowania czasem,

wyszukanie daty zaznaczonych czasem danych, weryfikacja ważności znacznika czasem, zarządzanie bazą danych certyfikatów odpowiadających znacznikom czasu, dystrybucja odpowiednich informacji do publicznej wiadomości. Funkcje znakowania czasem realizowane są przez centra znakowania czasem, które często wchodzą w skład centrum certyfikacji. Centrum znakowania czasem można utworzyć za pomocą wspomnianej biblioteki openTSA [68]. Wymogi, jakie muszą spełniać centra znakowania czasem, opisane są przez międzynarodowe normy [17].

**Niezaprzeczalność**

Mechanizm, który opiera się na generowaniu, gromadzeniu, odzyskiwaniu oraz interpretowaniu danych, które są wykorzystywane przy dowolnym kroku protokołu. Prowadzona ewidencja jest dodatkowo potwierdzana przez zaufaną trzecią stronę (TTP). Uzyskujemy dzięki temu jednoznaczność nadawcy lub odbiorcy oraz identyfikacje działań, które wykonują. Funkcje wchodzące w skład tego mechanizmu zawierają procesy inicjalizujące, unieważniające i rozwiązujące spory. Przykładowa architektura PKI, która realizuje mechanizmy niezaprzeczalności, zaprezentowana jest w pracach [25, 45].

**Zarządzanie kluczami**

Usługa ta opiera się na przechowywaniu kryptograficznych kluczy w odpowiedni, efektywny oraz bezpieczny sposób. Mechanizm ten obejmuje zagadnienia związane z generowaniem kluczy, dystrybucją kluczy, przechowywaniem kluczy, wyszukiwaniem kluczy, odzyskiwaniem kluczy, zarządzaniem kopiami zapasowymi kluczy oraz uaktualnianiem kluczy. Zagadnienia związane z zarządzaniem kluczami sprecyzowane są przez międzynarodowe normy [33, 34].

**Zarządzanie certyfikatami**

Certyfikaty są elektroniczną formą dokumentu łączącą tożsamość danej strony z jego kluczem publicznym. Zarządzanie certyfikatami polega na generowaniu, dystrybucji, przechowywaniu, wznawianiu oraz usuwaniu cyfrowych certyfikatów. Szczegółowy opis tych zagadnień wraz z regułami, jakie muszą być spełnione zawarte są w międzynarodowych standardach [33].

**Repozytorium danych**

Usługa ta polega na przechowywaniu oraz zarządzaniu danymi krytycznymi dla funkcjonowania zaufanej trzeciej strony (TTP). Główne funkcje opisywanego mechanizmu to: określenie danych do zarchiwizowania, określenie okresu przechowywania danych, autoryzacja, uaktualnienie archiwum, wyszukiwanie danych, kasowanie danych. Specyfikacja danych, uwzględniająca ich krytyczność dla ochrony informacji całego systemu, zawarta jest w stosownych opracowaniach utworzonych przez międzynarodowe instytuty [16]. Analizując te wymagania można zrealizować mechanizmy spełniające rolę repozytorium danych. Przykładowe dane zawarte są w pracach [25, 45].

**Usługa katalogowania**

Usługa ta polega na dostarczaniu informacji użytkownikom systemu PKI na temat innych użytkowników danego systemu. Funkcja ta jest realizowana

`

głównie dzięki: uaktualnianiu nowych certyfikatów, uaktualnianiu unieważnionych certyfikatów, dystrybucji, wyszukiwaniu danych. Mechanizmy określane jako usługa katalogowania, zaprezentowane są w architekturze klucza publicznego opisanej w pracach [25, 45].

**Anonimowość internetowa**

Korzyści z ukrycia komunikacji nie polegają jedynie na zwiększeniu poufności, ale również na ukryciu faktu powiązań między stronami protokołu (ukryciu komunikacji). Uzyskać to możemy za pomocą dodania pozornych wiadomości do strumienia danych, które przechodzą przez węzły sieci przesyłające właściwą informację. Szczegółowe zagadnienia związane z anonimowością internetową zawarte są w pracach [13, 94].

**Autoryzacja**

Użytkownicy systemu PKI przed uzyskaniem dostępu do usług oferowanych przez mechanizmy PKI, powinni przejść proces autoryzacji. Mechanizm ten opiera się głównie na definicji grup, uaktualnianiu praw, uaktualnianiu grup, zapisaniu użytkowników do grup i określeniu zaufanych stron. Mechanizmy autoryzacji zostały przedstawione szczegółowo w pracach [71, 83, 84].

**Audyt**

W celu zapewnienia wysokiej jakości oraz niezawodności operacji PKI procesy są weryfikowane. Działania te wykonywane są za pomocą audytu. Funkcje realizujące ten mechanizm można podzielić na dwie części:na przygotowawczy proces inicjalizujący system oraz okresowe procesy audytu sprecyzowane w stosownym planie. Szczegółowe mechanizmy audytu w stosunku do modułów kryptograficznych zawarte są w normach [20] oraz w pracy [47]. Zagadnienia audytu w zastosowaniu do całej infrastruktury PKI przedstawiono w pracach [25, 45].

**TTP-TTP weryfikacja**

Wzajemna weryfikacja przeprowadzana przez niezależne zaufane trzecie strony (TTP) zwiększa ich wiarygodność, dzięki czemu podwyższa wiarygodność całej operacji. Ten mechanizm wykorzystuje rozproszony model zaufania. Opisywany mechanizm bazuje głównie na procesach: akceptacji żądania, weryfikacji żądania, zwrocie weryfikacji żądania, znalezieniu ścieżki certyfikacji, weryfikacji ścieżki certyfikacji, akceptacji wyniku certyfikacji, wyszukiwania informacji z innych domen, odpowiedzi na zapytania z innych domen. Szczegółowa implementacja mechanizmów określonych jako „TTP-TTP weryfikacja" zawarta jest w pracy [45].

**Notariat**

Jest to publiczna weryfikacja stron biorących udział w protokole za pośrednictwem zaufanej trzeciej strony. Ten mechanizm może dostarczyć dodatkowej weryfikacji, która wzmocni np. proces autoryzacji. W tym przypadku wykorzystywany jest model zaufania oparty na centralnej weryfikacji. Protokoły wraz z mechanizmami realizującymi wspominany „notariat" opisane zostały szczegółowo w pracy [76].

### Dodatkowe (niezależne) mechanizmy ochrony informacji

**SSS (ang. Secure Secret Sharing)**
Mechanizm bezpiecznego podziału sekretu może zostać wykorzystany w przypadku gdy chcemy, żeby informacje zaszyfrowane przez klucz publiczny danej operacji zostały ujawnione tylko przy współpracy określonej liczby uprawnionych stron [53, 71, 84].

**PKG (ang. Personal Key Generator)**
Mechanizm generowania kluczy bazujący na metodzie biometrycznej [88]. Za pomocą tego mechanizmu można utworzyć unikatowe klucze wykorzystując cechy biometryczne konkretnej osoby biorącej udział w protokole.

**Crowds**
Skalowany system bazujący na usługach WWW, zapewniający nadawcy wiadomości zachowanie anonimowości wewnątrz ruchu sieciowego [72].

**AA (ang. Anonymous Authentication)**
Model zapewniający autoryzację uczestników protokołu z zachowaniem anonimowości nadawcy [89, 95, 96].

**Steganografia treści/sieciowa**
Mechanizm pozwalający ukryć informacje poufne w wiadomościach, które nie są tajne. Przykładowym medium są obrazy graficzne. Teoretyczne omówienie zagadnienia zawarte jest w pracy [76], a przykładowa praktyczna implementacja mechanizmu opisana jest w pracy [87].

## 2.3.3. Protokoły kryptograficzne

Istotnymi elementami zwiększającymi ochronę informacji całego procesu realizowanego drogą elektroniczną są moduły kryptograficzne. Szczególnie silną bronią przed nadużyciami są protokoły kryptograficzne, które korzystając z wielu technologicznych mechanizmów jakie daje kryptografia, pozwalają w skuteczny sposób zadbać o ochronę informacji. Protokół kryptograficzny można określić jako zespół kroków realizujących pewne usługi, w którym wykorzystywane są moduły kryptograficzne. O sile protokołu stanowią jego właściwości [76]:

- każdy użytkownik protokołu musi go znać i kolejno wykonywać wszystkie kroki;
- każdy użytkownik musi zgodzić się na jego stosowanie;
- protokół nie może mylić; każdy krok powinien być dobrze zdefiniowany i nie może wystąpić jakakolwiek szansa na nieporozumienie;
- protokół musi być kompletny, dla każdej możliwej sytuacji musi być podany odpowiedni sposób postępowania;
- protokół powinien zezwalać jedynie na wykonywanie takich operacji, które są w nim przewidziane.

Protokoły kryptograficzne można podzielić na arbitrażowe, rozjemcze i samowymuszające [76].

`

Protokoły arbitrażowe wprowadzają dodatkowego uczestnika protokołu, który charakteryzuje się tym, że jest obdarzony przez wszystkie przewidziane w protokole strony bezwarunkowym zaufaniem (zaufana trzecia strona). Opisywana strona w protokole pełni role arbitra, którego uczestnictwo jest niezbędne do zakończenia danego protokołu. Istotną cechą charakteryzującą arbitra jest fakt, że nie jest on w żaden sposób związany ze stronami protokołu oraz nie ma żadnego interesu w zakończeniu tego protokołu.

Inna grupa protokołów to protokoły rozjemcze. W tych protokołach również istotną rolę pełni strona pośrednia, tym razem jest to rozjemca, który wykorzystywany jest tylko wtedy, gdy wśród uczestników protokołu pojawi się spór i należy go rozstrzygnąć. Rozjemca, podobnie jak w protokołach arbitrażowych, jest stroną niezainteresowaną (neutralną) oraz pełni rolę zaufanej trzeciej strony. Główną różnicą jest to, że ingerencja rozjemcy nie jest konieczna do zakończenia protokołu, a w przypadku arbitra jest konieczna.

Ostatnia grupa protokołów to protokoły samowymuszające. W tych protokołach nie jest wprowadzana trzecia strona, czyli arbiter lub rozjemca. Protokół jest tak skonstruowany, że ewentualne spory rozstrzygane są przez sam protokół. Ta grupa protokołów jest najlepsza z punktu widzenia zarówno bezpieczeństwa, jak i optymalizacji procesów realizowanych przez dany protokół. Cechą charakterystyczną omawianej grupy protokołów jest to, że jeżeli jedna ze stron protokołu próbuje oszukiwać, wówczas druga strona (lub pozostali uczestnicy, gdy jest ich więcej) automatycznie wykryje to nadużycie. Przedstawione cechy prowadzą do wniosku, że wszystkie protokoły powinny bazować na tym modelu. Niestety, rzeczywistość jest taka, że nie ma protokołów samowymuszających odpowiednich dla każdego procesu realizowanego drogą elektroniczną.

## 2.4. Skalowane bezpieczeństwo - przegląd literatury

Zagadnienia ochrony informacji pełnią ważną rolę w przedsiębiorstwach oraz organizacjach zarówno sektora publicznego jak i prywatnego. Infrastruktury sieciowe danych organizacji tworzą architekturę dla komputerów stacjonarnych, urządzeń przenośnych oraz wszelkiego sprzętu łączącego daną firmę z siecią Internet. Wraz ze wzrostem zaawansowanych technologii informatycznych, problem stosowania skalowalnego bezpieczeństwa powinien znaleźć coraz więcej zastosowań.

Tradycyjnie zagadnienie zabezpieczania zasobów firmy było sprowadzane do zastosowania najwyższego możliwego bezpieczeństwa. Po zaimplementowaniu silnych środków ochrony informacji, co sprowadzało się do użycia najsilniejszych możliwych do zastosowania algorytmów kryptograficznych, użytkownik był pewien, że jego system jest bezpieczny. Jednak użycie tych silnych mechanizmów bezpieczeństwa może pogorszyć wydajność urządzenia z ograniczonymi zasobami i utorować drogę dla nowych zagrożeń, takich jak wyczerpanie zasobów. Rezultatem jest niski poziom jakości usługi, a nawet

odmowa usługi. Dodatkowym skutkiem użycia zawyżonych środków ochrony informacji są dodatkowe koszty finansowe, które musi ponieść firma w wyniku implementacji zaawansowanych mechanizmów bezpieczeństwa. Powodem takiego stanu rzeczy jest wybór między wydajnością systemu a zastosowanym poziomem ochrony informacji, w którym najwyższy poziom zabezpieczeń jest stosowany jedynie w wyjątkowych sytuacjach.

W świetle przedstawionych rozważań wskazane jest utworzenie mechanizmów bezpieczeństwa, które wydajnie i w sposób skalowany użytkują dostępne zasoby systemu. Potwierdzeniem tej myśli może być opinia Bruce'a Schneiera, który twierdzi, że: *„Przyszłością systemów cyfrowych jest ich złożoność, a złożoność jest najgorszym wrogiem systemów zabezpieczeń"*.

### 2.4.1. Skalowalność zabezpieczeń

Prace naukowe odnoszące się do zagadnienia skalowanego bezpieczeństwa są ilościowo ograniczone.

Lindskog wprowadza interesujące badania odnoszące się do skalowalności zabezpieczeń w swojej rozprawie doktorskiej [56]. W tej pracy zaprezentowane są metody na uzyskanie różnych poziomów zabezpieczeń dla aplikacji sieciowych. Opisane metody ograniczają się do zagadnień związanych z poufnością, bazują na wyborze szyfrujących systemów kryptograficznych, dzięki którym istnieje możliwość ustawienia różnych poziomów zabezpieczeń zwiększających wydajność całego systemu.

W pracy [75] Schneck i Schwan proponują skalowany protokół bezpieczeństwa skoncentrowany na usłudze autoryzacji o nazwie „Authenticast". Protokół ten zawiera różne poziomy bezpieczeństwa dla platform typu klient-serwer, który oblicza poziomy zabezpieczeń na podstawie metod heurystycznych. Metody te zawierają skalowaną autoryzacje regulowaną za pomocą wartości procentowych, które bazują na odpowiednim doborze kluczy prywatnych oraz wyborze algorytmów kryptograficznych. W pracy zostały zaprezentowane wyniki osiągnięte na podstawie strumieniowania obrazu video w formacie MPEG.

W pracy [66] Ong zaproponował mechanizm nazwany „Quality of Protection (QoP)", który wprowadza różne poziomy zabezpieczeń oraz świadomość jakości i wydajności systemu. Parametry mechanizmu QoP są uzależnione od wymagań bezpieczeństwa, które reprezentowane są poprzez usługi bezpieczeństwa. W pracy istnieje możliwość wyboru usługi autoryzacji, poufności oraz integralności, jednak poziom zabezpieczeń dla wspomnianych usług bezpieczeństwa nie jest łatwo mierzalny [57]. Parametrami, które są zmienne w QoP, są: długość klucza kryptograficznego, długość bloku szyfrowanego i rodzaj zawartości danych.

Hager wprowadza w swojej rozprawie doktorskiej [27] metodologię, która pozwala zwiększyć wydajność mechanizmów bezpieczeństwa dla sieci bezprzewodowych. Metodologia ta polega na klasyfikowaniu sieci

`

bezprzewodowych i grupowaniu ich w odrębne kategorie, do których to przypisywane są odpowiednie protokoły kryptograficzne. Następnie protokoły te są analizowane, a ich bezpieczeństwo reprezentowane za pomocą wprowadzonych metryk. Aplikacje korzystające z sieci bezprzewodowych byłyby realizowane za pomocą odpowiednich, stosownych do kategorii, protokołów kryptograficznych.

Opisane wyżej prace, podejmujące temat skalowalności środków zabezpieczeń, mają ograniczony charakter, ponieważ dotyczą tylko niektórych usług bezpieczeństwa. Aktualnie projektowane usługi elektroniczne, np. usługi „eGovernment" wymagają wprowadzenia zaawansowanych usług bezpieczeństwa, których najbardziej reprezentatywne rodzaje zostały krótko opisana w rozdziale 2.2.1. W przedstawianej książce procesy elektroniczne, w których stosowane są zabezpieczenia, traktowane są jako protokoły kryptograficzne, w których jednakowo traktowane są kroki związane z zastosowaniem metod ochrony informacji, jak i kroki realizujące ich podstawową funkcjonalność. Takie podejście do procesu elektronicznego pociąga za sobą utworzenie zaawansowanego protokołu kryptograficznego, którego wszystkie kroki traktowane są jako elementy jednej całości. Aktualnie w literaturze nie opisano metody skalowalności zabezpieczeń, którą można by zastosować do tak ogólnie sformułowanego zagadnienia.

Innym niedostatkiem w wymienionych pracach jest prezentowane tam podejście do wyznaczenia mechanizmów ochrony informacji składających się na dany poziom zabezpieczeń. Wymienione prace bazują na intuicyjnym wyborze parametrów zabezpieczeń. Wybór intuicyjny należy wspomóc procesem szacowania ryzyka, który pozwala w sposób bardzie precyzyjny określić potencjalne zagrożenia. Mechanizmy szacowania ryzyka wprowadzają możliwość zastosowania automatycznego wyboru zabezpieczeń. W obecnych czasach, gdy tempo pojawiania się ciągle nowych zagrożeń systemów informatycznych jest bardzo duże, cecha wprowadzająca automatyczny wybór zabezpieczeń jest szczególnie istotna.

### 2.4.2. Zarządzanie ryzykiem

Zagadnienia związane z zarządzaniem ryzykiem są szeroko rozważane przez naukowców w różnych dziedzinach wiedzy. Dla nowych systemów informatycznych oraz systemów będących na etapie planowania zagadnienie zarządzania ryzykiem powinno być nieodłącznym elementem analizy bezpieczeństwa. Zagadnienie szacowania ryzyka opisane jest przez normy [20, 31, 32, 33] oraz szeroko dyskutowane w pracach [18, 23, 26, 55, 59, 61].

W każdej z tych prac przyjęto, że musimy zadbać o ustalenie podobnych czynników wpływających na ryzyko danego procesu. Wśród nich można wymienić: zasoby biorące udział w procesie, potencjalne zagrożenia tych zasobów, wrażliwość zasobów, skutki udanego ataku i zabezpieczenia. Poniżej przedstawiono krótki opis wymienionych czynników wpływających na ryzyko.

**Zasoby**

Podstawowym krokiem w procesie ustalania programu bezpieczeństwa jest przeanalizowanie zasobów danej organizacji. Należy ustalić dla poszczególnych zasobów poziomy ich wrażliwości na atak. Na tej podstawie będą przydzielane odpowiednie środki bezpieczeństwa.

**Zagrożenia**

Potencjalne zagrożenia mogą spowodować szkody w zasobach gromadzonych przez daną organizacje. Szkody mogą być spowodowane atakiem na informacje biorące udział w procesie lub na sam system. Zagrożenia muszą dotyczyć wrażliwości w aktywach i dopiero wówczas mogą spowodować pewne szkody. Zagrożenia możemy podzielić na ludzkie oraz środowiskowe, a następnie na podstawowe i incydentalne. Poziomy takiego zagrożenia powinny być wyznaczone dla wszystkich zasobów. Dodatkowo powinno być obliczone prawdopodobieństwo wystąpienie określonego zagrożenia.

**Wrażliwość**

Podatność na uszkodzenia zasobów, które mogą zostać odkryte przez zagrożenia możemy określić jako wrażliwość tych zasobów. Wrażliwości zasobów może polegać na słabości warstwy fizycznej, procedur, personelu, zarządzania, sprzętu, oprogramowania, informacji itd. Wrażliwość sama w sobie nie powoduje szkód, dopiero w przypadku ataku możemy mówić o szkodach.

**Wpływ ataku na system**

Skutki ataku są miarą strat poniesionych w wyniku udanego ataku, spowodowanego przez zagrożenie, które dotyczy pewnych zasobów. Innym potencjalnym efektem jest zniszczenie wszystkich zasobów, częściowe uszkodzenie systemu lub skompromitowanie poszczególnych usług bezpieczeństwa. Pośrednią szkodą są straty finansowe, utrata renomy organizacji, itp.

**Zabezpieczenia**

Środki zabezpieczeń składają się z procedur i mechanizmów, które mają za zadanie chronić przed zagrożeniem, redukując wrażliwość systemu i zmniejszając jednocześnie ewentualne skutki udanego ataku.

**Ryzyko**

Ryzyko jest charakteryzowane przez iloczyn dwóch czynników: prawdopodobieństwa wystąpienia incydentu (zestawienie zagrożeń) oraz skutku ewentualnego ataku [23, 31, 32]:

**Ryzyko (R) = prawdopodobieństwo (P) * wpływ ataku na system (ω).**

Metody przeprowadzania szacowania ryzyka oparte są na matematycznych modelach analitycznych [12, 42, 58, 77, 86]. Modele matematyczne, na podstawie których dokonywana jest analiza ryzyka, są opisywane w literaturze w sposób ilościowo ograniczony.

W pracach [12, 42, 77] do szacowania ryzyka zastosowano metody analizy, takie jak „fault-tree” czy „event-tree”, które przedstawiają sposoby określania,

`

jaki wpływ ma indywidualna usterka na system. Metody te polegają na zdefiniowaniu znanych scenariuszy ataków na dany system za pomocą grafów. Niestety, proces reprezentacji za pomocą grafów wszelkich możliwych ataków na dany system jest procesem długim oraz złożonym.

W pracy [58] do analizowania zabezpieczeń systemu komputerowego zaprezentowano metodę bazującą na teorii gier. Określono oddziaływanie pomiędzy atakującym oraz administratorem jako stochastyczną grę dla dwóch graczy. Negatywną cechą takie podejścia jest jego złożoność, ponieważ utworzenie wszystkich możliwych stanów gry jest procesem długotrwałym i skomplikowanym. Dodatkowym minusem modelu jest jego system zarządzania, a konkretnie jego mało intuicyjny charakter.

Bardzo ciekawe podejście zostało zaprezentowane przez Stewarda [86], który analizuje ryzyko na podstawie konkretnych zasobów sieci i przedstawia możliwe konsekwencje udanego ataku. Jako wejście system potrzebuje bazy danych możliwych ataków, specyfikację sieci komputerowej wraz z jej architekturą oraz profilem atakującego. Następnie za pomocą grafów określa ścieżki potencjalnych ataków, które posiadają najwyższe prawdopodobieństwo zajścia.

Wymienione wyżej modele matematyczne charakteryzują się dużą złożonością zarówno w fazie początkowej konfiguracji, jak i w fazie późniejszego nim zarządzania. Stworzenie oraz zarządzanie modelem szacującym ryzyko dla zaawansowanego protokołu kryptograficznego, którego wymogi dotyczyłyby wielu usług bezpieczeństwa, byłoby bardzo skomplikowane. Wymagałoby to utworzenie wszystkich znanych scenariuszy ataków dla wszelkich możliwych zagrożeń dla użytych w protokole zasobów.

Co więcej, takie scenariusze należałoby utworzyć dla wszystkich wymaganych usług bezpieczeństwa. Tak skomplikowane modele szacujące ryzyko nie mogą być zastosowane do podejmowanego w tej pracy zagadnienia skalowanego bezpieczeństwa, które w założeniu ma wprowadzić skalowalność dla pełnego protokołu kryptograficznego oraz wszystkich wymaganych usług ochrony informacji.

Dodatkowym powodem niewystarczalności aktualnie znanych modeli jest brak ich zależności od mechanizmów bezpieczeństwa. Aktualne modele określają ryzyko ataku na poszczególne elementy systemu nie mniej jednak nie określają, jakie mechanizmy bezpieczeństwa powinny być użyte, żeby zminimalizować ryzyko.

W przedstawianej książce zaproponowano sprowadzenie skomplikowanego modelu teoretycznego szacowania ryzyka do prostego, intuicyjnego modelu, w którym ryzyko zależne będzie od parametrów łatwo mierzalnych oraz takich, które można oszacować, choćby wykorzystując metody statystyczne.

# ROZDZIAŁ 3

## MODEL ANALITYCZNY REALIZUJĄCY SKALOWANE BEZPIECZEŃSTWO

Realizacja procesu przeprowadzanego drogą elektroniczną jest uzależniona od zagwarantowania odpowiedniego poziomu bezpieczeństwa. Przy projektowaniu elektronicznych procesów ustala się mechanizmy ochrony informacji, których poziom zazwyczaj jest zawyżony w stosunku do istniejącego ryzyka. Można zauważyć, że także w ramach konkretnego procesu elektronicznego występują zróżnicowania zagrożeń, które dotyczą przesyłanych informacji. Polegają one na różnym poziomie strat, jakie w wyniku udanego ataku na dany zasób poniosą strony realizujące protokół. W przypadku, gdy zagrożenie to jest małe, są duże możliwości zmniejszenia nadmiarowych środków ochrony informacji, co w poprawia wydajność i dostępność systemu, a w efekcie podnosi jego bezpieczeństwo. Modyfikacja mechanizmów ochrony informacji w konkretnym procesie elektronicznym realizowana jest za pomocą opisywanego modelu skalowanego bezpieczeństwa. W tym rozdziale zaprezentowana jest koncepcja skalowanego bezpieczeństwa wraz z propozycją modelu analitycznego.

## 3.1. Założenia oraz zarys modelu skalowanego bezpieczeństwa

Bezpieczne procesy elektroniczne realizowane są zwykle w postaci protokołów kryptograficznych. W tak zorganizowanych procesach możemy wprowadzić wiele usług bezpieczeństwa, które pozwalają bezpiecznie zrealizować dany proces. Protokoły kryptograficzne realizują usługi bezpieczeństwa za pośrednictwem różnych składników bezpieczeństwa, np. usług PKI lub modułów kryptograficznych. Stosowanie tych elementów bezpieczeństwa jest ściśle określone przez sformułowanie protokołu kryptograficznego, w związku z tym jakakolwiek modyfikacja ich składu jest niedopuszczalna, gdyż ma wpływ na poprawność protokołu, a zatem i na poziom bezpieczeństwa procesu elektronicznego.

Rozwiązaniem zagadnienia konieczności dynamicznej modyfikacji protokołów kryptograficznych jest stworzenie różnych protokołów realizujących tę samą usługę, lecz na innym poziomie bezpieczeństwa[1]. Używając konkretnej usługi można wybrać protokół zgodny z ustalonymi wymogami bezpieczeństwa. Niektóre elementy bezpieczeństwa warto konfigurować przed uruchomieniem usługi elektronicznej, a nie w sposób dynamiczny w trakcie jej działania. Spowodowane to jest wykorzystaniem pewnych stałych elementów bezpieczeństwa, których zmiana jest krytyczna dla konkretnych procesów.

Definiowany w tym rozdziale model skalowanego bezpieczeństwa mógłby funkcjonować jako moduł warstwy pośredniej (ang. middleware) między warstwą aplikacji, a warstwą systemową konkretnego systemu.

Bezpieczeństwo procesu elektronicznego jest uzależnione od różnych czynników, w tym zastosowanych mechanizmów bezpieczeństwa. Właśnie

[1] Dla uproszczenia rozważań, gdy w protokole kryptograficznym będzie zmieniany element nieistotny z punktu widzenia funkcjonalnej `budowy protokołu, a istotny z punktu widzenia bezpieczeństwa, zmieniony protokół będziemy to nazywać nowym protokołem.

za sprawą ich odpowiedniego doboru można regulować bezpieczeństwa procesu elektronicznego. W przedstawianej koncepcji skalowanego bezpieczeństwa [49, 52] przyjmujemy, że poziom ochrony informacji jest funkcją trzech czynników (parametrów): poziomu zabezpieczeń ($L$), prawdopodobieństwa zajścia incydentu ($P$) oraz wpływu udanego ataku na system ($\omega$). W dalszej części pracy opisane zostaną powyższe parametry.

## 3.2. Poziom zabezpieczeń

Poziom bezpieczeństwa procesów elektronicznych zależy głównie od użytych składników ochrony informacji wymaganych przez usługi bezpieczeństwa. W przedstawianej pracy wykorzystane elementy bezpieczeństwa bazują na usługach PKI oraz modułach kryptograficznych. W tab. 3.1 przedstawione jest zestawienie usług bezpieczeństwa wraz z realizującymi je mechanizmami bezpieczeństwa. Każda usługa bezpieczeństwa może być realizowana przez różne zestawienia tych mechanizmów. Między innymi od ich wyboru będzie uzależniony poziom bezpieczeństwa danego protokołu. Każdy mechanizmu bezpieczeństwa określony jest jego indywidualnym wkładem ($L^{XY}$) do globalnej ochrony danej usługi $L^X$:

$$L^X = \sum_{Y=1}^{Y=N} L^{XY} , \tag{3.1}$$

gdzie $X$ jest oznaczeniem usługi bezpieczeństwa (określanej w tabeli także przez odpowiedni skrót); $Y$ jest numerem mechanizmu bezpieczeństwa; $N$ jest liczbą wybranych mechanizmów bezpieczeństwa; $L^{XY}$ jest indywidualnym wkładem danego mechanizmu bezpieczeństwa ($Y$) do całkowitego zabezpieczenia konkretnej usługi bezpieczeństwa ($X$); $L^X$ jest całkowitym zabezpieczenie usługi bezpieczeństwa ($X$). Indywidualny wkład określany jest w procentach.

Tab. 3.1 Tabela przedstawiająca możliwe usługi bezpieczeństwa wraz ze składnikami bezpieczeństwa realizującymi te usługi.

| | | **Mechanizmy bezpieczeństwa (*Y*)** | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** |
| **Usługi bezpieczeństwa (*X*)** | **Integralność danych (I)** | Podpis cyfrowy $L^{I1}$=50% | Zaawansowane zarządzanie kluczami $L^{I2}$=10% | Zaawansowane zarządzanie certyfikatami $L^{I3}$=10% | Usługi katalogowania $L^{I4}$=5% | TTP-TTP extra weryfikacja $L^{I5}$=15% | PKG $L^{I6}$=10% | | | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | **Niezaprzeczalność Zdarzenia (NRM)** | Podpis cyfrowy $L^{NRM1}$= 30% | Znakowanie czasem $L^{NRM2}$= 15% | Zaawansowane zarządzanie kluczami $L^{NRM3}$=10% | Zaawansowane zarządzanie certyfikatami $L^{NRM4}$= 10% | Audyt $L^{NRM5}$=5% | PKI (niezaprzeczalność) $L^{NRM6}$= 10% | Usługi katalogowania $L^{NRM7}$= 5% | Repozytorium danych $L^{NRM8}$= 5% | PKG $L^{NRM9}$= 10% |
| | **Niezaprzeczalność Nadawcy (NRS)** | Podpis cyfrowy $L^{NRS1}$= 30% | Znakowanie czasem $L^{NRS2}$= 15% | Zaawansowane zarządzanie kluczami $L^{NRS3}$=10% | Zaawansowane zarządzanie certyfikatami $L^{NRS4}$= 10% | Audyt $L^{NRS5}$=5% | PKI (niezaprzeczalność) $L^{NRS6}$= 10% | Usługi katalogowania $L^{NRS7}$= 5% | Repozytorium danych $L^{NRS8}$= 5% | PKG $L^{NRS9}$= 10% |
| | **Niezaprze-Czalność odbiorcy (NRR)** | Podpis cyfrowy $L^{NRR1}$= 30% | Znakowanie czasem $L^{NRR2}$= 15% | Zaawansowane zarządzanie kluczami $L^{NRR3}$=10% | Zaawansowane zarządzanie certyfikatami $L^{NRR4}$= 10% | Audyt $L^{NRR5}$=5% | PKI (niezaprzeczalność) $L^{NRR6}$= 10% | Usługi katalogowania $L^{NRR7}$= 5% | Repozytorium danych $L^{NRR8}$= 5% | PKG $L^{NRR9}$= 10% |
| | **Poufność danych (C)** | Szyfrowanie $L^{C1}$=50% | Zaawansowane Zarządzanie kluczami $L^{C2}$=10% | Zaawansowane zarządzanie certyfikatami $L^{C3}$=10% | Schemat podziału sekretu $L^{C4}$=15% | Usługi katalogowania $L^{C5}$=5% | PKG $L^{C6}$=10% | | | |
| | **Autoryzacja stron (Au)** | PKI (rejestracja) $L^{Au1}$=20% | Podpis cyfrowy $L^{Au2}$= 20% | Zaawansowane zarządzanie kluczami $L^{Au3}$=10% | Zaawansowane zarządzanie certyfikatami $L^{Au4}$= 10% | TTP –TTP extra weryfikacja $L^{Au5}$=10% | Usługi katalogowania $L^{Au6}$=5% | PKI (autoryzacja) $L^{Au7}$= 10% | AA $L^{Au8}$= 10% | |
| | **Zarządzanie przywilejami (MP)** | PKI (rejestracja) $L^{MP1}$=50% | PKI (autoryzacja) $L^{MP2}$= 50% | | | | | | | |
| | **Anonimowość odbiorcy (AR)** | Rozgłaszanie $L^{AR1}$=100% | | | | | | | | |
| | **Anonimowość „sieciowa” (AN)** | Crowds $L^{AN1}$=40% | Anonymizer $L^{AN2}$= 60% | | | | | | | |
| | **Anonimowość wiadomości (AM)** | Numery indywidualne $L^{AM1}$= 100% | | | | | | | | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | **Wzajemne zaufanie uczestników (PTA)** | Znakowanie czasem $L^{PTA1}$= 30% | Repozytorium danych $L^{PTA2}$= 30% | Audyt $L^{PTA3}$=20% | TTP –TTP extra weryfikacja $L^{PTA4}$= 20% | | | | | |
| | **Zaufanie przez TTP (PTT)** | Znakowanie czasem $L^{PTT1}$=30% | Repozytorium danych $L^{PTT2}$= 20% | Audyt $L^{PTT3}$=10% | TTP –TTP extra weryfikacja $L^{PTT4}$= 10% | Notariat $L^{PTT5}$= 30% | | | | |
| | **Rozliczalność sieciowa (NA)** | Rejestrowanie akcji $L^{NA1}$= 50% | Audyt $L^{NA2}$= 20% | Szyfrowanie $L^{NA3}$=10% | Podpis cyfrowy $L^{NA4}$=10% | Repozytorium danych $L^{NA5}$=10% | | | | |
| | **Rozliczalność protokołu/ usługi (PA)** | Rejestrowanie akcji $L^{PA1}$= 50% | Audyt $L^{PA2}$= 20% | Szyfrowanie $L^{PA3}$=10% | Podpis cyfrowy $L^{PA4}$=10% | Repozytorium danych $L=^{PA5}$=10% | | | | |
| | **Bezpieczne przechowywanie danych (SS)** | Szyfrowanie $L^{SS1}$=30% | Znakowanie czasem $L^{SS2}$= 10% | Zaawansowane zarządzanie kluczami $L^{SS3}$=10% | Zaawansowane zarządzanie certyfikatami $L^{SS4}$=10% | PKI (niezaprzeczalność) $L^{SS5}$=10% | Repozytorium danych $L^{SS6}$=15% | Usługi katalogowania $L^{SS7}$=5% | Audyt $L^{SS8}$=5% | PKG $L^{SS9}$=5% |

Przedstawiona tabela usług bezpieczeństwa (tab. 3.1) jest tylko przykładowym zestawieniem. Można ją tworzyć w dowolny sposób, używając różnych dostępnych mechanizmów bezpieczeństwa. Wartość parametru $L^{XY}$ jest stała dla elementów danej tablicy. Podczas tworzenia protokołów o różnych poziomach bezpieczeństwa nie modyfikujemy tego parametru.

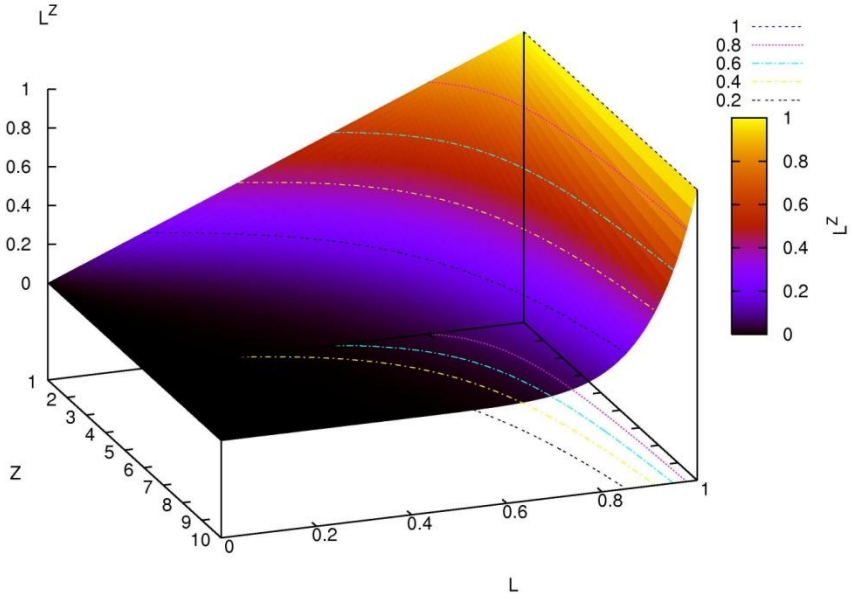
### 3.2.1. Wrażliwość mechanizmów bezpieczeństwa

W prezentowanym modelu mechanizmy bezpieczeństwa są głównymi elementami wpływającymi na zabezpieczenie usług elektronicznych. Dodatkowym czynnikiem jest wprowadzony w modelu parametr wrażliwości mechanizmów bezpieczeństwa ($Z$), który wprowadza poprawkę do uzyskanego poziomu zabezpieczeń ($L$). Przy jego pomocy można uwzględnić dodatkowe czynniki wpływające na bezpieczeństwo procesu elektronicznego. Przykładowym zagadnieniem jest zależność mechanizmów ochrony informacji. Wprowadzenie ich do systemu wiąże się z procedurami, które muszą być zrealizowane we wszystkich fazach konkretnego protokołu. Pominięcie ich w dowolnej fazie determinuje zagrożenia dla procesu, a to dalej wpływa na całkowite bezpieczeństwo systemu. Procesy realizowane drogą elektroniczną są w różnym stopniu podatne na zagrożenia pochodzące z Internetu; dzięki parametrowi wrażliwości można bardziej szczegółowo scharakteryzować

konkretny proces. Innym przykładem są procesy, które do zapewnienia minimalnego poziomu zabezpieczenia wymagają pewnego podstawowego zestawu mechanizmów bezpieczeństwa. W takich przypadkach można mówić o wzroście zabezpieczeń tylko wtedy, gdy te minimalne mechanizmy zostaną zastosowane. Wspomniany minimalny poziom można regulować za pomocą parametru wrażliwości.

Parametr określający wrażliwość mechanizmów bezpieczeństwa może przybierać wartości z przedziału (1-10); takie wartości przedziału zostały ustalone eksperymentalnie, po przeprowadzeniu szczegółowych symulacji. Na rys. 3.1 przedstawiono charakterystykę parametru określającego poziom zabezpieczeń wraz z wrażliwością mechanizmów bezpieczeństwa ($L^Z$).

Analizując rys. 3.1 można zauważyć, że gdy parametr wrażliwości mechanizmów bezpieczeństwa ($Z$) równy jest 1, to wówczas wartość parametru poziomu zabezpieczeń ($L$) pozostaje funkcją liniową swych argumentów. Wraz ze wzrostem parametru wrażliwości jego wpływ na wartość parametru poziomu zabezpieczeń rośnie. Wpływ ten charakteryzuje się zmniejszaniem obszaru, w którym parametr poziomu zabezpieczeń wraz z poprawką ($L^Z$) przekracza wartość 0,1 (czarny obszar). Skrajna sytuacja jest wówczas, gdy parametr wrażliwości ($Z$) będzie równy 10. Wówczas poziom zabezpieczeń wraz z wrażliwością ($L^Z$) nie osiągnie wartości 0,1 aż do momentu, gdy parametr $L$ nie przekroczy wartość 0,8. Zwiększając parametr wrażliwości ($Z$) można określić minimalny poziom zabezpieczeń dla danego procesu elektronicznego i dopiero wtedy, gdy zostanie on przekroczony parametr poziomu zabezpieczeń będzie wzrastał ($L^Z$).




Rys. 3.1 Charakterystyka poziomu zabezpieczeń wraz z wrażliwością mechanizmów bezpieczeństwa ($L^Z$).

## 3.3. Prawdopodobieństwo zajścia incydentu

Drugim elementem opisującym poziom bezpieczeństwa procesu elektronicznego (rozdział 3.1) jest prawdopodobieństwo zajścia incydentu [49, 52]. Jak wspominano w rozdziale 2.3, aktualnie w literaturze nie opisano metodologii, która mogłaby być zastosowany w prezentowanym modelu skalowalności mechanizmów bezpieczeństwa. W przedkładanej pracy opracowano model, który pozwala obliczyć prawdopodobieństwo wystąpienia zagrożeń, a następnie prawdopodobieństwo zajścia incydentu [50] jako funkcję zagrożeń. W prezentowanym modelu przyjęto następujący schemat logiczny. W pierwszym kroku ustalane są założenia bezpieczeństwa dla konkretnego procesu elektronicznego. Jak opisano w rozdziale 2.2, założenia bezpieczeństwa dla danego procesu możemy określić za pomocą zestawienia stosownych usług bezpieczeństwa. Wśród nich, w pierwszej kolejności należy zadbać o: poufność, integralność, niezaprzeczalność, anonimowość i dostępność danych, a następnie również o inne usługi bezpieczeństwa [55]. W kolejnym kroku dla zdefiniowanych wcześniej usług bezpieczeństwa ustalane są realizujące te usługi algorytmy kryptograficzne lub inne mechanizmy bezpieczeństwa, czyli np.: podpis cyfrowy, szyfrowanie, znakowanie czasem, wykorzystanie zaufanej trzeciej strony, schematów podziału sekretu, itd. (rozdział 2.2.2).

W prezentowanym modelu obliczane są indywidualne prawdopodobieństwa złamania poszczególnych zastosowanych mechanizmów bezpieczeństwa, a następnie wyszukiwane są te, których złamanie stanowi największe zagrożenie dla systemu. Prawdopodobieństwo zajścia incydentu jest rozumiane jako złożenie prawdopodobieństw zajścia poszczególnych zagrożeń. Dzięki takiej reprezentacji prawdopodobieństwa zajścia incydentu, osiągnięto znacznie mniejszy stopień złożoności modelu (a to ułatwia identyfikacje parametrów modelu na podstawie pomiarów i obserwacji jego działania). W takim przypadku nie należy analizować wszelkich możliwych ataków dla wszystkich dostępnych zasobów w systemie, a jedynie ataki na mechanizmy bezpieczeństwa rzeczywiście użyte w systemie. Dodatkowym atutem jest automatyczne wykrywanie zależności prawdopodobieństwa zajścia incydentu od mechanizmów bezpieczeństwa.

### 3.3.1. Parametry prawdopodobieństwa wystąpienia zagrożenia

Zestawienie aktualnie możliwych do zastosowania elementów bezpieczeństwa (tab. 3.1) jest następnie reprezentowane za pomocą grafu (rozdział 3.3.2). Wybór poszczególnych wierzchołków grafu pociąga za sobą wybór poszczególnych mechanizmów bezpieczeństwa. Mechanizmy bezpieczeństwa możliwe do zastosowania w procesie elektronicznym charakteryzowane są za pomocą zestawu dwóch grup parametrów: parametrów głównych oraz dodatkowych. Parametry przedstawione na grafie należą do głównej grupy parametrów wchodzących w skład modelu. Istnieje również

`

dodatkowa grupa parametrów, która wprowadza poprawki do modelu, ale ich wybór nie jest konieczny. Te parametry traktowane są w modelu jako pola wyboru. Poniżej przedstawiono parametry używane w modelu. Ich wartości przedstawione są głównie w postaci procentowej.

***1. Główne parametry prawdopodobieństwa (obowiązkowe) (graf):***

- *LZ* – zasoby zdobyte podczas udanego ataku na dany składnik bezpieczeństwa (100% - skompromitowanie całego protokołu) ;
- *LK* - wiedza potrzebna do przeprowadzenia ataku (100% - Ekspert) ;
- *LP* - koszt potrzebny do przeprowadzenia ataku (100% - najwyższy koszt);
- *C* - kroki komunikacji, jako dodatkowa możliwość ataku, $C \in [0 \div 0{,}1]$ (0,1 – największe zagrożenie);
- *M* - praktyczna implementacja. Trudność implementacji zwiększa prawdopodobieństwo nieprawidłowej konfiguracji. Raporty o błędach jako dodatkowe źródło informacji, itd., $M \in [0 \div 0{,}1]$ (0,1 – największe zagrożenie).

***Dodatkowe parametry bezpieczeństwa (opcjonalne) (lista wyboru):***

- *PP* - globalne zasoby możliwe do zdobycia w danym, konkretnym procesie, $PP \in [0 \div 0{,}1]$ (0,1 – maksymalne zagrożenie);
- *I* - rodzaj instytucji realizującej proces. Niektóre instytucje są narażone na większe zagrożenie, $I \in [0 \div 0{,}1]$ (0,1 – największe zagrożenie);
- *H* - hipotetyczne ryzyko poniesione przez atakującego w wyniku wykrycia włamania. Zależy od stosowanego prawodawstwa oraz penalizacji
  w krajach, gdzie przeprowadzany jest proces, $H \in [0 \div 0{,}1]$ (0,1-najmniej restrykcyjny kraj).

## 3.3.2. Graf usług bezpieczeństwa

Możliwe do zastosowania w procesie elektronicznym mechanizmy bezpieczeństwa przedstawiane są za pomocą grafu. Wybór poszczególnych wierzchołków grafu jest równoznaczny z wyborem konkretnych składników bezpieczeństwa. Wybierając konkretny element bezpieczeństwa, zestawiamy numery węzłów poszczególnych gałęzi grafu, łącząc je kropkami. Każdy węzeł

scharakteryzowany jest za pomocą parametrów głównych przewidzianych w modelu, szczegółowy opis znajduje się w rozdziale 3.3.1. Określenie wartości parametrów głównych jest poprzedzone szczegółową analizą wrażliwości wspomnianych składników. W pracy wartości te zostały dobrane w sposób intuicyjny, na podstawie analizy danych statystycznych dotyczących ataków (przedstawionych w rozdziale 2) oraz doświadczenia autora.

Wybór mechanizmów bezpieczeństwa nie może być dowolny, ponieważ jest on weryfikowany za pomocą funkcji boolowskich. Poszczególne wierzchołki grafu usług bezpieczeństwa łączą się ze sobą za pomocą krawędzi, do których przypisane są operacje boolowskie. Wybierając konkretną gałąź, tworzymy jednocześnie funkcję boolowską poszczególnych składników bezpieczeństwa. Warunkiem poprawności dokonanego wyboru jest wynik otrzymanych funkcji boolowskich równy 1.

Niektóre składniki bezpieczeństwa (wierzchołki grafu) mają taką właściwość, że ich wybór modyfikuje parametry wierzchołków grafu leżących na tym samym poziomie. Ta funkcjonalność jest oznaczana w postaci znaku „+", znajdującego się przy odpowiednim parametrze (np. 3.1.8 - LK=+5%, LP=+5%).

Dodatkowym oznaczeniem używanym w grafach jest „dziedziczenie". Wierzchołki tak oznaczone przyjmują najwyższe wartości parametrów z niższych gałęzi grafu.

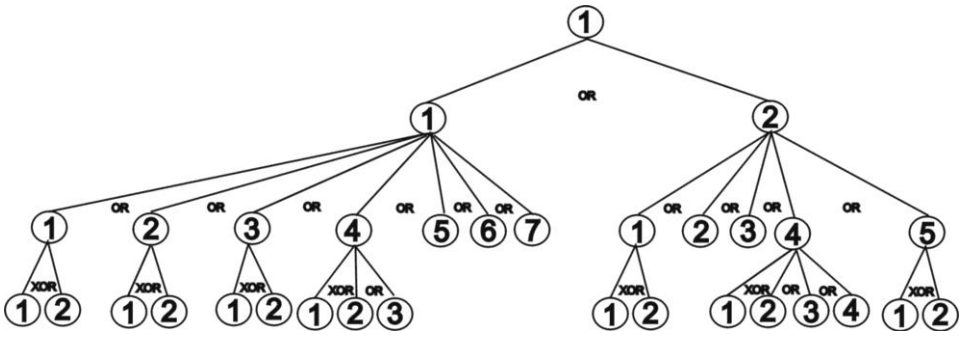
W dalszej części rozdziału za pomocą grafów wykonano zestawienie usług bezpieczeństwa wraz z mechanizmami bezpieczeństwa, które zawarte są w tab. 3.1 (rozdział 3.2). Wspomniane grafy zostały utworzone jedynie dla usług bezpieczeństwa, które będą wykorzystywane w przykładzie zaprezentowanym w dalszej części pracy. Dla każdej usługi bezpieczeństwa tworzymy osobny graf:

- Graf 1 – usługa integralności (rys. 3.2);
- Graf 2 – usługa poufności (rys. 3.3);
- Graf 3 – usługa niezaprzeczalności (rys. 3.4);
- Graf 4 – usługa bezpiecznego przechowywania danych (rys. 3.5);
- Graf 5 – usługa autoryzacji stron (rys. 3.6);
- Graf 6 – usługa zarządzania przywilejami (rys. 3.7).

Ze względu na przejrzystość opisu wierzchów grafów nie może on być obszerny, powinien być przedstawiony w sposób skrócony. Przy wielu wierzchołkach (np. 1.1.1.1, 1.1.3.1, 2.1.1) znajduje się ogólny opis: „Moduły kryptograficzne (min. poziom 2) [33]". Skrót ten oznacza, że dla tego wierzchołka i konkretnego elementu bezpieczeństwa będzie realizowany taki poziom zabezpieczeń, który jest określony dla modułów kryptograficznych, zaszeregowanych przez stosowne normy na minimum drugim poziomie. Zestawienie poziomów zabezpieczeń w zależności od poziomów tych modułów jest opisane w normach, do których jest przypisane cytowanie, w tym przypadku [33].

`

Warto zwrócić uwagę, że opisy grafów mają charakter specyfikacji technicznej, a nie szczegółowo omówionej dokumentacji. Poniżej przedstawiamy poszczególne grafy bezpieczeństwa wraz z ich opisami.




Rys. 3.2 Graf dla usługi integralności.

**1. Integralność**

1.1 Podpis cyfrowy *(LZ,LK,LP= dziedziczenie)*

1.1.1 Zarządzanie kluczami kryptograficznymi *(LZ,LK,LP = dziedziczenie)*

1.1.1.1 Moduły kryptograficzne (min. poziom 2) [33] (LZ=80%, LK=70%, LP=80%, C=0,05, M=0,01)

1.1.1.2 Moduły kryptograficzne (min. poziom 3) [33] (LZ=80%, LK=80%, LP=90%, C=0,05, M=0,02)

1.1.2 Porty i interfejsy modułów kryptograficznych *(LZ,LK,LP = dziedziczenie)*

1.1.2.1 Moduły kryptograficzne (min. poziom 2) [33] (LZ=70%, LK=50%, LP=80%)

1.1.2.2 Moduły kryptograficzne (min. poziom 3) [33] (LZ=70%, LK=70%, LP=80%)

1.1.3 Specyfikacja modułów kryptograficznych *(LZ,LK,LP = dziedziczenie)*

1.1.3.1 Moduły kryptograficzne (min. poziom 2) [33] (LZ=70%, LK=50%, LP=80%)

1.1.3.2 Moduły kryptograficzne (min. poziom 3) [33] (LZ=70%, LK=70%, LP=80%)

1.1.4 Generowanie kluczy *(LZ,LK,LP= dziedziczenie* )

1.1.4.1 Moduły kryptograficzne (min. poziom 2) [20], Techniki bezpieczeństwa (min. EAL 3) [33] (LZ=80%, LK=70%, LP=80%)

1.1.4.2 Moduły kryptograficzne (min. poziom 3) [20], Techniki bezpieczeństwa (min. EAL 4) [33], (LZ=80%, LK=80%, LP=90%, M=0,01)

1.1.4.3 Generowanie kluczy przy użyciu mechanizmu PKG (LZ=80%, LK=100%, LP=100%, M=0,02) (LK+5%, LP=+5%)

1.1.5 Rozpowszechnianie kluczy (LZ=80%, LK=50%, LP=80%, C=0,02)

1.1.6 Użycie kluczy (LZ=80%, LK=80%, LP=50%)

1.1.7 Zakończenie cyklu kluczy (LZ=30%, LK=80%, LP=50%, C=0,01)

1.2 Zarządzanie certyfikatami *(LZ,LK,LP= dziedziczenie)*

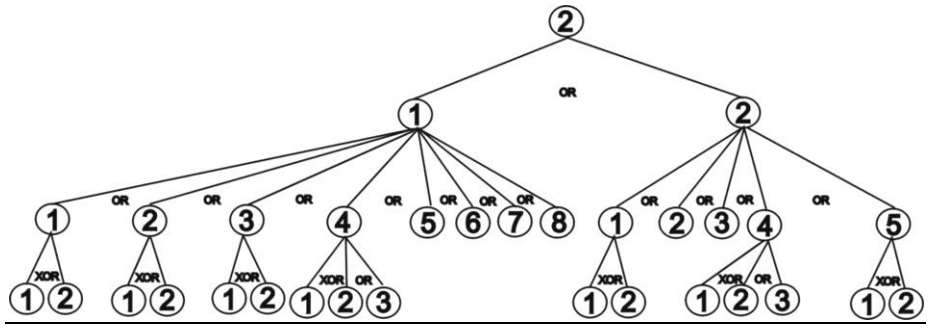
1.2.1 Rejestracja podmiotu *(LZ,LK,LP= dziedziczenie)*
- 1.2.1.1 Szczegółowa weryfikacja strony ubiegającej się o certyfikat (LZ=70%, LK=30%, LP=90%, C=0,02)
- 1.2.1.2 Podstawowa weryfikacja stron ubiegających się o certyfikat (LZ=70%, LK=20%, LP=70%, C=0,02, M=0,01)

1.2.2 Uaktualnienie certyfikatu (LZ=70%, LK=50%, LP=30%, C=0,02)

1.2.3 Generowanie certyfikatu (LZ=70%, LK=80%, LP=80%, M=0,01)

1.2.4 Rozgłaszanie certyfikatu *(LZ,LK,LP= dziedziczenie)*
- 1.2.4.1 Weryfikacja certyfikatów jest możliwa zgodnie z warunkami ustalonymi przez dany C.A. (LZ=30%, LK=60%, LP=30%, C=0,03, M=0,01)
- 1.2.4.2 Weryfikacja certyfikatów jest możliwa 24h na dobę, 7 dni w tygodniu (LZ=30%, LK=80%, LP=30%, C=0,03, M=0,02)
- 1.2.4.3 Weryfikacja certyfikatów jest dodatkowo sprawdzana przez inne TTP (LZ=30%, LK=80%, LP=70%,C=0,02, M=0,01) (LK+5%, LP+5%)
- 1.2.4.4 Informacje o właścicielach certyfikatów jest dostępna zgodnie z wcześniej ustalonymi prawami dostępu (usług katalogowania) (LZ=15%, LK=50%, LP=30%) ( LK+5%, LP+5%)

1.2.5 Zawieszenie i odwołanie certyfikatu *(LZ,LK,LP= dziedziczenie)*
- 1.2.5.1 Odwołanie certyfikatu oraz zmodyfikowanie list certyfikatów (CRL) w ciągu 72h od uzyskania stosownego żądania (LZ=30%, LK=60%, LP=40%, C=0,01)
- 1.2.5.2 Odwołanie certyfikatu oraz zmodyfikowanie list certyfikatów (CRL) w ciągu 24h od uzyskania stosownego żądania *(*LZ=30%, LK=80%, LP=40%, C=0,01, M=0,01*)*




Rys. 3.3 Graf dla usługi poufności.

**2. Poufność**

2.1 Szyfrowanie *(LZ,LK,LP= dziedziczenie)*

2.1.1 Zarządzanie kluczami kryptograficznymi *(LZ,LK,LP = dziedziczenie)*
- 2.1.1.1 Moduły kryptograficzne (min. poziom 2) [33] (LZ=80%, LK=70%, LP=80%, C=0,05, M=0,01)
- 2.1.1.2 Moduły kryptograficzne (min. poziom 3) [33] (LZ=80%, LK=80%, LP=90%, C=0,05, M=0,02)

2.1.2 Porty i interfejsy modułów kryptograficznych *(LZ,LK,LP = dziedziczenie)*

`

2.1.2.1 Moduły kryptograficzne (min. poziom 2) [33] (LZ=70%, LK=50%, LP=80%)

2.1.2.2 Moduły kryptograficzne (min. poziom 3) [33] (LZ=70%, LK=70%, LP=80%)

2.1.3 Specyfikacja modułów kryptograficznych *(LZ,LK,LP = dziedziczenie)*

2.1.3.1 Moduły kryptograficzne (min. poziom 2) [33] (LZ=70%, LK=50%, LP=80%)

2.1.3.2 Moduły kryptograficzne (min. poziom 3) [33] (LZ=70%, LK=70%, LP=80%)

2.1.4 Generowanie kluczy *(LZ,LK,LP= dziedziczenie* )

2.1.4.1 Moduły kryptograficzne (min. poziom 2) [20], Techniki bezpieczeństwa (min. EAL 3) [42] (LZ=80%, LK=70%, LP=80%)

2.1.4.2 Moduły kryptograficzne (min. poziom 3) [20], Techniki bezpieczeństwa (min. EAL 4) [33], (LZ=80%, LK=80%, LP=90%, M=0,01)

2.1.4.3 Generowanie kluczy przy użyciu mechanizmu PKG (LZ=80%, LK=100%, LP=100%, M=0,02) (LK+5%, LP=+5%)

2.1.5 Rozpowszechnianie kluczy (LZ=80%, LK=50%, LP=80%, C=0,02)

2.1.6 Użycie kluczy (LZ=80%, LK=80%, LP=50%)

2.1.7 Zakończenie cyklu kluczy (LZ=30%, LK=80%, LP=50%, C=0,01)

2.1.8 Bezpieczny schemat podziału sekretu (SSS) (LZ=50%, LK=80%, LP=80%, M=0,02, C=0,05)

2.2 Zarządzanie certyfikatami *(LZ,LK,LP= dziedziczenie)*

2.2.1 Rejestracja podmiotu *(LZ,LK,LP= dziedziczenie)*

2.2.1.1 Szczegółowa weryfikacja strony ubiegającej się o certyfikat (LZ=70%, LK=30%, LP=90%, C=0,02)

2.2.1.2 Podstawowa weryfikacja stron ubiegających się o certyfikat (LZ=70%, LK=20%, LP=70%, C=0,02, M=0,01)

2.2.2 Uaktualnienie certyfikatu (LZ=70%, LK=50%, LP=30%, C=0,02)

2.2.3 Generowanie certyfikatu (LZ=70%, LK=80%, LP=80%, M=0,01)

2.2.4 Rozgłaszanie certyfikatu *(LZ,LK,LP= dziedziczenie)*

2.2.4.1 Weryfikacja certyfikatów jest możliwa zgodnie z warunkami ustalonymi przez dany C.A. (LZ=30%, LK=60%, LP=30%, C=0,03, M=0,01)

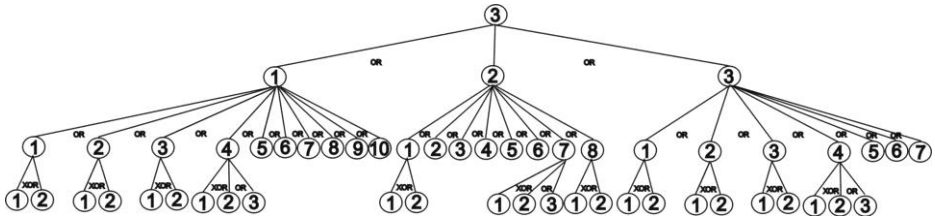
2.2.4.2 Weryfikacja certyfikatów jest możliwa 24h na dobę, 7 dni w tygodniu (LZ=30%, LK=80%, LP=30%, C=0,03, M=0,02)

2.2.4.3 Informacje o właścicielach certyfikatów jest dostępna zgodnie z wcześniej ustalonymi prawami dostępu (usług katalogowania) (LZ=15%, LK=50%, LP=30%) ( LK+5%, LP+5%)

2.2.5 Zawieszenie i odwołanie certyfikatu *(LZ,LK,LP= dziedziczenie)*

2.2.5.1 Odwołanie certyfikatu oraz zmodyfikowanie list certyfikatów (CRL) w ciągu 72h od uzyskania stosownego żądania (LZ=30%, LK=60%, LP=40%, C=0,01)

2.2.5.2 Odwołanie certyfikatu oraz zmodyfikowanie list certyfikatów (CRL) w ciągu 24h od uzyskania stosownego żądania *(*LZ=30%, LK=80%, LP=40%, C=0,01, M=0,01*)*



Rys. 3.4 Graf dla usługi niezaprzeczalności.

**3. Niezaprzeczalność**

3.1 Podpis cyfrowy *(LZ,LK,LP= dziedziczenie)*

3.1.1 Zarządzanie kluczami kryptograficznymi *(LZ,LK,LP = dziedziczenie)*

3.1.1.1 Moduły kryptograficzne (min. poziom 2) [33] (LZ=80%, LK=70%, LP=80%, C=0,05, M=0,01)

3.1.1.2 Moduły kryptograficzne (min. poziom 3) [33] (LZ=80%, LK=80%, LP=90%, C=0,05, M=0,02)

3.1.2 Porty i interfejsy modułów kryptograficznych *(LZ,LK,LP = dziedziczenie)*

3.1.2.1 Moduły kryptograficzne (min. poziom 2) [33] (LZ=70%, LK=50%, LP=80%)

3.1.2.2 Moduły kryptograficzne (min. poziom 3) [33] (LZ=70%, LK=70%, LP=80%)

3.1.3 Specyfikacja modułów kryptograficznych *(LZ,LK,LP = dziedziczenie)*

3.1.3.1 Moduły kryptograficzne (min. poziom 2) [33] (LZ=70%, LK=50%, LP=80%)

3.1.3.2 Moduły kryptograficzne (min. poziom 3) [33] (LZ=70%, LK=70%, LP=80%)

3.1.4 Generowanie kluczy *(LZ,LK,LP= dziedziczenie* )

3.1.4.1 Moduły kryptograficzne (min. poziom 2) [20], Techniki bezpieczeństwa (min. EAL 3) [42] (LZ=80%, LK=70%, LP=80%)

3.1.4.2 Moduły kryptograficzne (min. poziom 3) [20], Techniki bezpieczeństwa (min. EAL 4) [33], (LZ=80%, LK=80%, LP=90%, M=0,01)

3.1.4.3 Generowanie kluczy przy użyciu mechanizmu PKG (LZ=80%, LK=100%, LP=100%, M=0,02) (LK+5%, LP=+5%)

3.1.5 Rozpowszechnianie kluczy (LZ=80%, LK=50%, LP=80%, C=0,02)

3.1.6 Użycie kluczy (LZ=80%, LK=80%, LP=50%)

3.1.7 Zakończenie cyklu kluczy (LZ=30%, LK=80%, LP=50%, C=0,01)

3.1.8 Wewnętrzny audyt (LZ=10%, LK=60%, LP=40%, C=0,01, M=0,03) (LK=+5%, LP=+5%)

3.1.9 Niezaprzeczalność PKI (LZ=50%, LK=70%, LP=70%, C=0,04, M=0,03) (LK=+3%, LP=+3%)

3.1.10 Repozytorium danych (LZ=70%, LK=90%, LP=90%, M=0,02) (LK=+2%, LP=+2%)

3.2 Zarządzanie certyfikatami *(LZ,LK,LP= dziedziczenie)*

3.2.1 Rejestracja podmiotu *(LZ,LK,LP= dziedziczenie)*

3.2.1.1 Szczegółowa weryfikacja strony ubiegającej się o certyfikat (LZ=70%, LK=30%, LP=90%, C=0,02)

`

3.2.1.2 Podstawowa weryfikacja stron ubiegających się o certyfikat (LZ=70%, LK=20%, LP=70%, C=0,02, M=0,01)

3.2.2 Uaktualnienie certyfikatu (LZ=70%, LK=50%, LP=30%, C=0,02)

3.2.3 Generowanie certyfikatu (LZ=70%, LK=80%, LP=80%, M=0,01)

3.2.4 Wewnętrzny audyt (LZ=10%, LK=60%, LP=40%, C=0,01, M=0,03) (LK=+5%, LP=+5%)

3.2.5 Niezaprzeczalność PKI (LZ=50%, LK=70%, LP=70%, C=0,04, M=0,03) (LK=+3%, LP=+3%)

3.2.6 Repozytorium danych (LZ=70%, LK=90%, LP=90%, M=0,02) (LK=+2%, LP=+2%)

3.2.7 Rozgłaszanie certyfikatu *(LZ,LK,LP= dziedziczenie)*

3.2.7.1 Weryfikacja certyfikatów jest możliwa zgodnie z warunkami ustalonymi przez dany C.A. (LZ=30%, LK=60%, LP=30%, C=0,03, M=0,01)

3.2.7.2 Weryfikacja certyfikatów jest możliwa 24h na dobę, 7 dni w tygodniu (LZ=30%, LK=80%, LP=30%, C=0,03, M=0,02)

3.2.7.3 Informacje o właścicielach certyfikatów jest dostępna zgodnie z wcześniej ustalonymi prawami dostępu (usług katalogowania) (LZ=15%, LK=50%, LP=30%) ( LK+5%, LP+5%)

3.2.8 Zawieszenie i odwołanie certyfikatu *(LZ,LK,LP= dziedziczenie)*

3.2.8.1 Odwołanie certyfikatu oraz zmodyfikowanie list certyfikatów (CRL) w ciągu 72h od uzyskania stosownego żądania (LZ=30%, LK=60%, LP=40%, C=0,01)

3.2.8.2 Odwołanie certyfikatu oraz zmodyfikowanie list certyfikatów (CRL) w ciągu 24h od uzyskania stosownego żądania *(*LZ=30%, LK=80%, LP=40%, C=0,01, M=0,01*)*

3.3 Znakowanie czasem *(LZ,LK,LP= dziedziczenie)*

3.3.1 Zarządzanie kluczami kryptograficznymi *(LZ,LK,LP = dziedziczenie)*

3.3.1.1 Moduły kryptograficzne (min. poziom 2) [33] (LZ=80%, LK=70%, LP=80%, C=0,05, M=0,01)

3.3.1.2 Moduły kryptograficzne (min. poziom 3) [33] (LZ=80%, LK=80%, LP=90%, C=0,05, M=0,02)

3.3.2 Porty i interfejsy modułów kryptograficznych *(LZ,LK,LP = dziedziczenie)*

3.3.2.1 Moduły kryptograficzne (min. poziom 2) [33] (LZ=70%, LK=50%, LP=80%)

3.3.2.2 Moduły kryptograficzne (min. poziom 3) [33] (LZ=70%, LK=70%, LP=80%)

3.3.3 Specyfikacja modułów kryptograficznych *(LZ,LK,LP = dziedziczenie)*

3.3.3.1 Moduły kryptograficzne (min. poziom 2) [33] (LZ=70%, LK=50%, LP=80%)

3.3.3.2 Moduły kryptograficzne (min. poziom 3) [33] (LZ=70%, LK=70%, LP=80%)

3.3.4 Generowanie kluczy *(LZ,LK,LP= dziedziczenie* )

3.3.4.1 Moduły kryptograficzne (min. poziom 2) [20], Techniki bezpieczeństwa (min. EAL 3) [42] (LZ=80%, LK=70%, LP=80%)

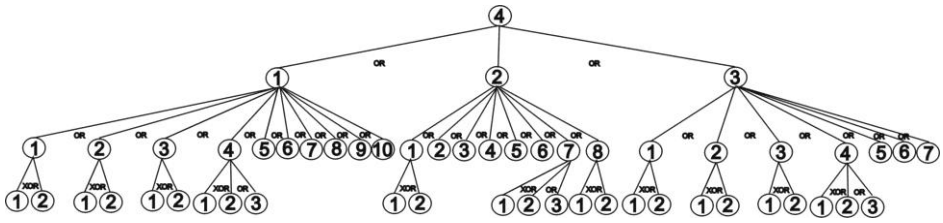
3.3.4.2 Moduły kryptograficzne (min. poziom 3) [20], Techniki bezpieczeństwa (min. EAL 4) [42], (LZ=80%, LK=80%, LP=90%, M=0,01)

3.3.4.3 Generowanie kluczy przy użyciu mechanizmu PKG (LZ=80%, LK=100%, LP=100%, M=0,02) (LK+5%, LP=+5%)

3.3.5 Wewnętrzny Audyt (LZ=10%, LK=60%, LP=40%, C=0,01, M=0,03) (LK=+5%, LP=+5%)

3.3.6 Niezaprzeczalność PKI (LZ=50%, LK=70%, LP=70%, C=0,04, M=0,03) (LK=+3%, LP=+3%)

3.3.7 Repozytorium danych (LZ=70%, LK=90%, LP=90%, M=0,02) (LK=+2%, LP=+2%)



Rys. 3.5 Graf dla usługi bezpiecznego przechowywania danych.

**4. Bezpieczne przechowywanie danych**

4.1 Szyfrowanie *(LZ,LK,LP= dziedziczenie)*

4.1.1 Zarządzanie kluczami kryptograficznymi *(LZ,LK,LP = dziedziczenie)*

4.1.1.1 Moduły kryptograficzne (min. poziom 2) [33] (LZ=80%, LK=70%, LP=80%, C=0,05, M=0,01)

4.1.1.2 Moduły kryptograficzne (min. poziom 3) [33] (LZ=80%, LK=80%, LP=90%, C=0,05, M=0,02)

4.1.2 Porty i interfejsy modułów kryptograficznych *(LZ,LK,LP = dziedziczenie)*

4.1.2.1 Moduły kryptograficzne (min. poziom 2) [33] (LZ=70%, LK=50%, LP=80%)

4.1.2.2 Moduły kryptograficzne (min. poziom 3) [33] (LZ=70%, LK=70%, LP=80%)

4.1.3 Specyfikacja modułów kryptograficznych *(LZ,LK,LP = dziedziczenie)*

4.1.3.1 Moduły kryptograficzne (min. poziom 2) [33] (LZ=70%, LK=50%, LP=80%)

4.1.3.2 Moduły kryptograficzne (min. poziom 3) [33] (LZ=70%, LK=70%, LP=80%)

4.1.4 Generowanie kluczy *(LZ,LK,LP= dziedziczenie* )

4.1.4.1 Moduły kryptograficzne (min. poziom 2) [20], Techniki bezpieczeństwa (min. EAL 3) [33] (LZ=80%, LK=70%, LP=80%)

4.1.4.2 Moduły kryptograficzne (min. poziom 3) [20], Techniki bezpieczeństwa (min. EAL 4) [33], (LZ=80%, LK=80%, LP=90%, M=0,01)

4.1.4.3 Generowanie kluczy przy użyciu mechanizmu PKG (LZ=80%, LK=100%, LP=100%, M=0,02) (LK+5%, LP=+5%)

4.1.5 Rozpowszechnianie kluczy (LZ=80%, LK=50%, LP=80%, C=0,02)

4.1.6 Użycie kluczy (LZ=80%, LK=80%, LP=50%)

4.1.7 Zakończenie cyklu kluczy (LZ=30%, LK=80%, LP=50%, C=0,01)

`

4.1.8 Wewnętrzny Audyt (LZ=10%, LK=60%, LP=40%, C=0,01, M=0,03) (LK=+5%, LP=+5%)
4.1.9 Niezaprzeczalność PKI (LZ=50%, LK=70%, LP=70%, C=0,04, M=0,03) (LK=+3%, LP=+3%)
4.1.10 Repozytorium danych (LZ=70%, LK=90%, LP=90%, M=0,02) (LK=+2%, LP=+2%)

4.2 Zarządzanie certyfikatami *(LZ,LK,LP= dziedziczenie)*
4.2.1 Rejestracja podmiotu *(LZ,LK,LP= dziedziczenie)*
4.2.1.1 Szczegółowa weryfikacja strony ubiegającej się o certyfikat (LZ=70%, LK=30%, LP=90%, C=0,02)
4.2.1.2 Podstawowa weryfikacja stron ubiegających się o certyfikat (LZ=70%, LK=20%, LP=70%, C=0,02, M=0,01)
4.2.2 Uaktualnienie certyfikatu (LZ=70%, LK=50%, LP=30%, C=0,02)
4.2.3 Generowanie certyfikatu (LZ=70%, LK=80%, LP=80%, M=0,01)
4.2.4 Wewnętrzny Audyt (LZ=10%, LK=60%, LP=40%, C=0,01, M=0,03) (LK=+5%, LP=+5%)
4.2.5 Niezaprzeczalność PKI (LZ=50%, LK=70%, LP=70%, C=0,04, M=0,03) (LK=+3%, LP=+3%)
4.2.6 Repozytorium danych (LZ=70%, LK=90%, LP=90%, M=0,02) (LK=+2%, LP=+2%)
4.2.7 Rozgłaszanie certyfikatu *(LZ,LK,LP= dziedziczenie)*
4.2.7.1 Weryfikacja certyfikatów jest możliwa zgodnie z warunkami ustalonymi przez dany C.A. (LZ=30%, LK=60%, LP=30%, C=0,03, M=0,01)
4.2.7.2 Weryfikacja certyfikatów jest możliwa 24h na dobę, 7 dni w tygodniu (LZ=30%, LK=80%, LP=30%, C=0,03, M=0,02)
4.2.7.3 Informacje o właścicielach certyfikatów jest dostępna zgodnie z wcześniej ustalonymi prawami dostępu (usług katalogowania) (LZ=15%, LK=50%, LP=30%) ( LK+5%, LP+5%)
4.2.8 Zawieszenie i odwołanie certyfikatu *(LZ,LK,LP= dziedziczenie)*
4.2.8.1 Odwołanie certyfikatu oraz zmodyfikowanie list certyfikatów (CRL) w ciągu 72h od uzyskania stosownego żądania (LZ=30%, LK=60%, LP=40%, C=0,01)
4.2.8.2 Odwołanie certyfikatu oraz zmodyfikowanie list certyfikatów (CRL) w ciągu 24h od uzyskania stosownego żądania *(*LZ=30%, LK=80%, LP=40%, C=0,01, M=0,01*)*

4.3 Znakowanie czasem *(LZ,LK,LP= dziedziczenie)*
4.3.1 Zarządzanie kluczami kryptograficznymi *(LZ,LK,LP = dziedziczenie)*
4.3.1.1 Moduły kryptograficzne (min. poziom 2) [33] (LZ=80%, LK=70%, LP=80%, C=0,05, M=0,01)
4.3.1.2 Moduły kryptograficzne (min. poziom 3) [33] (LZ=80%, LK=80%, LP=90%, C=0,05, M=0,02)
4.3.2 Porty i interfejsy modułów kryptograficznych *(LZ,LK,LP = dziedziczenie)*
4.3.2.1 Moduły kryptograficzne (min. poziom 2) [33] (LZ=70%, LK=50%, LP=80%)
4.3.2.2 Moduły kryptograficzne (min. poziom 3) [33] (LZ=70%, LK=70%, LP=80%)
4.3.3 Specyfikacja modułów kryptograficznych *(LZ,LK,LP = dziedziczenie)*

4.3.3.1 Moduły kryptograficzne (min. poziom 2) [33] (LZ=70%, LK=50%, LP=80%)

4.3.3.2 Moduły kryptograficzne (min. poziom 3) [33] (LZ=70%, LK=70%, LP=80%)

4.3.4 Generowanie kluczy *(LZ,LK,LP= dziedziczenie* )

4.3.4.1 Moduły kryptograficzne (min. poziom 2) [20], Techniki bezpieczeństwa (min. EAL 3) [33] (LZ=80%, LK=70%, LP=80%)

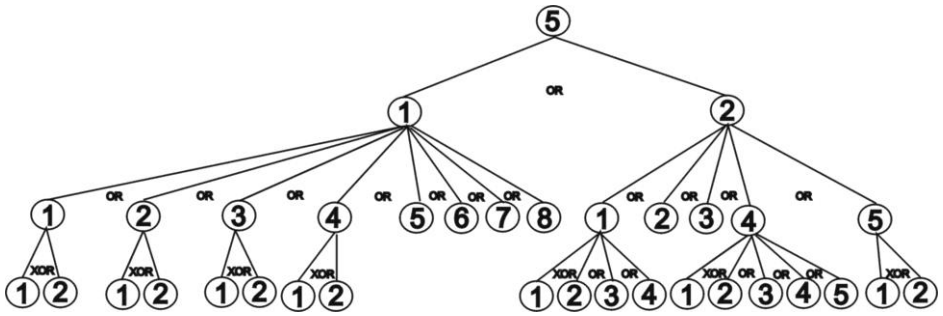
4.3.4.2 Moduły kryptograficzne (min. poziom 3) [20], Techniki bezpieczeństwa (min. EAL 4) [33], (LZ=80%, LK=80%, LP=90%, M=0,01)

4.3.4.3 Generowanie kluczy przy użyciu mechanizmu PKG (LZ=80%, LK=100%, LP=100%, M=0,02) (LK+5%, LP=+5%)

4.3.5 Wewnętrzny Audyt (LZ=10%, LK=60%, LP=40%, C=0,01, M=0,03) (LK=+5%, LP=+5%)

4.3.6 Niezaprzeczalność PKI (LZ=50%, LK=70%, LP=70%, C=0,04, M=0,03) (LK=+3%, LP=+3%)

4.3.7 Repozytorium danych (LZ=70%, LK=90%, LP=90%, M=0,02) (LK=+2%, LP=+2%)




Rys. 3.6 Graf dla usługi autoryzacji stron.

**5. Autoryzacja stron**

5.1 Podpis cyfrowy *(LZ,LK,LP= dziedziczenie)*

5.1.1 Zarządzanie kluczami kryptograficznymi *(LZ,LK,LP = dziedziczenie)*

5.1.1.1 Moduły kryptograficzne (min. poziom 2) [33] (LZ=80%, LK=70%, LP=80%, C=0,05, M=0,01)

5.1.1.2 Moduły kryptograficzne (min. poziom 3) [33] (LZ=80%, LK=80%, LP=90%, C=0,05, M=0,02)

5.1.2 Porty i interfejsy modułów kryptograficznych *(LZ,LK,LP = dziedziczenie)*

5.1.2.1 Moduły kryptograficzne (min. poziom 2) [33] (LZ=70%, LK=50%, LP=80%)

5.1.2.2 Moduły kryptograficzne (min. poziom 3) [33] (LZ=70%, LK=70%, LP=80%)

5.1.3 Specyfikacja modułów kryptograficznych *(LZ,LK,LP = dziedziczenie)*

5.1.3.1 Moduły kryptograficzne (min. poziom 2) [33] (LZ=70%, LK=50%, LP=80%)

`

5.1.3.2 Moduły kryptograficzne (min. poziom 3) [33] (LZ=70%, LK=70%, LP=80%)

5.1.4 Generowanie kluczy *(LZ,LK,LP= dziedziczenie* )

5.1.4.1 Moduły kryptograficzne (min. poziom 2) [20], Techniki bezpieczeństwa (min. EAL 3) [33] (LZ=80%, LK=70%, LP=80%)

5.1.4.2 Moduły kryptograficzne (min. poziom 3) [20], Techniki bezpieczeństwa (min. EAL 4) [33], (LZ=80%, LK=80%, LP=90%, M=0,01)

5.1.5 Rozpowszechnianie kluczy (LZ=80%, LK=50%, LP=80%, C=0,02)

5.1.6 Użycie kluczy (LZ=80%, LK=80%, LP=50%)

5.1.7 Zakończenie cyklu kluczy (LZ=30%, LK=80%, LP=50%, C=0,01)

5.1.8 Wewnętrzny Audyt (LZ=10%, LK=60%, LP=40%, C=0,01, M=0,03) (LK=+5%, LP=+5%)

5.2 Zarządzanie certyfikatami *(LZ,LK,LP= dziedziczenie)*

5.2.1 Rejestracja podmiotu *(LZ,LK,LP= dziedziczenie)*

5.2.1.1 Szczegółowa weryfikacja strony ubiegającej się o certyfikat (LZ=70%, LK=30%, LP=90%, C=0,02)

5.2.1.2 Podstawowa weryfikacja stron ubiegających się o certyfikat (LZ=70%, LK=20%, LP=70%, C=0,02, M=0,01)

5.2.1.3 PKI_Rejestracja (LZ=50%, LK=70%, LP=60%, C=0,02, M=0,01) (LK+5%, LP+5%)

5.2.1.4 PKI_Autoryzacja (LZ=30%, LK=60%, LP=60%, M=0,05) (LK+10%, LP+5%)

5.2.2 Uaktualnienie certyfikatu (LZ=70%, LK=50%, LP=30%, C=0,02)

5.2.3 Generowanie certyfikatu (LZ=70%, LK=80%, LP=80%, M=0,01)

5.2.4 Rozgłaszanie certyfikatu *(LZ,LK,LP= dziedziczenie)*

5.2.4.1 Weryfikacja certyfikatów jest możliwa zgodnie z warunkami ustalonymi przez dany C.A. (LZ=30%, LK=60%, LP=30%, C=0,03, M=0,01)

5.2.4.2 Weryfikacja certyfikatów jest możliwa 24h na dobę, 7 dni w tygodniu (LZ=30%, LK=80%, LP=30%, C=0,03, M=0,02)

5.2.4.3 Weryfikacja certyfikatów jest dodatkowo sprawdzana przez inne TTP (LZ=30%, LK=80%, LP=70%,C=0,02, M=0,01) (LK+5%, LP+5%)

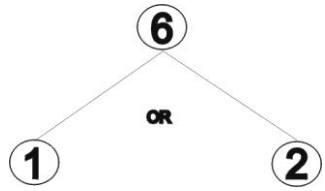
5.2.4.4 Informacje o właścicielach certyfikatów jest dostępna zgodnie z wcześniej ustalonymi prawami dostępu (usługa katalogowania) (LZ=15%, LK=50%, LP=30%) ( LK+5%, LP+5%)

5.2.4.5 Anonimowa autoryzacja (LZ=20%, LK=60%, LP=60%, C=0,03, M=0,03) (LK+10%, LP+5%)

5.2.5 Zawieszenie i odwołanie certyfikatu *(LZ,LK,LP= dziedziczenie)*

5.2.5.1 Odwołanie certyfikatu oraz zmodyfikowanie list certyfikatów (CRL) w ciągu 72h od uzyskania stosownego żądania (LZ=30%, LK=60%, LP=40%, C=0,01)

5.2.5.2 Odwołanie certyfikatu oraz zmodyfikowanie list certyfikatów (CRL) w ciągu 24h od uzyskania stosownego żądania *(*LZ=30%, LK=80%, LP=40%, C=0,01, M=0,01*)*




Rys. 3.7 Graf dla usługi zarządzania przywilejami.

**6. Zarządzanie przywilejami**
6.1 PKI_Rejestracja (LZ=50%, LK=70%, LP=60%, C=0,02, M=0,01)
6.2 PKI_Autoryzacja (LZ=30%, LK=60%, LP=60%, M=0,05)

### 3.3.3. Mechanizmy bezpieczeństwa

Wybrane wierzchołki grafów, które reprezentują zastosowane mechanizmy bezpieczeństwa, posłużą następnie do obliczenia prawdopodobieństw wystąpienia zagrożeń. Pod pojęciem prawdopodobieństwa rozumiane jest indywidualne prawdopodobieństwo obliczone dla poszczególnych wierzchołków. W tym rozdziale przedstawiono algorytm, dzięki któremu możemy obliczyć wspomniane prawdopodobieństwa zagrożeń. Gdy prawdopodobieństwa wystąpienia zagrożenia dla wszystkich wybranych wierzchołków są obliczone, to wówczas na ich podstawie wyznaczane jest całkowite prawdopodobieństwo zajścia incydentu.

Główną miarą, która określa (dla poszczególnych zagrożeń) czy odpowiednie zasoby *LZ* zostaną zdobyte, są parametry: *LK***,** jako wymagany poziom wiedzy atakującego oraz *LP*, jako wymagane koszty poniesione przez atakującego (rozdział 3.3.1). Współczynniki te są modyfikowane przez odpowiednie wagi $\omega_{LK}$ i $\omega_{LP}$ ($\omega_{LK} + \omega_{LP} \leq 1$), które określają potencjalne przygotowanie atakującego pod względem poziomu wiedzy ($\omega_{LK}$) oraz skłonność do poniesienia kosztów ($\omega_{LP}$).

Dodatkową miarą, która pozwala uwzględnić zwiększoną wrażliwość na dane zagrożenie całego procesu są: parametr *C* jako dodatkowy krok komunikacji zastosowany w danym składniku (stwarza on możliwość dodatkowego ataku) oraz parametr *M*, który opisuję złożoność praktycznej implementacji mechanizmów bezpieczeństwa. Wraz ze zwiększeniem zastosowanych środków bezpieczeństwa zwiększamy możliwość popełnienia błędów w implementacji, czego przykładowym wynikiem są raporty o błędach, które atakującemu dostarczają dodatkowych informacji. Jeżeli wspomniane parametry nie są zaznaczone na danej gałęzi grafu oznacza to, że przyjmują one standardową (neutralną) wartość i nie wnoszą nic do obliczanej wartości prawdopodobieństwa zajścia incydentu.

Wykorzystując wszystkie wspomniane wyżej parametry uzyskujemy

wyrażenie dla prawdopodobieństwa zajścia pojedynczego zagrożenia. Przedstawione niżej wzory mają charakter empiryczny. Ich postać odzwierciedla aktualny stan wiedzy dotyczącej incydentów (uwzględniającą między innymi raporty CERT) oraz intuicję autora, popartą doświadczeniem z pracy na stanowisku administratora sieci. Poniżej przedstawiono wzór, na podstawie którego obliczane jest prawdopodobieństwo zajścia pojedynczego zagrożenia:

$$P_{ij,z}^{x} = (1-(LK_{ij,z}^{x}(1-\omega_{LK})+LP_{ij,z}(1-\omega_{LP}))) \cdot (LZ_{ij,z}^{x} + (1-LZ_{ij,z}^{x})(C_{ij,z}^{x} + M_{ij,z}^{x})) \tag{3.2}$$

We wzorze (3.2) przyjęto, że *x* jest numerem usługi bezpieczeństwa, które przyjmuje wartości *x*=(1,…,*c*), *c* jest liczbą wymaganych w danym przypadku usług bezpieczeństwa; *i* jest numerem konkretnego podprotokołu, który przyjmuje wartości *i*=(1,…,*a*), *a* jest liczbą podprotokołów w rozpatrywanym protokole kryptograficznym; *j* jest numerem kroku konkretnego podprotokołu, który przyjmuje wartości *j*=(1,….,*b*), *b* jest liczbą kroków w danym podprotokole; *z* jest numerem wierzchołku grafu, który przyjmuje wartości *z*= (1,…,*g*), gdzie *g* jest liczbą wierzchołków wybranych z grafu bezpieczeństwa dla danej usługi bezpieczeństwa *x*; $P_{ij,z}^{x}$ jest prawdopodobieństwem wystąpienia zagrożenia dla wierzchołka *z* w podprotokole *i* , kroku *j*, dla usługi bezpieczeństwa *x*; $\omega_{LK}$ jest wagą określającą potencjalne przygotowanie atakującego pod względem posiadanej wiedzy (stała dla wszystkich elementów rozpatrywanego protokołu); $\omega_{LP}$ jest wagą określająca potencjalne przygotowanie atakującego pod względem ewentualnych poniesionych kosztów (stała dla wszystkich elementów rozpatrywanego protokołu); $\omega_{LP} + \omega_{LK} \leq 1$.

W procesie wyznaczania prawdopodobieństwa ataku możemy użyć parametrów, które w sposób szczególny mogą scharakteryzować bieżący proces. Własności te w modelu opisywane za pomocą dodatkowych parametrów bezpieczeństwa (rozdział 3.3.1). Te dodatkowe parametry wprowadzają poprawkę do obliczonego wcześniej prawdopodobieństwa wystąpienie zagrożenia ( $P_{ij,z}^{x}$ ). Poniżej przedstawiono formułę wprowadzającą wspomnianą poprawkę:

$$P_{ij,z,A}^{x} = P_{ij,z}^{x} + [(PP + I + H) \cdot (1 - P_{ij,z}^{x})]. \tag{3.3}$$

We wzorze (3.3) znaczenie symboli *x*, *c*, *i*, *a*, *j*, *b*, *g*, jest takie, jak to przyjęto we wzorze (3.2), $P_{ij,z}^{x}$ jest prawdopodobieństwem wystąpienia zagrożenia dla wierzchołka *z* w podprotokole *i*, kroku *j* dla usługi bezpieczeństwa *x*, natomiast $P_{ij,z,A}^{x}$ jest prawdopodobieństwem wystąpienia zagrożenia dla wierzchołka *z*

w podprotokole *i*, kroku *j* dla usługi bezpieczeństwa *x*, uwzględniającym dodatkowe parametry *PP, I, H* (rozdział 3.3.1).

W celu pełnego opisu stanu zagrożeń protokołu kryptograficznego realizującego daną usługę bezpieczeństwa obliczamy wszystkie cząstkowe prawdopodobieństwa dla każdej wybranej gałęzi grafu. W ten sposób obliczamy prawdopodobieństwa zajścia pojedynczych zagrożeń.

Kolejną czynnością prowadząca do pełnego modelu jest wyznaczenie prawdopodobieństwa wystąpienia incydentu w danym kroku jako zestawienie pojedynczych zagrożeń. W tym celu wyszukamy wśród obliczonych cząstkowych prawdopodobieństw najwyższe prawdopodobieństwo. Ta wartość będzie głównym wkładem do prawdopodobieństwa wystąpienia incydentu w danym kroku. Jest to spowodowane faktem, że zabezpieczenia systemu informatycznego są tak silne, jak jego najsłabszy element. Poniżej przedstawiono wzór, na podstawie którego jest obliczany główny wkład do prawdopodobieństwa zajścia incydentu:

$$P_{ij,M}^{x} = \max\left( P_{ij,z,A}^{x} \right). \tag{3.4}$$

Oznaczenia we wzorze (3.4) są takie same, jak we wzorach (3.2) i (3.3), $P_{ij,z}^{x}$ jest prawdopodobieństwem wystąpienia zagrożenia dla wierzchołka *z* w podprotokole *i* , kroku *j*, dla usługi bezpieczeństwa *x*; $P_{ij,z,A}^{x}$ jest prawdopodobieństwem wystąpienia zagrożenia dla wierzchołka *z* w podprotokole *i* , kroku *j* dla usługi bezpieczeństwa *x* , uwzględniającym dodatkowe parametry *PP, I, H* (rozdział 3.3.1); $P_{ij,M}^{x}$ jest prawdopodobieństwem wystąpienia incydentu w podprotokole „*i*", kroku „*j*" dla usługi bezpieczeństwa „*x*".

Prawdopodobieństwo wystąpienia incydentu w danym kroku jest uzależnione nie tylko od zagrożenia, które przyjmuje najwyższą wartość, ale również od wszystkich innych zagrożeń możliwych w danym kroku. W celu uwzględnienia tego faktu, na podstawie pozostałych, mniejszych od maksymalnego cząstkowego prawdopodobieństwa zajścia zagrożenia (prawdopodobieństwa zajścia incydentu) obliczamy stosowną poprawkę. Uzyskujemy to tworząc szereg cząstkowych prawdopodobieństw. Liczba elementów szeregu jest zmienna i możemy ją ustalić przyjmując odpowiednią wartość parametru *N*. Pierwszy element szeregu, $a_1$ , ma postać:

$$a_1 = (1- P_{ij,M}^{x} ) P_{ij,z}^{x} , \tag{3.5}$$

gdzie *z* jest wierzchołkiem grafu.

*N*-ty element szeregu wyznaczany jest według wzoru:

`

$$a_N = [(1- \ P^x_{ij,M}) - \sum_{n=2}^{n=N} a_{n-1}] \ \ P^x_{ij,z} \ , \tag{3.6}$$

gdzie $a_n$ jest *n*-tym elementem szeregu oraz *n* jest z przedziału *n*=(2,…,*N*); *N* jest liczbą uwzględnianych poprawek do maksymalnego prawdopodobieństwa przyjmującą wartości z przedziału *N*=(2,..,*k*); *k* jest liczbą wybranych w danym kroku wierzchołków grafu; *z* jest konkretnym wierzchołkiem grafu.

Całkowita poprawka do prawdopodobieństwa zajścia incydentu będzie zatem równa:

$$P^x_{ij,C} = \sum_{l=1}^{l=n} a_l \qquad , \tag{3.7}$$

gdzie *l* jest liczbą elementów zsumowanych do poprawki; *n* jest liczbą elementów w szeregu; $P^x_{ij,C}$ jest całkowitą poprawką do prawdopodobieństwa zajścia incydentu.

Po obliczeniu wspomnianych czynników możemy wyznaczyć całkowite prawdopodobieństwo zajścia incydentu dla danej usługi w ustalonym kroku:

$$P^x_{ij,ALL} = \ P^x_{ij,M} + \ P^x_{ij,C} \, . \tag{3.8}$$

We wzorze (3.8) znaczenie symboli *x*, *c*, *i*, *a*, *j*, *b*, *g* jest takie, jak to przyjęto we wzorze (3.2) i dalszych wzorach; $P^x_{ij,z}$ jest prawdopodobieństwem wystąpienia zagrożenia dla wierzchołka *z* w podprotokole *i*, kroku *j* dla usługi bezpieczeństwa *x*; $P^x_{ij,ALL}$ jest całkowitym prawdopodobieństwem zajścia incydentu w podprotokole *i* w kroku *j* dla usługi bezpieczeństwa *x;* $P^x_{ij,M}$ jest prawdopodobieństwem wystąpienia incydentu w podprotokole *i*, kroku *j* dla usługi bezpieczeństwa *x*; $P^x_{ij,C}$ jest całkowitą poprawką do prawdopodobieństwa zajścia incydentu w podprotokole *i*, w kroku *j* dla usługi bezpieczeństwa *x*.

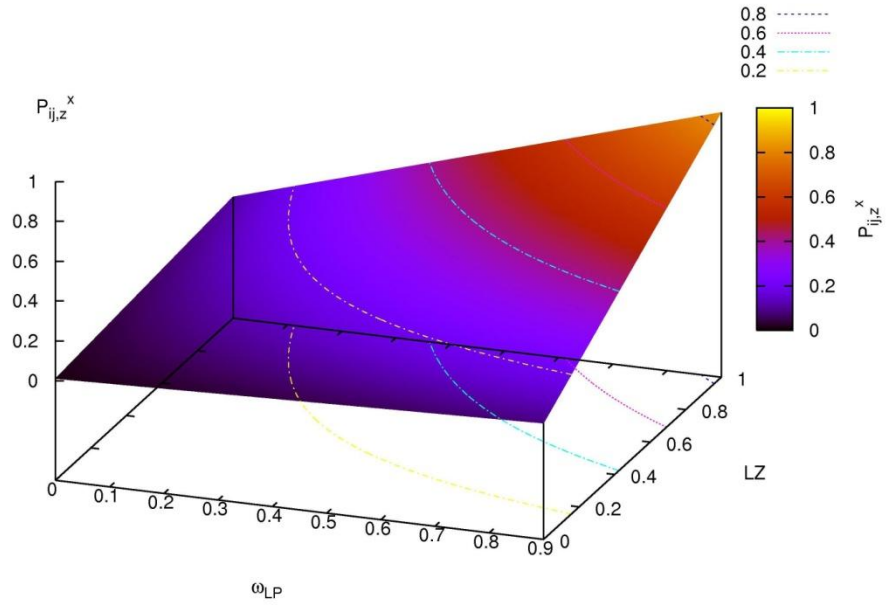
### 3.3.4. Charakterystyka modelu prawdopodobieństwa zajścia incydentu

W rozdziale 3.3.3 przedstawiono model pozwalający obliczyć prawdopodobieństwo zajścia incydentu. W bieżącym rozdziale przedstawiono charakterystykę wspomnianego modelu. W tym celu zostało rozważonych szereg różnych przykładów procesów elektronicznych, które zostały określone

za pomocą parametrów opisanego wyżej modelu. Dla rozważanych przypadków są przedstawione wykresy charakteryzujące model, a następnie przeprowadzana jest jego analiza. W celu zilustrowania modelu, w omawianych poniżej przypadkach rozpatrywane są indywidualne prawdopodobieństwa zajścia zagrożenia ( $P_{ij,z}^{x}$ ) (rozdział 3.3.3). Takie podejście jest wystarczające, ponieważ w modelu wśród indywidualnych obliczonych prawdopodobieństw zajścia zagrożenia ( $P_{ij,z}^{x}$ ) wyszukiwane jest takie zagrożenie, którego wartość prawdopodobieństwa jest najwyższa ( $P_{ij,M}^{x}$ ) i właśnie ta wartość jest podstawowym wkładem do całkowitego prawdopodobieństwa zajścia incydentu ( $P_{ij,ALL}^{x}$ ).

W pierwszym rozważanym przypadku założono, że zasoby biorące udział w procesie elektronicznym mogą być zaatakowane, gdy strona atakująca będzie posiadała małą wiedzę ($LK$=0,1). Biorąc pod uwagę ten warunek, dokładnie na takim poziomie została ustalona wiedza atakującego $\omega_{LK}$ =0,1. Żeby dokonać ataku należy posiadać również stosowne środki finansowe. W rozważanym przypadku ustalono potrzebny poziom na wysokości $LP$=0,8. Zgodnie z założeniem modelu takim, że $\omega_{LP} + \omega_{LK} \leq 1$, $\omega_{LP}$ może przyjmować wartość maksymalną 0,9. Kroki komunikacyjne ($C$) są realizowane w stopniu średnim oraz praktyczną implementację procesu elektronicznego ($M$) jest średnio skomplikowana, czyli parametry przyjmują wartość $C$=0,05 oraz $M$=0,05. Cząstkowe prawdopodobieństwa poszczególnych zagrożeń obliczane są według wzoru (3.2).

Na rys. 3.8 przedstawiono wartości, jakie przyjmuje prawdopodobieństwo indywidualnych zagrożeń ( $P_{ij,z}^{x}$ **)** w rozważanym przypadku w zależności od możliwych do zdobycia zasobów ($LZ$) oraz przygotowania atakującego pod kątem wiedzy ( $\omega_{LP}$ ). Dla podsumowania, wspomniane parametry przyjmują wartości: $LK$=0,1, $\omega_{LK}$ =0,1, $LP$=0,8, $C$=0,05, $M$=0,05.




Rys. 3.8 Prawdopodobieństwo indywidualnych zagrożeń ( $P_{ij,z}^{x}$ ) w zależności od możliwych do zdobycia zasobów (*LZ*) oraz przygotowania atakującego pod kątem wiedzy ( $\omega_{LP}$ ).

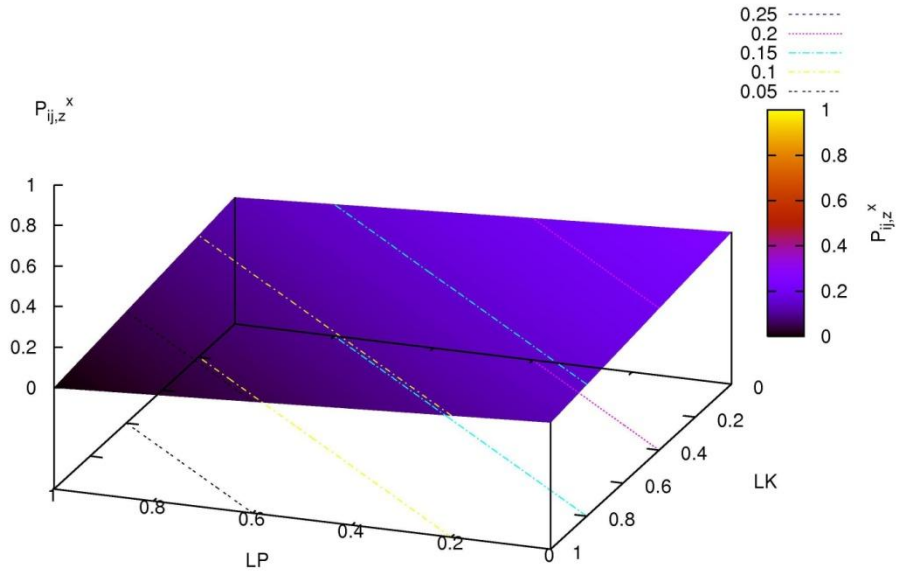
W przedstawionym przypadku widać, że nawet przy założeniu, że atakujący jest maksymalnie przygotowany finansowo ( $\omega_{LP} = 0{,}9$ ) zasoby, które posiadają niską wartość ( np. *LZ*=0,2) będą atakowane z małym prawdopodobieństwem ( $P_{ij,z}^{x} < 0{,}2$). Wraz ze wzrostem wartości zasobów możliwych do zdobycia, prawdopodobieństwo ataku rośnie aż do wartości $P_{ij,z}^{x} \approx 0{,}8$, czyli osiągając wysoką wartość.

Jeżeli atakujący jest przygotowany finansowo jedynie w 50% koniecznych do ataku środków, czyli $\omega_{LP} = 0{,}45$ to chcąc zaatakować zasoby, które posiadają najwyższe wartości ($LZ \approx 1$) prawdopodobieństwo zajścia zagrożenia jest na średnim poziomie ( $P_{ij,z}^{x} < 0{,}4$).

Podsumowując rozważany przypadek można stwierdzić, że wraz ze wzrostem przygotowania atakującego pod względem finansowym aż do poziomu wymaganego, rośnie prawdopodobieństwo zajścia zagrożenia. Poziom osiąganego prawdopodobieństwa jest uzależniony również od możliwych zasobów do zdobycia. Im ich wartość jest wyższa, tym prawdopodobieństw zajścia zagrożenia jest większe.

Jeżeli w rozważanym przypadku, zamienimy parametr poziomu wiedzy (*LK*) z parametrem poziomu kosztów (*LP*) oraz parametr posiadanej wiedzy przez atakującego ($\omega_{LK}$) z posiadanymi możliwościami finansowymi ($\omega_{LP}$), wówczas otrzymamy identyczne wyniki. Jest to spowodowane faktem, że wspomniane parametry są symetryczne.

W drugim rozważanym przypadku założono, że zasoby biorące udział w procesie elektronicznym mają wartość niską, czyli *LZ*=0,25. Poziom wiedzy atakującego ($\omega_{LK}$) został równomiernie rozłożony z poziomem możliwości finansowych ($\omega_{LP}$) i przyjmują wartości $\omega_{LK} = \omega_{LP} = 0{,}5$. Kroki komunikacyjne (*C*) są realizowane w stopniu średnim a praktyczna implementację procesu elektronicznego (*M*) jest średnio skomplikowana, czyli parametry przyjmują wartość *C*=0,05 oraz *M*=0,05. Cząstkowe prawdopodobieństwa poszczególnych zagrożeń obliczane są według formuły (3.2). Na rys. 3.9 przedstawiono wartości, jakie przyjmuje prawdopodobieństwo indywidualnych zagrożeń ( $P_{ij,z}^{x}$ ) w zależności od wymaganego poziomu wiedzy (*LK*) oraz wymaganych kosztów (*LP*) dla poziomu możliwych do zdobycia zasobów *LZ*=0,25. Dla podsumowania wspomniane parametry przyjmują wartości: *LZ*=0,25, $\omega_{LK} = \omega_{LP} = 0{,}5$, *C*=0,05, *M*=0,05.



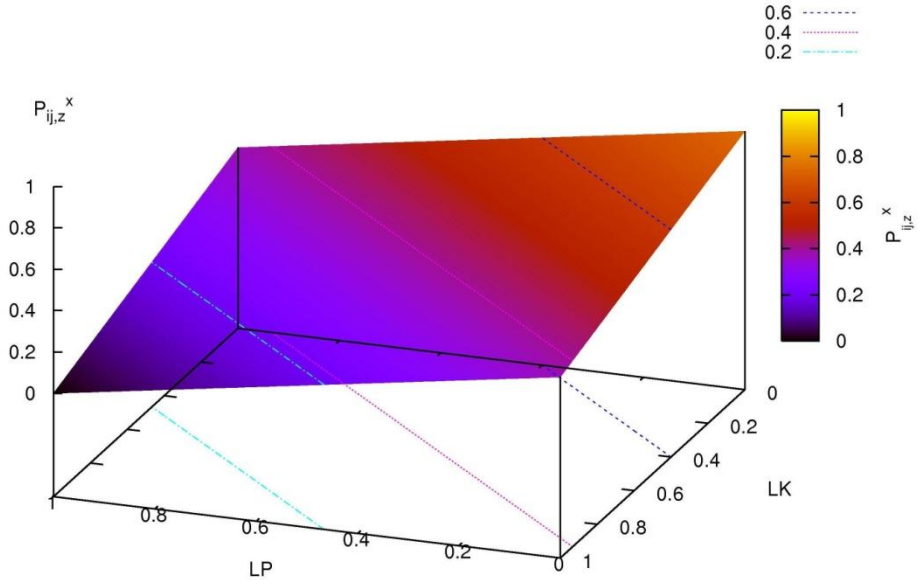

Rys. 3.9 Prawdopodobieństwo indywidualnych zagrożeń ( $P_{ij,z}^{x}$ ) w zależności od wymaganego poziomu wiedzy (*LK*) oraz wymaganych kosztów (*LP*) dla poziomu możliwych do zdobycia zasobów *LZ*=0,25.

Rys. 3.9 obrazuje drugi omawiany przypadek. W tym przypadku elementem wpływającym na osiągane wartości prawdopodobieństwa są zasoby możliwe do zdobycia. Są one na niskim poziomie (*LZ*=0,25). Przy takim poziomie możliwych do osiągnięcia zysków przez atakującego, nawet wówczas, gdy do przeprowadzania ataku potrzebna jest niewielka wiedza ($LK \approx 0{,}2$) oraz niskie koszty ($LP \approx 0{,}2$), prawdopodobieństwo ataku jest bardzo niskie ( $P_{ij,z}^{x} \approx 0{,}2$).

Warto zwrócić uwagę, że gdy do przeprowadzenia ataku jest konieczny najwyższy poziom wiedzy ($LK \approx 1$) oraz najwyższe koszty ($LP \approx 1$), wówczas prawdopodobieństwo zajścia indywidualnego zagrożenia jest bliskie 0 ( $P_{ij,z}^{x} \approx 0$). Z przedstawionej analizy można wywnioskować, że warto stosować mechanizmy bezpieczeństwa, których złamanie dostarcza atakującemu małe zasoby, a do ich złamania potrzeba jest dużych kosztów i dużej wiedzy. Stosując takie mechanizmy zwiększamy zabezpieczenia systemu, minimalizując jednocześnie ryzyko ataku.

W trzecim przypadku warto rozważyć sytuację, w której możliwe do zdobycia zasoby zostaną zwiększone trzykrotnie względem wcześniej rozważanego przypadku, czyli do wartości *LZ*=0,75. Pozostałe parametry pozostaną bez zmian, czyli będą przyjmowały wartości: $\omega_{LK} = \omega_{LP} = 0{,}5$, *C*=0,05, *M*=0,05. Na rys. 3.10 przedstawiono wartości, jakie przyjmuje prawdopodobieństwo indywidualnych zagrożeń ( $P_{ij,z}^{x}$ **)** w zależności od wymaganego poziomu wiedzy (*LK*) oraz wymaganych kosztów (*LP*) dla poziomu możliwych do zdobycia zasobów *LZ*=0,75.

Przy trzykrotnie większym poziomie możliwych do osiągnięcia zysków przez atakującego (*LZ*=0,75), gdy do przeprowadzania ataku potrzebna jest niewielka wiedza ($LK \approx 0{,}2$) oraz niskie koszty ($LP \approx 0{,}2$), prawdopodobieństwo zajścia zagrożenia wzrasta trzykrotnie i przyjmuje wartość $P_{ij,z}^{x} \approx 0{,}6$.



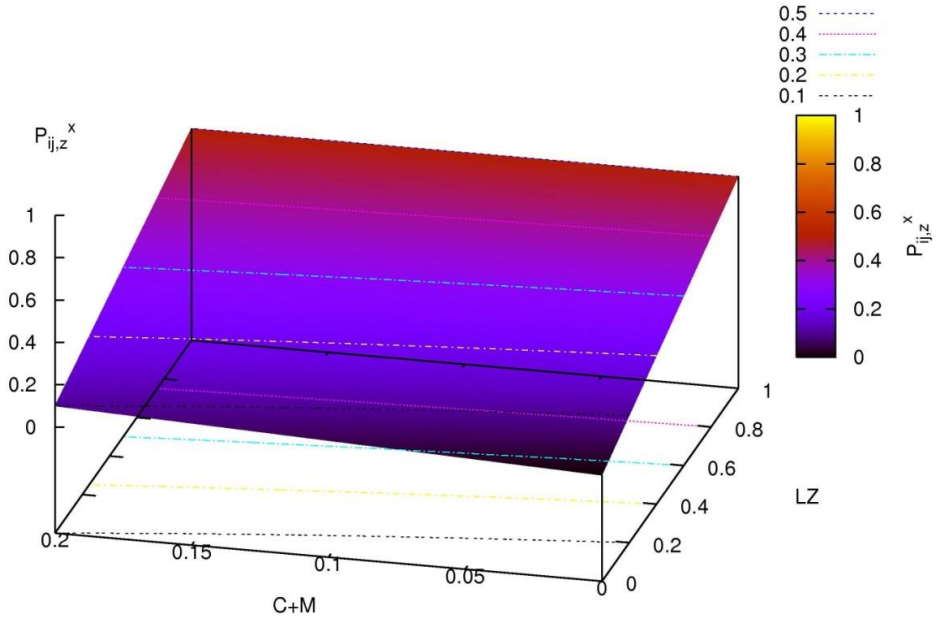

Rys. 3.10 Prawdopodobieństwo indywidualnych zagrożeń ( $P_{ij,z}^{x}$ ) w zależności od wymaganego poziomu wiedzy (*LK*) oraz wymaganych kosztów (*LP*) dla poziomu możliwych do zdobycia zasobów *LZ*=0,75.

Analizując dalej ten przypadek można zauważyć, że gdy do przeprowadzenia ataku jest konieczny najwyższy poziom wiedzy ($LK \approx 1$) oraz najwyższe koszty ($LP \approx 1$), wówczas prawdopodobieństwo zajścia indywidualnego zagrożenia nadal jest bliskie 0 ( $P_{ij,z}^{x} \approx 0$). Różnica w stosunku do przypadku, w którym poziom możliwych do zdobycia zasobów jest trzykrotnie niższy (rys. 3.9), jest taka, że wzrost prawdopodobieństwa zajścia zagrożenia jest trzykrotnie większy (rys. 3.10). Analizując omawiany przypadek, można stwierdzić, że czym większe możliwe do zdobycia zasoby podczas złamania konkretnego mechanizmu bezpieczeństwa, tym większe prawdopodobieństwo, że atak na taki element bezpieczeństwa zostanie przeprowadzony.

W kolejnym, czwartym rozważanym przypadku przeanalizowano, jaki wpływa na prawdopodobieństwo zajścia zagrożenia mają parametry określane jako kroki komunikacyjne (*C*) i praktyczna implementacja (*M*) (rozdział 3.3.1). W tym celu ustalono poziom wymaganej wiedzy na *LK*=0,5 oraz poziom koniecznych kosztów również na *LP*=0,5. Następnie określono poziomy przygotowania atakującego pod kątem wiedzy i kosztów i ustalono je zgodnie z wymaganiami, czyli $\omega_{LK} = \omega_{LP} = 0{,}5$. Cząstkowe prawdopodobieństwa poszczególnych zagrożeń obliczane są według formuły (3.2). Na rys. 3.12 przedstawiono wartości, jakie przyjmuje prawdopodobieństwo indywidualnych zagrożeń ( $P_{ij,z}^{x}$ ) w zależności od możliwych do zdobycia zasobów (*LZ*) i sumy

parametrów charakteryzujących kroki komunikacyjne (*C*) oraz praktyczną implementacje (*M*), czyli (*C*+*M*). Zgodnie ze zdefiniowanymi przedziałami, suma wspomnianych parametrów (*C*+*M*) może osiągnąć maksymalną wartość równą 0,2 (rozdział 3.3.1). Dla podsumowanie ustalone parametry przyjmują wartości: *LP*=*LK*=0,5, $\omega_{LK} = \omega_{LP} = 0{,}5$.

Analizując otrzymany wyniki (rys. 3.11) warto zwrócić uwagę, że wpływ parametrów określających kroki komunikacyjne i praktyczną implementację (*C*+*M*) wnosi poprawkę do otrzymanego prawdopodobieństwa zajścia zagrożenia, gdy w wyniku zagrożeń mogą być zdobyte zasoby o niższych wartościach. Przykładowo, gdy możliwe do zdobycia zasoby będą przyjmowały wartości *LZ*=0,4 oraz suma parametrów *C*+*M*=0, wówczas prawdopodobieństwo zajścia zagrożenia osiągnie wartość $P^{x}_{ij,z} = 0{,}2$. Natomiast, jeżeli suma parametrów C+M=0,2, wówczas prawdopodobieństwo zajścia zagrożenia osiągnie wartość $P^{x}_{ij,z} \approx 0{,}25$, czyli wzrośnie o 30% względem wcześniejszego przypadku. Warto jednak nadmienić, że stanowi to 5% wzrostu względem maksymalnego prawdopodobieństwa zajścia zagrożenia. Można zauważyć, że wraz ze wzrostem możliwy do zdobycia zasobów (*LZ*), osiągnięta poprawka przez sumę wspomnianych parametrów (*C*+*M*) się zmniejsza. W przypadku, gdy *LZ*=1, ich wpływ jest minimalny.



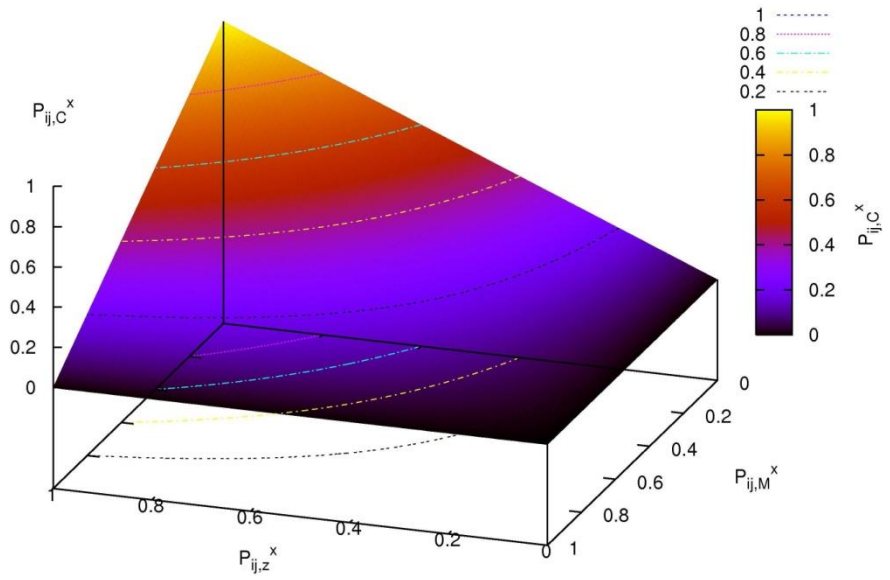

Rys. 3.11 Prawdopodobieństwo indywidualnych zagrożeń ( $P^{x}_{ij,z}$ ) w zależności od możliwych do zdobycia zasobów (*LZ*) i sumy parametrów charakteryzujących kroki komunikacyjne (*C*) oraz praktyczną implementacje (*M*), czyli (*C*+*M*).

Kolejnym elementem, na który warto zwrócić uwagę na rys. 3.11, jest wartość osiągniętego prawdopodobieństwa, gdy poziom możliwych do zdobycia zasobów jest równy *LZ*=0. Jeżeli suma parametrów *C*+*M*=0, wówczas $P_{ij,z}^{x} = 0$, natomiast, gdy suma parametrów *C*+*M*=0,2, wtedy $P_{ij,z}^{x} = 0{,}1$. Interpretacja takiego zachowania modelu jest taka, że pomimo faktu, że złamanie danego element bezpieczeństwa nie prowadzi za sobą zdobycia żadnych zasobów systemu, atakujący chcąc zdobyć pośrednie informacje zaatakuje dany element. Będzie to możliwe za sprawą błędnej implementacji (*C*) oraz dodatkowych kroków komunikacyjnych (*M*).

W piątym rozpatrywanym przypadku rozważono, jaką wartość może osiągać poprawka do prawdopodobieństwa zajścia zagrożenia ($P_{ij,C}^{x}$) w zależności od maksymalnej wartości prawdopodobieństwa zajścia zagrożenia ($P_{ij,M}^{x}$) oraz wartości prawdopodobieństwa zajścia kolejnego branego pod uwagę zagrożenia ($P_{ij,z}^{x}$). Wspomniana poprawka jest omówiona w rozdziale 3.3.3.

Analizując rys. 3.12 można zauważyć, że poprawka do prawdopodobieństwa zajścia zagrożenia ($P_{ij,C}^{x}$) jest tym większa im mniejsze jest maksymalne prawdopodobieństwo zajścia zagrożenia ($P_{ij,M}^{x}$). Wzrost poprawki prawdopodobieństwa ($P_{ij,C}^{x}$) jest proporcjonalny do wzrostu prawdopodobieństw kolejnych zagrożeń ($P_{ij,z}^{x}$). Poprawka do prawdopodobieństwa zagrożenia ma charakter rosnący, ponieważ każdorazowe zastosowanie nowego elementu bezpieczeństwa wprowadza możliwość ataku na ten składnik. Warto zwrócić uwagę na fakt, że wprowadzenie nowego elementu bezpieczeństwa oprócz zwiększania prawdopodobieństwa zajścia zagrożenia, wpływa na zabezpieczenie zasobów. Dlatego prawdopodobieństwo wystąpienia zagrożenia może wzrastać, ale istotne jest żeby użyte zabezpieczenia były na tyle wysokie, żeby nie pozwoliły na udany atak.

`

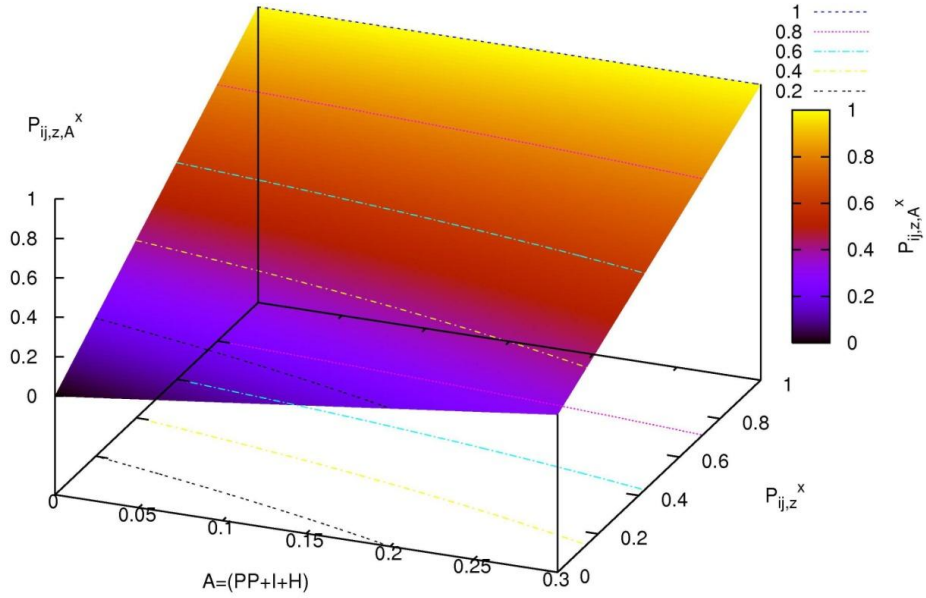



Rys. 3.12 Poprawka do prawdopodobieństwa zajścia zagrożenia ( $P_{ij,C}^{x}$ ) w zależności od maksymalnej wartości prawdopodobieństwa zajścia zagrożenia ( $P_{ij,M}^{x}$ ) oraz wartości prawdopodobieństwa zajścia kolejnego branego pod uwagę zagrożenia ( $P_{ij,z}^{x}$ ).

Ostatni, szósty rozważany przypadek (rys. 3.13) przedstawia charakterystykę poprawki, jaką wnoszą do prawdopodobieństwa zajścia zagrożenia ( $P_{ij,z,A}^{x}$ ) dodatkowe parametry przewidziane w modelu ($A=PP+I+H$) (rozdział 3.3.1), w zależności od podstawowej wartości prawdopodobieństwa zajścia zagrożenia ( $P_{ij,z}^{x}$ ). W skład nich wchodzą parametry opisujące globalne możliwe zasoby do zdobycia w danym procesie (*PP*), rodzaj instytucji (*I*) oraz hipotetyczne ryzyko poniesione przez atakującego (*H*). Maksymalna wartość, jaką może przyjąć każdy parametr jest równa 0,1. Wpływ tych parametrów na prawdopodobieństwa zajścia zagrożenia jest obliczany według wzoru (3.3).

Dodatkowe parametry wpływające na prawdopodobieństwo zajścia incydentu ($A=PP+I+H$) (rozdział 3.3.1) charakteryzują sam proces elektroniczny i odzwierciedlają ryzyko rezydentne (stałe) [32], które jest przypisane indywidualnie do każdego procesu elektronicznego. Wielkość wpływu tych parametrów jest uzależniona od indywidualnego prawdopodobieństwa zajścia zagrożenia ( $P_{ij,z}^{x}$ ). W początkowej wersji, gdy parametr $P_{ij,z}^{x}=0$, wówczas parametry $A=PP+I+H$ przyjmują swoją maksymalną wartość, czyli 0,3. Wraz

ze wzrostem parametru $P^{x}_{ij,z}$, poprawka wniesiona przez dodatkowe parametry ( $P^{x}_{ij,z,A}$) jest mniejsza, a jeżeli $P^{x}_{ij,z} = 1$, to wówczas $P^{x}_{ij,z,A} = 0$.




Rys. 3.13 Charakterystyka poprawki, jaką wnoszą do prawdopodobieństwa zajścia zagrożenia ( $P^{x}_{ij,z,A}$) dodatkowe parametry przewidziane w modelu ($A$=$PP$+$I$+$H$) w zależności od podstawowej wartości prawdopodobieństwa zajścia zagrożenia ( $P^{x}_{ij,z}$).

## 3.4. Wpływ udanego ataku na system

Trzecim elementem opisującym poziom bezpieczeństwa procesu elektronicznego (rozdział 3.1) jest wpływ udanego ataku na system ( $\omega$ ) [52]. Element ten określa średnie poniesione straty w zasobach spowodowane przez określone zagrożenia. W opisywanym modelu skalowanego bezpieczeństwa, wpływ udanego ataku na system ( $\omega$ ) charakteryzowany jest przez dwie grupy parametrów. Pierwsza związana jest z bezpośrednim wpływem ataku na zasoby, druga z wpływem pośrednim [31, 32]. Wpływ udanego ataku na system obliczany jest indywidualnie dla wszystkich kroków zawartych w konkretnym

podprotokole kryptograficznym realizującym daną usługę bezpieczeństwa. Taka czynność jest wykonywana dla wszystkich podprotokołów kryptograficznych, które realizują wybrane w konkretnym przypadku usługi bezpieczeństwa. Parametry przedstawione są w postaci procentowej.

***1. Bezpośrednie parametry:***

- $LZ$ - maksymalne zasoby zdobyte podczas udanego ataku (100% - skompromitowanie całego protokołu);
- $F$ - finansowe straty podczas udanego ataku (100% - całkowite możliwe straty finansowe).

***2. Pośrednie parametry:***

- $\alpha$ - straty finansowe konieczne do usunięcia awarii, które zostały spowodowane udanym atakiem (100% - maksymalne koszty);
- $\beta$ - straty poniesione w wyniku spadku reputacji firmy (100% - maksymalne straty).

W celu obliczenia wpływu ataku na system ($\omega$) używa się kombinacji parametrów przedstawionych wyżej. Parametr $LZ$ opisuje wpływ potencjalnej szkody spowodowanej przez określone zagrożenie na skompromitowanie całego protokołu (zdobycie wszystkich zasobów). Wartość tego parametru jest równa odpowiedniej wartości parametru $LZ$ zdefiniowanej w modelu obliczającym prawdopodobieństwo zajścia incydentu (rozdział 3.3.1). Mówiąc o odpowiedniej wartości, autor miał na myśli taką wartość na podstawie, której obliczone zostało najwyższe prawdopodobieństwo zajścia zagrożenia ($P_{ij,M}^{x}$) (rozdział 3.3.3). Parametr $F$ określa bezpośrednie straty finansowe spowodowane w wyniku konkretnego zagrożenia. Przykładowym mogą być ataki, w których bezpośrednim efektem są straty finansowe, np. zablokowanie wykonania przelewu bankowego w wyniku czego zostały naliczone odsetki bankowe.

Następne parametry związane są z czynnikami pośrednimi określającymi wpływ ataku na system. Pierwszy - $\alpha$ - jest związany z pośrednimi stratami finansowymi, które muszą być poniesione w wyniku udanego ataku. Wspomniane wydatki mogą być spowodowane usunięciem awarii i uszkodzeń zaatakowanego systemu informatycznego. Drugi parametr w tej grupie - $\beta$ określa straty reputacji firmy na rynku. Przykładowym atakiem tego rodzaju, może być atak na witrynę WWW firmy oferującej zabezpieczenia systemów informatycznych.

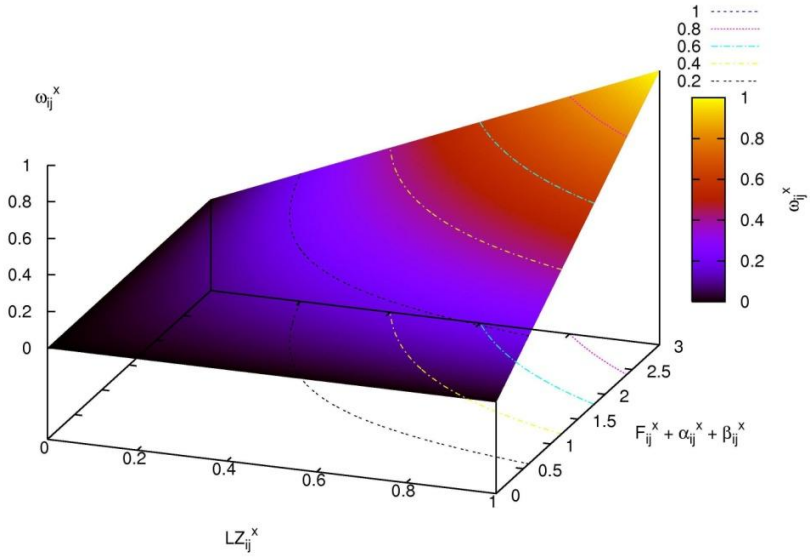
Poprzez kombinację wspomnianych wyżej parametrów wyznaczany jest

wpływ udanego ataku na system. Przedstawiona poniżej formuła ma charakter empiryczny, która została wyznaczona bazując na intuicji autora oraz wykonanych symulacjach:

$$\omega_{ij}^{x} = \frac{LZ_{ij}^{x}}{3}\left(F_{ij}^{x} + \beta_{ij}^{x} + \alpha_{ij}^{x}\right), \tag{3.9}$$

gdzie *x* jest usługą bezpieczeństwa, która przyjmuje wartości *x*=(1,…,*c*), gdzie *c* jest liczbą wymaganych w danym przypadku usług bezpieczeństwa; *i* jest konkretnym podprotokołem, który przyjmuje wartości *i*=(1,…,*a*), gdzie *a* jest liczbą podprotokołów w rozpatrywanym protokole kryptograficznym; *j* jest krokiem konkretnego podprotokołu, który przyjmuje wartości *j*=(1,….,*b*), gdzie *b* jest liczbą kroków w danym podprotokole; *z* jest wierzchołkiem grafu, który przyjmuje wartości *z*= (1,…,*g*), gdzie *g* jest liczbą wierzchołków wybranych z grafu bezpieczeństwa dla danej usługi bezpieczeństwa *x*.

Na rys. 3.14 przedstawiono charakterystykę wpływu udanego ataku na system ( $\omega_{ij}^{x}$ ) w zależności od możliwych do zdobycia zasobów ( $LZ_{ij}^{x}$ ) oraz parametrów ( $F_{ij}^{x} + \beta_{ij}^{x} + \alpha_{ij}^{x}$ ).Wyniki zostały otrzymane na podstawie formuły (3.9). Wszystkie parametry, które wchodzą w skład formuły (3.9), mają wartość maksymalną 1, dlatego suma parametrów $F_{ij}^{x} + \beta_{ij}^{x} + \alpha_{ij}^{x}$ może przyjmować maksymalnie wartość 3.




Rys 4.14 Charakterystyka wpływu udanego ataku na system ( $\omega_{ij}^{x}$ ) w zależności od możliwych do zdobycia zasobów ( $LZ_{ij}^{x}$ ) oraz parametrów ( $F_{ij}^{x} + \beta_{ij}^{x} + \alpha_{ij}^{x}$ ).

`

Analizując rozpatrywany przypadek można zauważyć, że gdy możliwe do zdobycia zasoby (*LZ*) przyjmują wartość 0, wówczas wpływ udanego ataku na system ($\omega_{ij}^{x}$) również jest równy 0. Taka prawidłowość wskazuje, że nie można mówić o wpływie udanego ataku na system, gdy nie istnieją zasoby możliwe do zdobycia. Na rys. 3.14 można zauważyć prawidłowość, że wraz ze wzrostem możliwych do zdobycia zasobów rośnie wpływ udanego ataku na system. Nawet, gdy możliwe do osiągnięcia zasoby mają bardzo wysoką wartość, czyli $LZ \approx 1$, to gdy suma parametrów $F_{ij}^{x} + \beta_{ij}^{x} + \alpha_{ij}^{x} \approx 1$, wpływ udanego ataku na system jest niski i osiąga wartość $\omega_{ij}^{x} \approx 0{,}3$. Taka sytuacja opisuje przypadek, gdy potencjalne możliwe do zdobycia zasoby w danym procesie elektronicznym są duże, ale ich wartość dla systemu jest niska. W takim przypadku wpływ udanego ataku będzie niski.

## 3.5. Poziom bezpieczeństwa

Procesy elektroniczne, w których zagadnienia ochrony informacji są szczególnie istotne, bazują na protokołach kryptograficznych. Protokoły kryptograficzne wypełniają założenia ochrony informacji, które są reprezentowane przez usługi bezpieczeństwa. Protokół kryptograficzny składa się z podprotokołów, które następnie podzielone są na indywidualne kroki. W przedkładanej książce zaprezentowano model skalowanego bezpieczeństwa, który w zależności od potencjalnego ryzyka dobierze odpowiedni poziom bezpieczeństwa (rozdział 3.1).

Opisana w rozdziale 3.1 koncepcja skalowanego bezpieczeństwa [49, 52], bazuje na wyznaczeniu różnych poziomów bezpieczeństwa dla poszczególnych wersji tego samego protokołu kryptograficznego. Wyznaczany poziom bezpieczeństwa jest funkcją trzech czynników (parametrów): poziomu zabezpieczeń ($L^{Z}$) (rozdział 3.2), prawdopodobieństwa zajścia incydentu (*P*) (rozdział 3.3) oraz wpływu udanego ataku na system ($\omega$) (rozdział 3.4). Jak opisano w rozdziale 2.3 za pomocą iloczynu prawdopodobieństwa zajścia incydentu (*P*) oraz wpływu udanego ataku na systemu ($\omega$) określane jest ryzyko ataku na system.

We wcześniejszych rozdziałach opracowano oraz scharakteryzowano modele opisujące wspomniane czynniki. W bieżącym rozdziale przedstawiono formułę na podstawie, której obliczany będzie poziom bezpieczeństwa dla danego procesu elektronicznego. Parametry wchodzące w skład modelu obliczane są dla wszystkich podprotokołów, z których składa się dany protokół kryptograficzny oraz wszystkich kroków tych podprotokołów. Efektem końcowym jest obliczenie poziomów bezpieczeństwa dla poszczególnych wersji protokołów konkretnego procesu elektronicznego. Ostatnim krokiem jest obliczenie poziomu bezpieczeństwa dla całego procesu elektronicznego. Wzór, na podstawie którego obliczany jest poziom bezpieczeństwa procesu

elektronicznego, ma charakter empiryczny. Został on wyznaczony na podstawie istniejącej wiedzy w tej dziedzinie nauki (rozdział 2.3) oraz intuicji autora wspomaganej przez wiele przeprowadzonych testów. Poniżej przedstawiono wspomnianą formułę:

$$F_S = \frac{1}{a}\sum_{i=1}^{a}\frac{1}{b_i}\sum_{j=1}^{b_i}\frac{1}{c_{ij}}\sum_{x=1}^{c_{ij}}(L_{ij}^{x})^{Z}[(1-\omega_{ij}^{x})(1-P_{ij,ALL}^{x})], \qquad (3.10)$$

gdzie $F_s$ jest obliczanym poziomem bezpieczeństwa, który jest realizowany przez daną wersje protokołu, $F_s \in (0,1)$; gdzie $x$ jest usługą bezpieczeństwa, która przyjmuje wartości $x=(1,\ldots,c)$, gdzie $c$ jest liczbą wymaganych w danym przypadku usług bezpieczeństwa; $i$ jest konkretnym podprotokołem, który przyjmuje wartości $i=(1,\ldots,a)$, gdzie $a$ jest liczbą podprotokołów w rozpatrywanym protokole kryptograficznym; $j$ jest krokiem konkretnego podprotokołu, który przyjmuje wartości $j=(1,\ldots,b)$ gdzie $b$ jest liczbą kroków w danym podprotokole; $\omega_{ij}^{x}$ – waga określająca średni koszt strat poniesiony w wyniku udanego ataku dla danej usługi, gdzie $\omega \in (0,1)$; $Z$ jest wrażliwością mechanizmów bezpieczeństwa, gdzie $Z \in (0,10)$; $(L_{ij}^{x})^{Z}$ jest osiągniętym poziomem zabezpieczeń w podprotokole $i$ , kroku $j$ dla usługi bezpieczeństwa $x$ oraz wrażliwości $Z$, gdzie $L \in (0,1)$; $P_{ij,ALL}^{x}$ jest całkowitym prawdopodobieństwem zajścia incydentu w podprotokole $i$ w kroku $j$ dla usługi bezpieczeństwa $x$, gdzie $P \in (0,1)$.

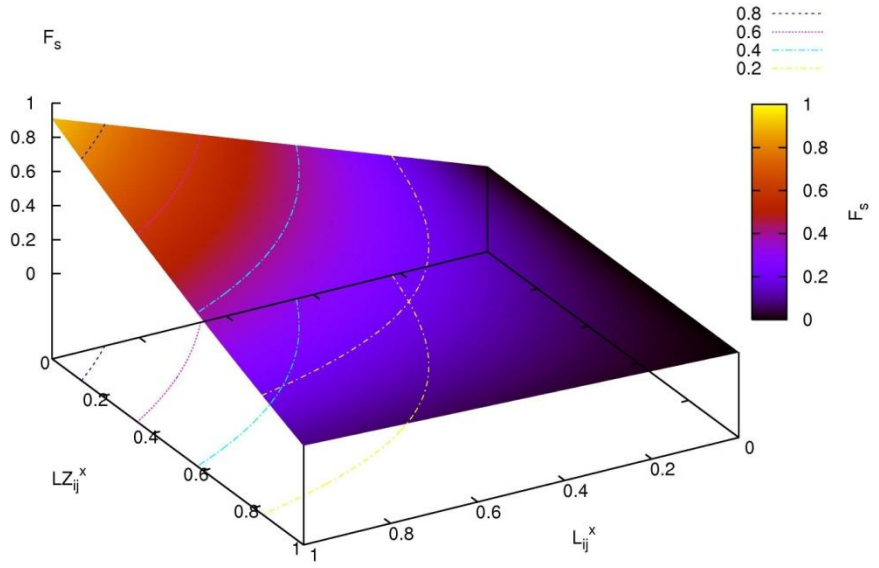
### 3.5.1. Charakterystyka modelu skalowanego bezpieczeństwa

W rozdziale 3.5 zaprezentowano wzór realizujący skalowane bezpieczeństwo. W skład formuły (3.10) wchodzą składniki, które są obliczane na podstawie przedstawionych we wcześniejszych rozdziałach algorytmów realizujących przedstawione modele. W bieżącym rozdziale zawarto charakterystykę modelu skalowanego bezpieczeństwa, który opisywany jest przez formułę (3.10). Charakterystyka modelu polega na rozważeniu wybranych przypadków procesu elektronicznego, którego wersje będą określane za pomocą elementów składowych modelu skalowanego bezpieczeństwa. Dla uproszczenia rozważań opisywany proces elektroniczny, będzie składał się z jednego podprotokołu, który składa się z jednego kroku.

W pierwszy rozważanym przypadku przedstawiono charakterystykę otrzymanego poziomu bezpieczeństwa ($F_S$) w zależności od zasobów użytych w danym procesie ($LZ$) oraz wybranych zabezpieczeń systemu ($L$) (rys. 3.15). Do zdobycia użytych zasobów ($LZ$) wystarczy posiadać niewielką wiedzę ($LK$=0,1) oraz niewielkie środki finansowe ($LP$=0,1). Przygotowanie atakującego, zarówno pod kątem finansowym, jaki i posiadanej wiedzy jest

`

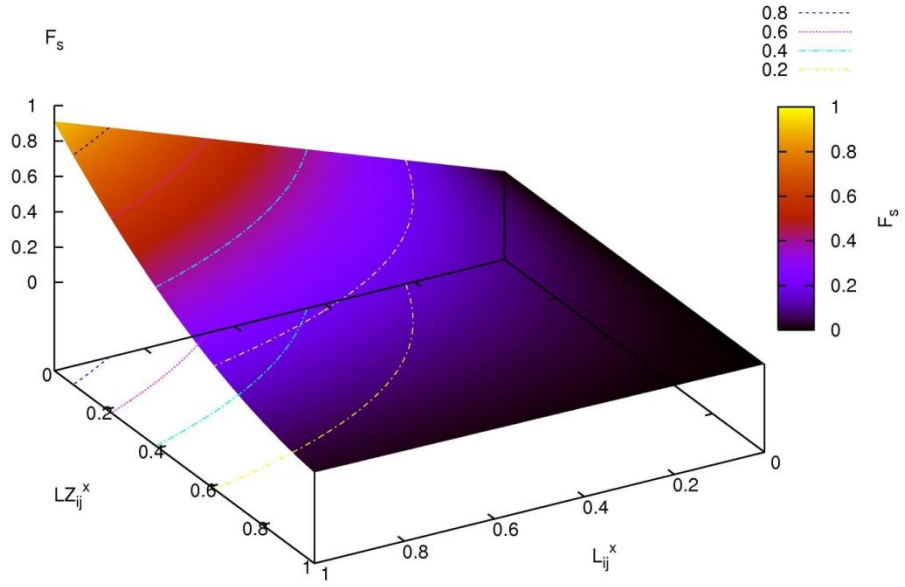
na średnim poziomie, ale wystarczającym do zdobycia zasobów $\omega_{LK} = \omega_{LP}$ =0,5. Zagrożenia związane z dodatkową komunikacją (*C*) oraz praktyczną implementacją (*M*) zostały ustalone na średnim poziomie *C*=*M*=0,05. Udany atak, powoduje szkody w systemie, w wyniku, czego dana organizacja ponosi straty. Przyjęto, że bezpośrednie jak i pośrednie straty finansowe wynikłe z ataku są małe i wynoszą $F_{ij}^{x} = \alpha_{ij}^{x} = 0{,}2$. Straty związane z utratą reputacji firmy określona na poziomie bardzo niskim, czyli $\beta_{ij}^{x} = 0{,}1$. Nie wprowadzono poprawki do zastosowanych mechanizmów bezpieczeństwa, zabezpieczających proces elektroniczny, czyli parametr określający ich wrażliwość będzie równy 1 (*Z*=1).




Rys. 3.15 Charakterystyka otrzymanego poziomu bezpieczeństwa ($F_S$) w zależności od użytych w danym procesie zasobów (*LZ*) oraz wybranych zabezpieczeń systemu (*L*) dla *LK*=*LP*=0,1,
$F_{ij}^{x} = \alpha_{ij}^{x} = 0{,}2$ , $\beta_{ij}^{x} = 0{,}1$.

Analizując rys. 3.15, można zauważyć, że w rozważanym przypadku, stosując mechanizmy bezpieczeństwa na wysokim poziomie ($L \approx 0{,}8$) osiągany poziom bezpieczeństwa ($F_S$) bardzo zależy od możliwych do zdobycia zasobów (*LZ*). Jeżeli to możliwe, gdy do zdobycia są bardzo wysokie ($LZ \approx 0{,}8$) wówczas osiągany poziom bezpieczeństwa jest na poziomie $F_S \approx 0{,}2$. Wraz, ze zmniejszeniem, możliwych do zdobycia zasobów poziom bezpieczeństwa rośnie, a w przypadku, gdy osiąga poziom $LZ \approx 0{,}4$, przyjmuje wartość $F_S \approx 0{,}5$. Warto również zwrócić uwagę, że w przypadku, gdy wybrane mechanizmy bezpieczeństwa są na niskim poziomie ($L \approx 0{,}2$), nawet przy możliwych

do zdobycia zasobów bliskim zeru ($LZ \approx 0$), osiągany poziom bezpieczeństwa jest niski i jest mniejszy od 0,1 ($F_S < 0{,}1$). W przedstawionym modelu istotnym elementem są różnice w uzyskanym poziomie bezpieczeństwa między wersjami tego samego protokołu. Na rys. 3.16 przedstawiono drugi przypadek, który różni się od pierwszego opisywanego przypadku (rys. 3.15) tylko wpływem udanego ataku na system. Ustalono, że wpływ znacznie wzrośnie i pośrednie oraz bezpośrednie straty finansowe będą przyjmowały wartości maksymalne, czyli $F_{ij}^{x} = \alpha_{ij}^{x} = 1$. Straty wynikłe ze zmniejszeniem reputacji firmy ustalono na średnim możliwym poziomie, czyli $\beta_{ij}^{x} = 0{,}2$.

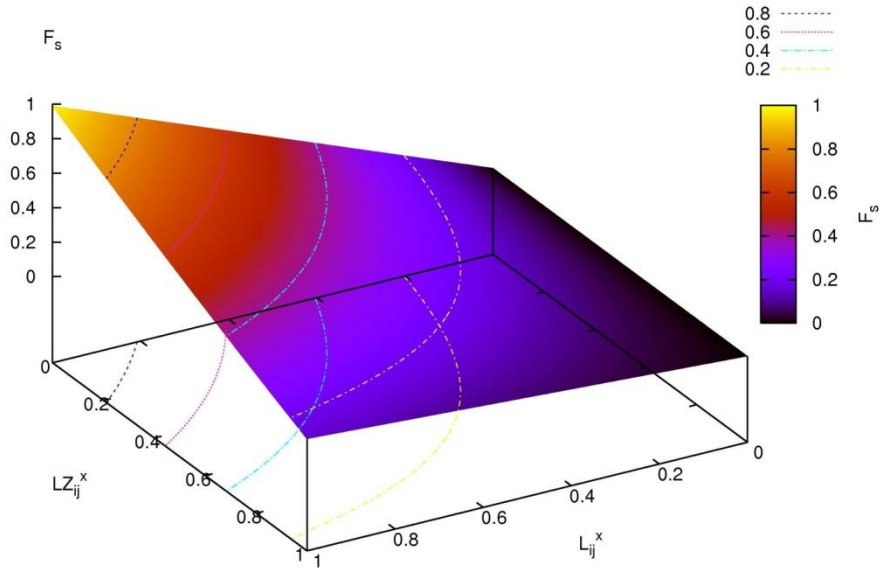



Rys. 3.16 Charakterystyka otrzymanego poziomu bezpieczeństwa ($F_S$) w zależności od użytych w danym procesie zasobów ($LZ$) oraz wybranych zabezpieczeń systemu ($L$) dla $LK$=$LP$=0,1 , $F_{ij}^{x} = \alpha_{ij}^{x} = 1$ oraz $\beta_{ij}^{x} = 0{,}5$.

Porównując rys. 3.15 oraz rys. 3.16 można zauważyć, że wraz ze wzrostem potencjalnie możliwych strat ($\omega$) wynikających z udanego ataku na zasoby systemu ($LZ$) poziom bezpieczeństwa maleje ($F_S$). W przypadku, gdy możliwe do zdobycia zasoby będą ustalone na poziomie $LZ \approx 0{,}8$ oraz poziom zabezpieczeń $L \approx 0{,}8$, różnica w poziomie zabezpieczeń wynosi około 0,1. Ta cecha potwierdza poprawność modelu, ponieważ jeżeli skutki ataku na proces elektroniczny są wyższe to poziom bezpieczeństwa powinien być niższy. Warto zwrócić uwagę, że uzyskiwane wartości poziomu bezpieczeństwa są niskie, ponieważ w założeniach przyjęto, że wiedza potrzebna do ataku oraz konieczne koszty są bardzo niewielkie ($LK$=$LP$=0,1).

W kolejnym, trzecim przypadku przyjęto takie same założenia dla procesu

elektronicznego jak w drugim z tą różnicą, że poziom potrzebnej wiedzy do ataku oraz koniecznych kosztów znacznie zwiększono i ustalono, że *LK*=*LP*=0,9. Na rys. 3.17 przedstawiono uzyskaną charakterystykę.



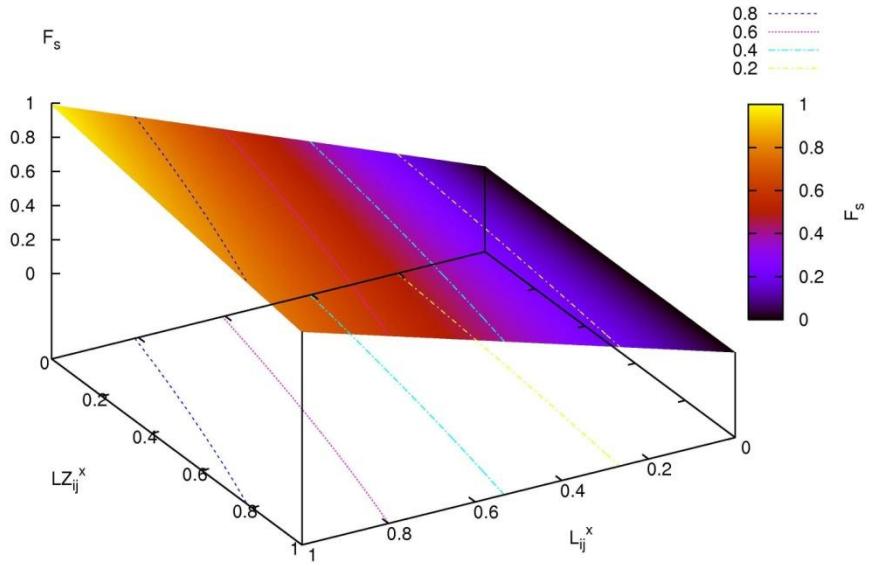

Rys. 3.17 Charakterystyka otrzymanego poziomu bezpieczeństwa ($F_S$) w zależności od użytych w danym procesie zasobów (*LZ*) oraz wybranych zabezpieczeń systemu (*L*) dla *LK*=*LP*=0,9 , $F_{ij}^{x} = \alpha_{ij}^{x} = 1$ oraz $\beta_{ij}^{x} = 0{,}5$.

Analizując przypadek drugi (rys. 3.16) i przypadek trzeci (rys. 3.17) można zauważyć, że uzyskiwane wartości poziomu bezpieczeństwa ($F_S$) zostały zwiększone. Jak widać na rys. 3.16, gdy w procesie elektronicznym możliwe zasoby do zdobycia są wysokie czyli na poziomie $LZ \approx 0{,}8$ i poziom zabezpieczeń jest również wysoki, czyli $L \approx 0{,}8$, wówczas uzyskany poziom bezpieczeństwa ma wartość $F_S \approx 0{,}3$. W porównaniu z rys. 3.17, gdzie $F_S$ = 0,1, wartość ta wzrosła aż o 0,2, czyli o 200%. Taka cecha modelu wskazuje, że jeżeli atakujący musi spełnić wysokie wymagania, żeby móc zaatakować konkretne zasoby systemu, wówczas poziom bezpieczeństwa procesu elektronicznego jest wysoki.

W kolejnym, czwartym przypadku (rys. 3.18) przyjęto takie same założenia jak w rozpatrywanym pierwszym przypadku z tą różnicą, że poziom potrzebnej wiedzy do ataku oraz koniecznych kosztów znacznie zwiększono i ustalono, że *LK*=*LP*=0,9. Na rys. 3.18 przedstawiono uzyskaną charakterystykę. Analizując ten przykład, można zauważyć, że gdy do wykonania ataku jest potrzebna duża wiedza i wysokie przygotowanie finansowe (*LK*=*LP*=0,9), wówczas wielkość zasobów możliwych do zdobycia (*LZ*) nie wpływa znacząco na obliczany poziom bezpieczeństwa ($F_S$).

Przykładowo, gdy poziom zabezpieczeń jest równy 0,6 ($L$=0,6), to różnica w uzyskanym poziomie bezpieczeństwa ($F_S$) dla możliwych zasobów do zdobycia równych $LZ$=0,9 i $LZ$=0,1 wynosi jedynie około 0,1.

Rozpatrywany czwarty przypadek (rys. 3.18) warto porównać z rozpatrywanym trzecim przypadkiem (rys. 3.17). W tych dwóch sytuacjach różnica polega jedynie na tym, że w trzecim przypadku założono, że wpływ udanego ataku na system jest bardzo duży i wynosi $F_{ij}^x = \alpha_{ij}^x = 1$ , $\beta_{ij}^x = 0{,}5$ a w czwartym jest bardzo niski i wynosi $F_{ij}^x = \alpha_{ij}^x = 0{,}2$ , $\beta_{ij}^x = 0{,}1$.



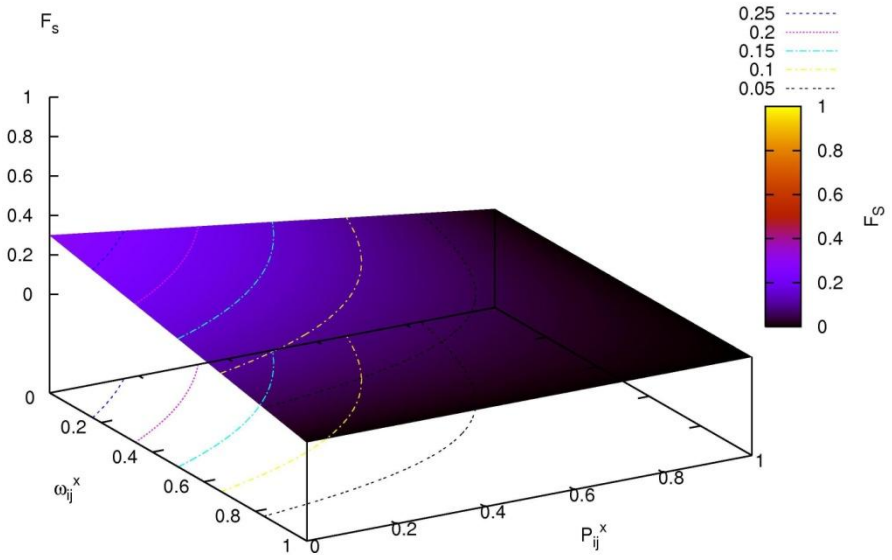

Rys. 3.18 Charakterystyka otrzymanego poziomu bezpieczeństwa ($F_S$) w zależności od użytych w danym procesie zasobów ($LZ$) oraz wybranych zabezpieczeń systemu ($L$) dla $LK$=$LP$=0,9, $F_{ij}^x = \alpha_{ij}^x = 0{,}2$ oraz $\beta_{ij}^x$ =0,1.

Porównując te dwie charakterystyki można zauważyć taką samą tendencję jak w porównanych wcześniej pierwszym (rys. 3.15) i czwartym przypadku (rys. 3.18). Tendencja ta pokazuje, że jeżeli użyte zasoby w danym procesie elektronicznym zostaną zaatakowane i poniesione straty będą niskie, wówczas uzyskany poziom bezpieczeństwa w małym stopniu zależy od możliwych do zdobycia zasobów.

W kolejnym, piątym rozważanym przypadku przedstawiono charakterystykę otrzymanego poziomu bezpieczeństwa ($F_S$) w zależności od prawdopodobieństwa zajścia zagrożenia ($P$) oraz wpływu udanego ataku na system ($\omega$). W tym przypadku zastosowane są niskie środki bezpieczeństwa, czyli poziom zabezpieczeń zdefiniowano na $L$=0,3. Nie wprowadzono poprawki do zastosowanych mechanizmów bezpieczeństwa, zabezpieczających proces elektroniczny, czyli parametr określający ich wrażliwość będzie równy 1 ($Z$=1).

Otrzymane wyniki zostały obliczone według formuły (3.10) (rozdział 3.5.1).

Analizując rys. 3.19 można zauważyć tendencję, że wraz ze wzrostem prawdopodobieństwa zajścia incydentu ($P$) oraz wpływu udanego ataku na system ($\omega$) maleje poziom bezpieczeństwa procesu elektronicznego ($F_S$). Warto zwrócić uwagę, że w przypadku, gdy zastosowany do danego procesu elektronicznego poziom zabezpieczeń jest na poziomie niskim ($L$=0,3), wówczas osiągany poziom bezpieczeństwa jest bardzo mały. W przedstawionym przypadku maksymalna osiągana wartość dla poziomu bezpieczeństwa nie przekracza 0,3 ($F_S < 0{,}3$).

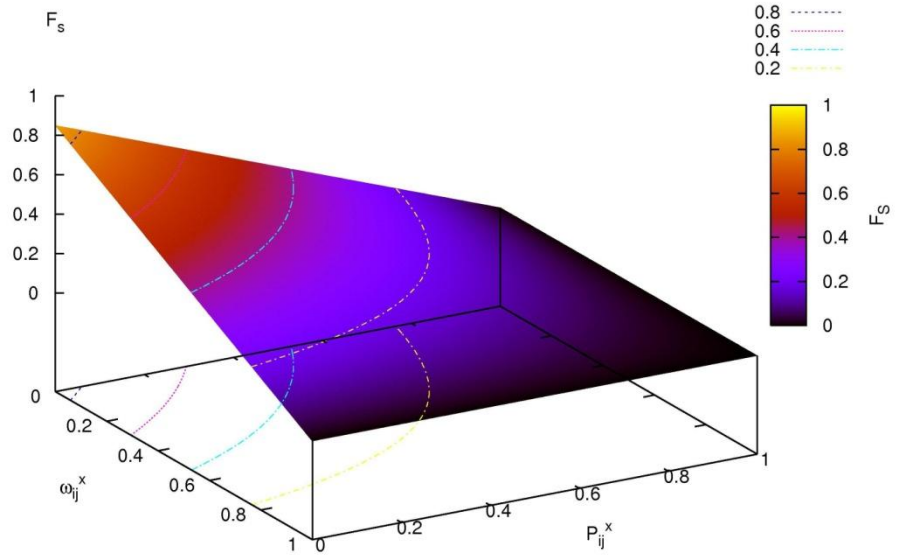



Rys. 3.19 Charakterystykę otrzymanego poziomu bezpieczeństwa ($F_S$) w zależności od prawdopodobieństwa zajścia zagrożenia ($P$) oraz wpływu udanego ataku na system ($\omega$) dla $L$=0,3 i $Z$=1.

Warto zastanowić się, jak w przypadku piątym zmieni się uzyskiwany poziom bezpieczeństwa ($F_S$), gdy zostanie podwyższony poziom zabezpieczeń ($L$). W kolejnym, szóstym przypadku (rys. 3.20) przedstawiono taką właśnie charakterystykę otrzymanego poziomu bezpieczeństwa ($F_S$) w zależności od prawdopodobieństwa zajścia zagrożenia ($P$) oraz wpływu udanego ataku na system ($\omega$). W tym przypadku zastosowano wysokie środki bezpieczeństwa, czyli poziom zabezpieczeń zdefiniowano na $L$=0,85.

Porównując rys. 3.19 i 4.20 można zauważyć, że wraz ze wzrostem poziomu zabezpieczeń (rys. 3.20) znacznie wzrasta uzyskiwany poziom bezpieczeństwa ($F_S$). Dla przykładu, gdy poziom zabezpieczeń jest niski $L$=0,3 (rys. 3.19) oraz proces elektroniczny jest narażony na prawdopodobieństwo zajścia incydentu na średnim poziomie ($P \approx 0{,}4$) oraz wpływ udanego ataku na system jest również na poziomie średnim ($\omega \approx 0{,}4$), wówczas poziom bezpieczeństwa przyjmuje niską

wartość i wynosi $F_S \approx 0{,}1$. Jeżeli dla tego samego przypadku zwiększymy poziom zabezpieczeń do $L$=0,85 (rys. 3.20), wówczas uzyskany poziom bezpieczeństwa wzrośnie trzykrotnie i osiągnie wartość około $F_S \approx 0{,}3$. Porównując przypadek piąty i szósty można zwrócić uwagę, że w przypadku szóstym, dla małych wartości prawdopodobieństwa zajścia incydentu ($P \approx 0{,}2$) oraz gdy potencjalny atak ma mały wpływ na system ($\omega \approx 0{,}2$), osiągany poziom bezpieczeństwa jest wyższy niż średni i jest równy około $F_S \approx 0{,}6$.

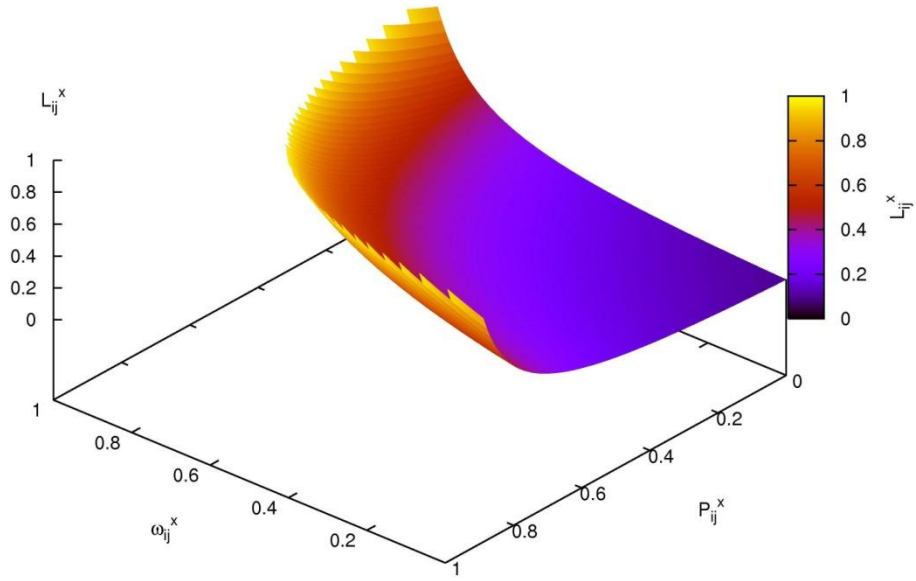



Rys. 3.20 Charakterystyka otrzymanego poziomu bezpieczeństwa ($F_S$) w zależności od prawdopodobieństwa zajścia zagrożenia ($P$) oraz wpływu udanego ataku na system ($\omega$) dla $L$=0,85 i $Z$=1.

W przedstawionych powyżej przypadkach zaprezentowano charakterystyki opisujące zależności elementów modelu skalowalności na uzyskiwany poziom bezpieczeństwa ($F_S$). W kolejnym kroku warto postawić pytanie, jakie mechanizmy bezpieczeństwa powinny być zastosowane w danym procesie elektronicznym, jeżeli chcemy osiągnąć pewien ustalony poziom bezpieczeństwa ($F_S$). Poziom bezpieczeństwa (rozdział 3.5) reprezentowany jest jako funkcje trzech parametrów: prawdopodobieństwa zajścia incydentu ($P$), wpływu udanego ataku na system ($\omega$) oraz wspomnianego poziomu zabezpieczeń ($L$). W kolejnych przypadkach zostanie rozpatrzone to zagadnienie. W przypadku siódmym (rys. 3.21 i 3.22) przedstawiono charakterystykę określającą wymagany poziom zabezpieczeń ($L$) dla danego procesu elektronicznego w zależności od prawdopodobieństwa zajścia incydentu ($P$) oraz wpływu udanego ataku na system ($\omega$). W opisywanym przypadku możliwe do zdobycia zasoby są wysokie i wynoszą $LZ$=0,8. Ustalono poziom bezpieczeństwa na poziomie niskim, czyli $F_S$ =0,1. Wyniki otrzymano

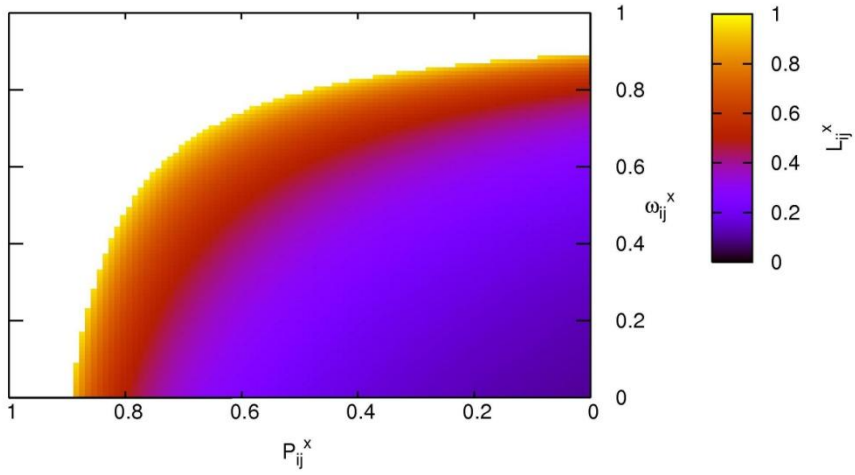
na podstawie formuły (3.10).

Na rys. 3.21 i 3.23, widać, że przedstawiona charakterystyka ma kształt ćwiartki „kielicha". Otrzymana postać „kielicha" charakteryzuje się tym, że istnieją duże przedziały wartości prawdopodobieństwa zajścia incydentu (*P*) oraz wpływu udanego ataku na system (ω), dla których wymagany poziom zabezpieczeń (*L*) jest bardzo zbliżony („denko kielicha").




Rys 4.21 Charakterystyka określająca wymagany poziom zabezpieczeń (*L*) dla danego procesu elektronicznego, w zależności od prawdopodobieństwa zajścia incydentu (*P*) oraz wpływu udanego ataku na system (*ω*) dla *LZ*=0,8 oraz $F_S$ =0,1.

Przykładowo, aby osiągnąć wymagany poziom bezpieczeństwa równy $F_S$ =0,1, dla procesu elektronicznego, dla którego wspomniane parametry $P < 0{,}6$ oraz $\omega < 0{,}6$, należy zastosować mechanizmy bezpieczeństwa, których zestawienie osiągnie poziom zabezpieczeń z przedziału: $0{,}2 < L < 0{,}4$. Taka charakterystyka wskazuje, że stosowane mechanizmy bezpieczeństwa nie muszą rosnąć wprost proporcjonalnie do wzrastającego prawdopodobieństwa zajścia incydentu (*P*) oraz wpływu udanego ataku na system (*ω*).

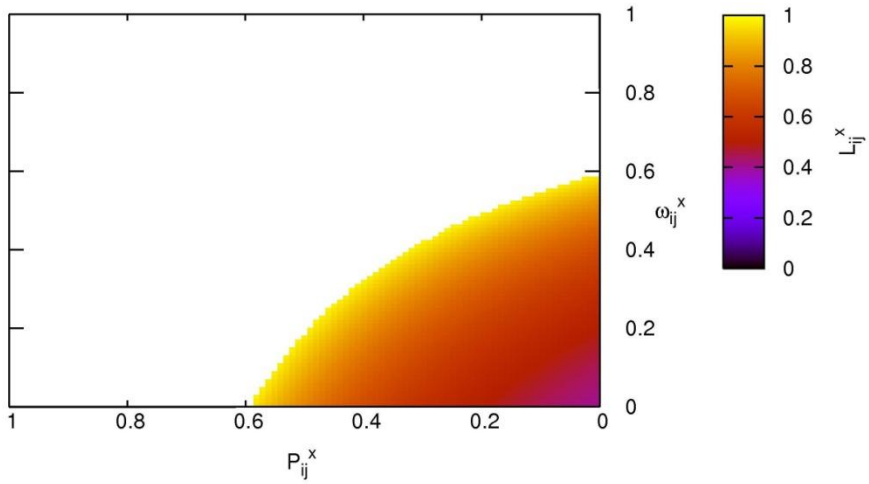



Rys 4.22 Charakterystyka określająca wymagany poziom zabezpieczeń ($L$) dla danego procesu elektronicznego, w zależności od prawdopodobieństwa zajścia incydentu ($P$) oraz wpływu udanego ataku na system ($\omega$) dla $LZ$=0,8 oraz $F_S$ =0,1.

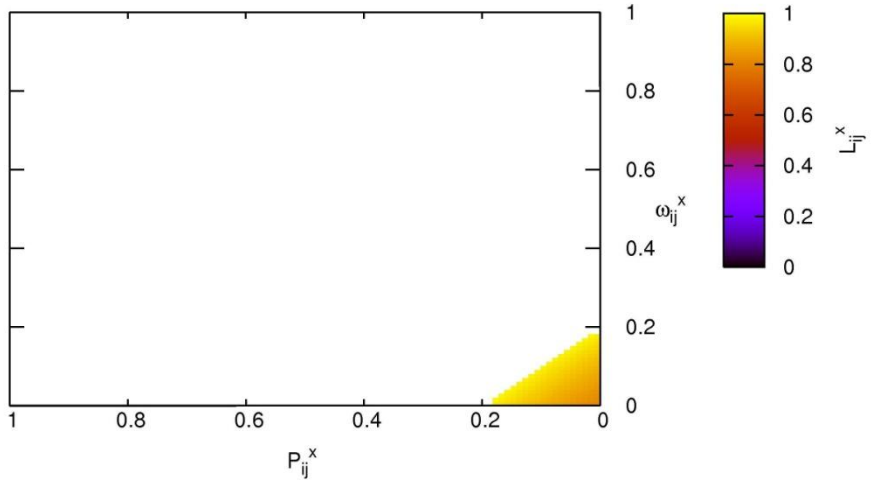
Jak wspomniano wyżej, otrzymana na rys. 3.21 i 3.22 charakterystyka ma postać ćwiartki „kielicha". Kolejną cechą takiej charakterystyki jest to, że obok dużych przedziałów, które są mało wrażliwe na wymogi mechanizmów bezpieczeństwa („denko kielicha"), są przedziały, które są bardzo wrażliwe na zastosowane środki zabezpieczające („ścianki kielicha"). Przykładowo, dla założonego poziomu bezpieczeństwa $F_S$ = 0,1 oraz, gdy prawdopodobieństwa zajścia incydentu jest wysokie ($P \approx 0{,}7$) a wpływ udanego ataku na system jest również wysoki ($\omega \approx 0{,}7$), istnieje tylko wąski przedział wartości, jakie musi osiągnąć poziom zabezpieczeń i wynosi $L \approx 0{,}9$ („ścianka kielicha").

W kolejnym kroku warto zadać pytanie: czy charakterystyka „kielicha" zostanie utrzymana dla przypadków, w których wymagany poziom zabezpieczeń będzie zwiększany? Na rys. 3.23 przedstawiono charakterystykę określającą wymagany poziom zabezpieczeń ($L$) dla danego procesu elektronicznego w zależności od prawdopodobieństwa zajścia incydentu ($P$) oraz wpływu udanego ataku na system ($\omega$) dla średniego wymaganego poziomu bezpieczeństwa równego $F_S$ = 0,4. Na rys. 3.24 przyjęta takie same założenia, jak we wcześniejszym przykładzie, lecz ustalono wymagany poziom bezpieczeństwa na wysokim poziomie $F_S$ =0,8.

`




Rys 4.23 Charakterystyka określająca wymagany poziom zabezpieczeń ($L$) dla danego procesu elektronicznego, w zależności od prawdopodobieństwa zajścia incydentu ($P$) oraz wpływu udanego ataku na system ($\omega$) dla $LZ$=0,8 oraz $F_S$ =0,4.




Rys 4.24 Charakterystyka określająca wymagany poziom zabezpieczeń ($L$) dla danego procesu elektronicznego, w zależności od prawdopodobieństwa zajścia incydentu ($P$) oraz wpływu udanego ataku na system ($\omega$) dla $LZ$=0,8 oraz $F_S$ =0,8.

Porównując otrzymane wyniki dla różnych wymaganych poziomów bezpieczeństwa można stwierdzić, że w przypadku gdy poziom bezpieczeństwa jest równy $F_S$ =0,4 (rys. 3.23), wówczas wcześniej otrzymany „kielich" (rys. 3.22 i 3.23) traci swój charakter. Na rys. 3.23 można zaobserwować

proporcjonalny wzrost wymaganych mechanizmów bezpieczeństwa ($L$) w zależności od prawdopodobieństwa zajścia incydentu ($P$) oraz wpływu udanego ataku na system ($\omega$). Podobną tendencje, można zaobserwować na rys. 3.24, gdy wymagany poziom bezpieczeństwa został ustalony na wysokim poziomie $F_S$ =0,8.

Analizując otrzymane charakterystyki, w których następował wzrost wymaganego poziomu bezpieczeństwa, czyli rys. 3.22 gdzie $F_S$ = 0,1 , rys. 3.23, gdzie $F_S$ = 0,4 oraz rys. 3.24, gdzie $F_S$ = 0,8, można zauważyć ciekawą tendencję. Tendencja ta charakteryzuje się tym, że wraz ze wzrostem wymaganego poziomu bezpieczeństwa możliwość jego osiągnięcia przez proces elektroniczny znacznie maleje. Na rys. 3.24 taka charakterystyka jest szczególnie widoczna, ponieważ osiągnięcie poziomu bezpieczeństwa na poziomie $F_S$ = 0,8 jest możliwe jedynie wówczas, gdy prawdopodobieństwo zajścia incydentu ($P$) i wpływ udanego ataku na system ($\omega$) jest bardzo mały i wynoszą na przykład $P \approx 0{,}1$ i $\omega \approx 0{,}1$.

Przedstawione w rozdziale 3.5.1 charakterystyki opisują kluczowy element określany w modelu skalowanego bezpieczeństwa, czyli poziom bezpieczeństwa danego procesu elektronicznego. W tym rozdziale przedstawiono szereg przypadków, które opisywały zależności poszczególnych elementów przedstawianego modelu od obliczanego końcowego poziomu bezpieczeństwa. Analizując wszystkie przedstawione w powyższym rozdziale przypadki można stwierdzić, że uzyskane charakterystyki zaprezentowanych teoretycznie przypadków, które obliczane były na podstawie modelu skalowalności, posiadają tendencje pokrywające się z przypadkami rzeczywistymi.

## 3.6. Schemat postępowania dla prezentowanej metodologii skalowanego bezpieczeństwa

We wcześniejszych rozdziałach przedstawiono oraz scharakteryzowano model skalowanego bezpieczeństwa. W bieżącym rozdziale opisany jest schemat postępowania dla wspomnianej metodologii wprowadzającej model skalowanego bezpieczeństwa. Schemat postępowania został podzielony na cztery zasadnicze fazy, czyli inicjalizację skalowanego bezpieczeństwa, definiowanie protokołu kryptograficznego, ustalenie parametrów modelu skalowanego bezpieczeństwa dla konkretnych wersji protokołu oraz obliczenie poziomu bezpieczeństwa dla danej wersji protokołu.

Faza pierwsza składa się z czterech kroków. W pierwszym kroku tworzymy tabelę usług bezpieczeństwa, której przykład został zaprezentowany w tab. 3.1 (rozdział 3.2). Tabela ta przedstawia zestawienie możliwych usług bezpieczeństwa wraz z realizującymi je mechanizmami.

W kroku drugim, w wyniku szczegółowej analizy ustalane są wkłady poszczególnych mechanizmów zapewniających ochronę odpowiednich usług bezpieczeństwa w modelu reprezentowane przez parametr $L^{XY}$, gdzie $X$ jest usługą bezpieczeństwa, a $Y$ indywidualnym numerem mechanizmu bezpieczeństwa (rozdział 3.2).

`

W kroku trzecim tworzymy grafy bezpieczeństwa dla poszczególnych usług bezpieczeństwa oraz definiujemy ich wzajemne zależności, przypisując funkcje logiczne do krawędzi łączących wierzchołki. Grafy te posłużą do obliczenia prawdopodobieństwa zajścia incydentu. Opis zagadnień związanych z grafami bezpieczeństwa zaprezentowany jest w rozdziale 3.3.

Czwarty krok polega na zdefiniowaniu wartości parametrów określających prawdopodobieństwo zajścia incydentu dla mechanizmów zawartych w poszczególnych utworzonych grafach bezpieczeństwa. Wspomniane wartości wyznaczane są po szczegółowej analizie. Parametry charakteryzujące poszczególne wierzchołki grafu zostały opisane w rozdziale 3.3.1.

Opisana wyżej pierwsza faza, czyli inicjalizacja skalowanego bezpieczeństwa, jest uzależniona od aktualnego poziomu wiedzy informatycznej, czyli wiedzy na temat ochrony informacji oraz technologii teleinformatycznych. Zagadnienia zawarte w tej części wykonywane są tylko raz i kolejne trzy fazy bazują na tych ustaleniach. Oczywiście, wraz ze wzrostem wiedzy informatycznej na temat ochrony informacji czynność ta powinna być okresowo powtarzana.

W dalszej części rozdziału zaprezentowana jest druga faza schematu postępowania, czyli definiowanie protokołu kryptograficznego. Czynności tam zawarte podzielone są na dwa kroki i wykonywane są jednorazowo dla każdego rozpatrywanego protokołu kryptograficznego.

W pierwszym kroku wybieramy protokół kryptograficzny, dla którego chcemy zastosować prezentowany w pracy mechanizm skalowanego bezpieczeństwa. Protokół ten może składać się z dowolnej liczby podprotokołów, które to z kolei mogą być realizowane w wielu krokach.

Kiedy mamy już ustalony protokół kryptograficzny, to w drugim kroku dokonujemy szczegółowego podziału tego protokołu na podprotokoły kryptograficzne a w ich obrębie na poszczególne realizujące go kroki.

Dalsza część rozdziału opisuje trzecią fazę schematu postępowania, czyli ustalenie parametrów modelu skalowanego bezpieczeństwa dla danej wersji protokołu kryptograficznego. Przewidziane tu czynności wykonywane są indywidualnie dla każdej wersji zdefiniowanego protokołu kryptograficznego. Zgodnie z założeniami modelu, wersje te realizują taką samą usługę elektroniczną, opisaną przez zdefiniowany protokół kryptograficzny, lecz na innym poziomie bezpieczeństwa (rozdział 3.1). Pierwsze trzy kroki trzeciej fazy postępowania odpowiedzialne są za ustalenie parametrów potrzebnych do obliczenia poziomu zabezpieczeń (rozdział 3.2). Czwarty i piąty krok za ustalenie parametrów potrzebnych do obliczenia prawdopodobieństwa zajścia incydentu (rozdział 3.3), a krok szósty za parametry określające wpływ udanego ataku na system (rozdział 3.4).

Opiszemy teraz bardziej szczegółowo trzecią fazę konstrukcji skalowanego bezpieczeństwa. W pierwszym kroku trzeciej fazy schematu postępowania, dla wszystkich kroków każdego rozpatrywanego podprotokołu kryptograficznego, definiujemy wymagane w danej wersji protokołu usługi bezpieczeństwa. Wybór

ten może być zapisany w postaci tabeli, której przykład zaprezentowany jest w tab. 3.2. Wiersze reprezentowane są przez skróty nazw poszczególne usług bezpieczeństwa, a kolumny reprezentują poszczególne kroki danego podprotokołu. Jeżeli w danym kroku konkretna usługa bezpieczeństwa jest wymagana, wówczas wpisywane jest słowo „tak", a jeżeli nie - wówczas słowo „nie".

Tab. 3.2 Tabela prezentująca formę zapisu wymaganych usług bezpieczeństwa dla kroków podprotokołów.

| | **Kroki podprotokołu** | | |
|---|---|---|---|
| **Usługi bezpieczeństwa** | | **Krok 1** | **Krok 2** |
| | **I** | TAK | TAK |
| | **C** | TAK | NIE |
| | **NRM** | NIE | TAK |
| | **Au** | TAK | NIE |
| | **AN** | NIE | TAK |

Jeżeli wymagane usługi bezpieczeństwa dla poszczególnych kroków podprotokołu zostały już określone, to wówczas należy wybrać mechanizmy bezpieczeństwa, które będą realizowały te usługi. Taki wybór jest dokonywany w kolejnym, drugim kroku trzeciej fazy schematu postępowania. Wybór ten bazuje na zdefiniowanej w pierwszej fazie tabeli bezpieczeństwa, która zawiera zestawienie usług bezpieczeństwa wraz z realizującymi je mechanizmami bezpieczeństwa. Do realizacji konkretnej usługi bezpieczeństwa można wybrać różne mechanizmy bezpieczeństwa, które przewidziane są w tabeli bezpieczeństwa. Wybór ten może być również zapisany w postaci tabeli a jej przykład jest przedstawiony w tab. 3.3. Tak samo jak w tab. 3.2, wiersze reprezentowane są przez skróty nazw poszczególnych usług bezpieczeństwa, a kolumny reprezentują poszczególne kroki danego podprotokołu. Jeżeli w danym kroku ma być użyty konkretny mechanizm bezpieczeństwa zaprezentowany w tabeli bezpieczeństwa, to wówczas w odpowiednie rubryce wpisujemy jego numer.

`

Tab. 3.3 Tabela prezentująca formę zapisu wybranych mechanizmów bezpieczeństwa realizujących poszczególne usługi bezpieczeństwa dla konkretnych kroków podprotokołów.

| | **Kroki podprotokołu** | | |
|---|---|---|---|
| **Wybrane mechanizmy bezpieczeństwa** | | **Krok 1** | **Krok 2** |
| | **I** | 1,2,3 | 1,2,3,5,6 |
| | **C** | 1 | NIE |
| | **NRM** | NIE | 1,2 |
| | **Au** | 2 | NIE |
| | **AN** | NIE | 2 |

W tym kroku można zdefiniować różne wersje rozpatrywanego podprotokołu, które będą różniły się wykorzystanymi w nich mechanizmami bezpieczeństwa. W tym celu dla każdej wersji można utworzyć osobną tabelę, w której dla poszczególnych kroków będą zaznaczone użyte mechanizmy bezpieczeństwa.

Trzeci kroku trzeciej fazy schematu postępowania polega na określeniu poziomu wrażliwości użytych mechanizmów bezpieczeństwa. Charakterystyka tego parametru jest przedstawiona w rozdziale 3.2.1.

W kroku czwartym i piątym trzeciej fazy postępowania ustalamy parametry potrzebne do obliczenia prawdopodobieństwa zajścia incydentu. W tym celu w czwartym kroku wybieramy wierzchołki grafów bezpieczeństwa, utworzonych w pierwszej fazie schematu postępowania, które odpowiadają wcześniej wybranym z tabeli bezpieczeństwa mechanizmom bezpieczeństwa. Wybór tan dokonywany jest dla wszystkich kroków poszczególnych podprotokołów kryptograficznych. Jak opisano w rozdziale 3.3.2 wierzchołki grafów łączą się ze sobą za pomocą krawędzi, którym przypisane są funkcje boolowskie. Wybierając konkretną gałąź, tworzymy jednocześnie funkcją boolowską poszczególnych składników bezpieczeństwa. Warunkiem poprawnego wyboru jest otrzymanie wyniku funkcji boolowskiej równej 1. Dokonany wybór może być zapisany za pomocą funkcji boolowskiej, która łączy poszczególne wybrane wierzchołki odpowiednimi operacjami boolowskimi. Wierzchołkom wybranym z odpowiednich grafów bezpieczeństwa, wierzchołkom przypisywana jest wartość 1 a wszystkim pozostałym wartość 0. Przykładowy zapis wyboru dokonany na podstawie grafu dla usługi niezaprzeczalności (rys. 3.4) może wyglądać następująco:

Wierzchołki = 3.1 = 3.1.2 = 3.1.2.2 = 3.1.6 = 3.1.3 = 3.1.3.2 = 1,

$F_{BOOL}$= (3.1.3.1 $\oplus$ 3.1.3.2) $\vee$ [ (3.1.2.1 $\oplus$ 3.1.2.2) $\vee$ (3.1.6)],

gdzie wybrane wierzchołki poprzedzone są wyrazem „Wierzchołki”, a utworzona na ich podstawie funkcja boolowska określeniem „$F_{BOOL}$”. Jeżeli we wcześniejszym drugim kroku zostały zdefiniowane różne wersje danego podprotokołu, wówczas wybór wierzchołków jest dokonywany dla każdej wersji indywidualnie.

W kroku piątym ustalane są dalsze parametry potrzebne do obliczania prawdopodobieństwa zajścia incydentu dla danej usługi. Do tych parametrów zaliczamy dodatkowe parametry bezpieczeństwa, które charakteryzują konkretny proces elektroniczny. Wśród nich definiujemy globalne zasoby możliwe do zdobycia w danym procesie elektronicznym (*PP*), rodzaj instytucji realizującej proces (*I*), hipotetyczne ryzyko poniesione przez atakującego w wyniku wykrycia włamania (*H*). Parametry te opisane są w rozdziale 3.3.1. Innymi określanymi w tym kroku parametrami są te, które potrzebne są do ostatecznego obliczenia prawdopodobieństwa zajścia incydentu. Do nich zaliczamy: współczynniki, które określają potencjalne przygotowanie atakującego pod względem poziomu wiedzy ( $\omega_{LK}$ ) oraz do poniesienia kosztów ( $\omega_{LP}$ ). Obliczając końcową wartość prawdopodobieństwa zajścia incydentu, można uwzględnić stosowną poprawkę, która szczegółowo jest opisana w rozdziale 3.3.3. Jej wartość jest zależna między innymi od ilości prawdopodobieństw pojedynczych zagrożeń, które zostaną uwzględnione w poprawce. W tym kroku należy tę liczbę określić, czyli parametr *N* (formuła (3.6)). Parametry te opisane są w rozdziale 3.3.3.

W ostatnim, szóstym kroku trzeciej fazy schematu postępowania, określamy parametry opisujące wpływ udanego ataku na system. W tym celu określane są parametry opisujące maksymalne zasoby zdobyte podczas udanego ataku (*LZ*), finansowe straty podczas udanego ataku (*F*), straty finansowe konieczne do usunięcia awarii, które zostały spowodowane udanym atakiem ( $\alpha$ ) oraz straty poniesione w wyniku spadku reputacji firmy ( $\beta$ ). Parametry te opisane są w rozdziale 3.4. Podczas tego kroku, można wprowadzić kolejne rozróżnienie wersji rozpatrywanego protokołu. Rozróżnienie to będzie polegało na określeniu różnego wpływu udanego ataku na system dla poszczególnych wersji protokołu, które jest charakteryzowane przez wspomniane wyżej parametry. Dokonany wybór może być zapisany w postaci tabeli, której przykład jest przedstawiony w tab. 3.4. W tym przypadku protokół składa się z dwóch kroków, a wymagane usługi w tych krokach są adekwatne z tymi które zostały zdefiniowane w pierwszym kroku trzeciej fazy postępowania (tab. 3.2). W tab. 3.4 wprowadzono rozróżnienie wersji protokołów, zostały one określone jako wersja A i wersja B.

`

Tab. 3.4 Tabela prezentująca formę zapisu wybranych parametrów określających wpływ udanego ataku na system dla poszczególnych usług bezpieczeństwa oraz konkretnych kroków podprotokołu.

| | **Wersja A** | | | | **Wersja B** | | | |
|---|---|---|---|---|---|---|---|---|
| | ***LZ*** | ***F*** | $\alpha$ | $\beta$ | ***LZ*** | ***F*** | $\alpha$ | $\beta$ |
| *Krok 1* | | | | | | | | |
| **I** | 0,5 | 0,5 | 0,3 | 0,3 | 0,5 | 0,2 | 0,1 | 0,2 |
| **C** | 0,3 | 0,8 | 0,2 | 0,3 | 0,3 | 0,1 | 0,5 | 0,2 |
| **Au** | 0,7 | 0,2 | 0,1 | 0,6 | 0,7 | 0,35 | 0,2 | 0,4 |
| *Krok 2* | | | | | | | | |
| **I** | 0,8 | 0,9 | 0,8 | 0,4 | 0,8 | 0,5 | 0,3 | 0,3 |
| **NRM** | 0,9 | 0,2 | 0,3 | 0,8 | 0,9 | 0,2 | 0,1 | 0,2 |
| **AN** | 0,3 | 0,2 | 0,5 | 0,9 | 0,3 | 0,15 | 0,3 | 0,1 |

Czwarta faza schematu postępowania składa się z jednego kroku. Na tym etapie obliczany jest poziom bezpieczeństwa dla poszczególnej wersji protokołu. Szczegóły tego kroku opisane są w rozdziale 3.5.

Omówione wyżej cztery fazy wchodzące w skład schematu postępowania dla prezentowanej metodologii skalowanego bezpieczeństwa wykonywane są z różną częstotliwością. Pierwsza i druga faza schematu postępowania, czyli inicjacja modelu skalowanego bezpieczeństwa oraz definiowanie protokołu kryptograficznego jest stała dla konkretnego analizowanego przypadku. Natomiast faza druga i trzecia, czyli ustalenie parametrów modelu skalowanego bezpieczeństwa dla danej wersji protokołu oraz obliczenie poziomu bezpieczeństwa jest zmienna. Każdorazowe wykonanie czynności tam zawartych tworzy osobny protokół realizujący określoną usługę na indywidualnym i ustalonym poziomie bezpieczeństwa. Odpowiednio modyfikując zawarte w modelu parametry skalowanego bezpieczeństwa, opisane w szczegółowo w rozdziale 3, możemy osiągnąć różne poziomy bezpieczeństwa protokołów kryptograficznych realizujących ten sam proces elektroniczny.

W celu podsumowania przedstawionego wyżej schematu postępowania dla prezentowanej metodologii skalowanego bezpieczeństwa utworzono tab. 3.5, która zawiera, w skróconej formie, opis poszczególnych faz omawianego schematu postępowania.

Tab. 3.5 Schemat postępowania dla prezentowanej metodologii skalowanego

bezpieczeństwa.

| | |
|---|---|
| ***I. Inicjalizacja modelu skalowanego bezpieczeństwa*** | **1.** Tworzymy tabelę bezpieczeństwa |
| | **2.** Ustalamy wartości parametrów dla poszczególnych mechanizmów bezpieczeństwa |
| | **3.** Tworzymy grafy bezpieczeństwa |
| | **4.** Ustalamy wartości parametrów dla poszczególnych grafów bezpieczeństwa |
| ***II. Definiowanie protokołu kryptograficznego*** | **1.** Wybieramy protokół kryptograficzny realizujący dany proces elektroniczny |
| | **2.** Dzielimy wybrany protokół kryptograficzny na podprotokoły, a następnie na pojedyncze kroki |
| ***III. Ustalanie parametrów modelu skalowanego bezpieczeństwa dla danej wersji protokołu kryptograficznego*** | **1.** Definiujemy wymagane usługi bezpieczeństwa dla pojedynczych kroków każdego rozpatrywanego podprotokołu |
| | **2.** Przydzielamy mechanizmy bezpieczeństwa realizujące usługi bezpieczeństwa dla wszystkich wyodrębnionych kroków |
| | **3.** Określamy poziom wrażliwości mechanizmów bezpieczeństwa |
| | **4.** Wybieramy wierzchołki grafów bezpieczeństwa dla wszystkich wyodrębnionych kroków |
| | **5.** Ustalamy pozostałe parametry dla modelu określającego prawdopodobieństwo zajścia incydentu |
| | **6.** Ustalamy parametry określające wpływ udanego ataku na system |
| ***IV. Obliczanie poziomu bezpieczeństwa*** | **1.** Obliczmy poziom bezpieczeństwa dla danej wersji protokołu |

## 3.7. Przykładowe zastosowanie skalowanego bezpieczeństwa dla protokołu SSL v.3.00

W rozdziale 3 dotychczas omówiono zagadnienia związane z metodologią wprowadzającą model skalowanego bezpieczeństwa. W rozdziale 3.6 przedstawiono schemat postępowania dla tej metodologii. W celu lepszego zilustrowania sposobu postępowania w modelu skalowanego bezpieczeństwa, w bieżącym rozdziale przedstawiono przykładowe zastosowanie modelu dla istniejącego protokołu kryptograficznego. Do tego celu wybrano protokół kryptograficzny stworzonym przez Netscape Communications Corporation [82], czyli SSL (ang. Secure Sockets Layer) w wersji 3.00.

Jest to protokół, którego głównym celem jest zapewnienie prywatności oraz niezawodności pomiędzy dwoma komunikującymi się stronami (aplikacjami). Protokół składa się z dwóch warstw. Na niższym poziomie, znajduje się SSL

`

Record Protocol, który funkcjonuje na najwyższej warstwie dowolnego niezawodnego protokołu transportowego, czyli np. TCP [30]. SSL Record Protocol jest używany do enkapsulacji [30] różnych protokołów funkcjonujących na wyższych poziomach. Opisywany protokół SSL składa się również z drugiej, funkcjonującej na wyższym poziomie warstwie. Na tym wyższym poziomie znajduje się SSL Handshake Protocol który między innymi pozwala dokonać wzajemnej autoryzacji dwóch stron protokołu, czyli stronę serwera i klienta. SSL Handshake Protocol przed wysłaniem przez aplikację pierwszych danych, negocjuje również między komunikującymi się stronami, algorytmy szyfrowania oraz klucze kryptograficzne. Wielką zaletą protokołu SSL jest jego niezależność względem protokołu konkretnej aplikacji.

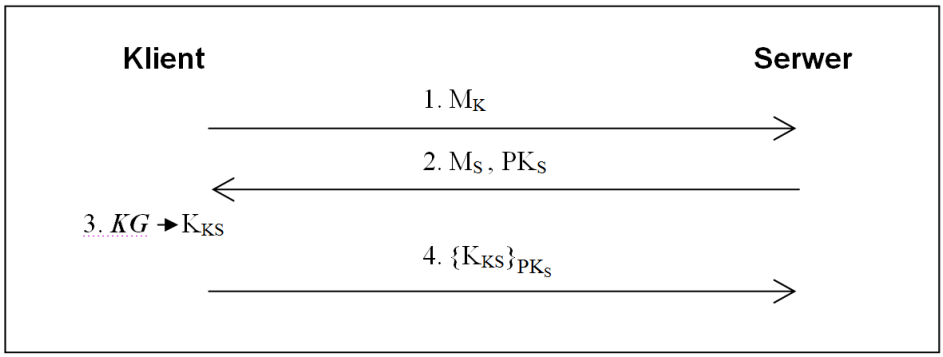
Protokół SSL pozwala nawiązać połączenie między stronami realizującymi daną aplikację, które może spełniać trzy podstawowe usługi bezpieczeństwa, czyli: integralność, poufność oraz autoryzację. Integralność przesyłanych danych jest osiągana za pomocą kryptograficznych sum kontrolnych (MAC), które opierają swoje działanie na kryptograficznych funkcjach skrótu (np. SHA, MD5 [65, 74]). Poufność przesyłanych danych jest realizowana za pomocą szyfrowania algorytmami symetrycznymi (np. DES [2], RC4 [76]). Autoryzacja stron biorących udział w protokole jest wykonywana przy użyciu kryptografii asymetrycznej (np. RSA[73], DSS[64]). Wymienione usługi bezpieczeństwa mogą być realizowane za pomocą różnych algorytmów kryptograficznych (wybranych z algorytmów udostępnianych przez konkretną implementację protokołu SSL), a ponadto dla każdego algorytmu mogą być modyfikowane parametry kryptograficzne, czyli np. klucze kryptograficzne. Elementy te są modyfikowane za pomocą, wspomnianego wyżej protokołu, czyli SSL Handshake Protocol. Modyfikacja tych elementów (wpływających na bezpieczeństwo) pozwala wprowadzić rozróżnienie protokołu SSL ze względu na poziom zastosowanych zabezpieczeń. W ten sposób można utworzyć różne wersji tego samego protokołu, lecz realizowanego na różnym poziomie bezpieczeństwa. W książce opisano metodologię skalowanego bezpieczeństwa, za pomocą której można dokonać takiej modyfikacji.

Jak wspomniano wyżej protokół SSL składa się z dwóch protokołów, czyli SSL Record Protocol i SSL Handshake Protocol. Model skalowalności będzie zastosowany dla drugiego protokołu (SSL Handshake Protocol), ponieważ właśnie ten protokół jest odpowiedzialny za ustalenie używanych algorytmów kryptograficznych oraz ich parametrów kryptograficznych.

### 3.7.1. Opis protokołu SSL Handshake Protocol

W dalszej części rozdziału opisano w formie skróconej protokół SSL Handshake Protocol. Kroki tego protokołu są zmienne w zależności od konkretnych wymagań realizujących go aplikacji [82]. W rozpatrywanym przypadku przyjęto najpopularniejszą jego realizacje, czyli taką, w której klient początkowo chce zweryfikować tożsamość serwera a następnie chce nawiązać

z nim poufne połączenie. Schemat przepływu informacji dla rozpatrywanego przypadku jest przedstawiony na rys. 3.25.




Rys. 3.25 Schemat przepływu informacji dla danej wersji protokołu SSL Handshake Protocol.

Strona klienta chcąca nawiązać połączenie wysyła wiadomość $M_K$ do strony serwera, która na taką wiadomość odpowiada podobną wiadomością, czyli $M_S$. Wiadomości $M_K$ i $M_S$ są używane do ustalenia parametrów bezpieczeństwa dla konkretnego ustanawianego połączenia. Do tych atrybutów należą: wersja protokołu, numer identyfikacyjny sesji, wybór algorytmów kryptograficznych oraz ich opcji kryptograficznych, metody kompresji, wymiana wygenerowanych przez obie strony liczb pseudolosowych. Oprócz wiadomości uzgadniającej parametry bezpieczeństwa danego połączenia $M_S$ serwer przesyła swój klucz publiczny oraz przypisany do niego certyfikat $PK_S$. Otrzymana przez klienta wiadomość $M_S$ zawiera wszelkie informacje potrzebne do ustalenia używanych podczas połączenia algorytmów kryptograficznych oraz do wygenerowania (stosownych do wyboru) kluczy kryptograficznych. W kolejnym etapie strona klienta weryfikuje otrzymany od serwera certyfikat $PK_S$. Po pozytywnej weryfikacji generuje (*KG*) odpowiednie klucze kryptograficzne ($K_{KS}$), które to następnie szyfruje za pomocą otrzymanego od strony serwera klucza publicznego $PK_S$. W następnym kroku tak utworzony przez klienta szyfrogram jest przesyłany do serwera. Ostatnim elementem opisywanego protokołu jest dostarczenie uzgodnionych kluczy do aplikacji ustanawiających połączenie.

### 3.7.2. Inicjalizacja modelu skalowanego bezpieczeństwa dla protokołu SSL Handshake Protocol

Jak opisano w rozdziale 3.6, schemat postępowania dla prezentowanej metodologii skalowanego bezpieczeństwa składa się z czterech faz. Pierwsza

faza, czyli inicjalizacja modelu skalowalności, składa się z czterech kroków. W bieżącym rozdziale dla wybranej i opisanej w rozdziale 3.7.1 wersji protokołu SSL Handshake Protocol, zastosowano wszystkie kroki przewidziane w fazie pierwszej.

W pierwszym kroku tworzymy tabelę bezpieczeństwa, która przedstawia zestawienie możliwych usług bezpieczeństwa wraz z realizującymi je mechanizmami. Protokół SSL umożliwia wybór trzech podstawowych usług bezpieczeństwa, czyli integralności, poufności oraz autoryzacji [82]. Konstruując tabelę bezpieczeństwa należy wybrać mechanizmy bezpieczeństwa, realizujące możliwe do wprowadzenia usługi bezpieczeństwa. Do tego celu można zastosować mechanizmy, które są przewidziane w konkretnym protokole, takie informacje są zawarte w dokumentacji protokołów[82].

Tab. 3.6 Tabela przedstawiająca możliwe usługi bezpieczeństwa wraz ze składnikami bezpieczeństwa realizującymi te usługi dla omawianego protokołu SSL Handshake Protocol .

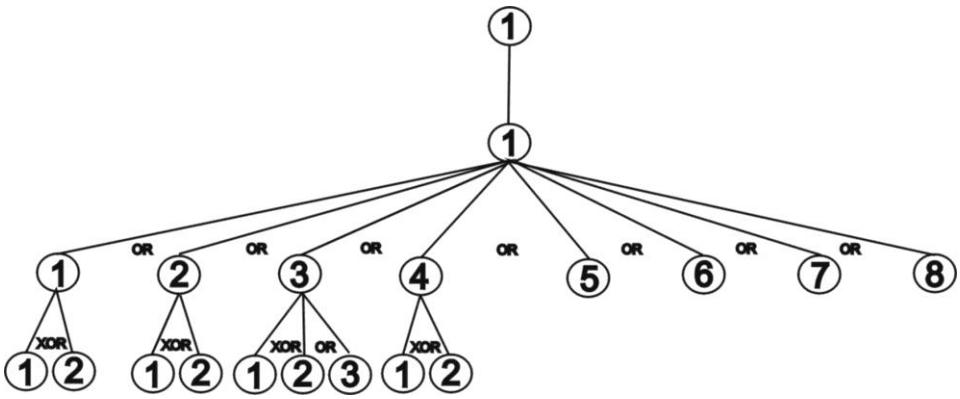
| | **Mechanizmy bezpieczeństwa** | | | | | |
|---|---|---|---|---|---|---|
| **Usługi bezpieczeństwa** | | 1 | 2 | 3 | 4 | 5 |
| | **Integralność danych (I)** | Suma kontrolna (MAC) $L^{I1}$=60% | Zaawansowane Zarządzanie kluczami $L^{I2}$=10% | Zwiększenie długości kluczy $L^{I3}$=20% | Audyt $L^{I4}$=10% | |
| | **Poufność danych (C)** | Szyfrowanie $L^{C1}$= 60% | Zaawansowane Zarządzanie kluczami $L^{C2}$=10% | Zwiększenie długości kluczy $L^{C3}$=30% | | |
| | **Autoryzacja stron (Au)** | Podpis cyfrowy $L^{Au1}$=50% | Zaawansowane Zarządzanie kluczami $L^{Au2}$=10% | Zaawansowane zarządzanie certyfikatami $L^{Au3}$=10% | Zwiększenie długości kluczy $L^{Au4}$=25% | Audyt $L^{Au5}$= 5% |

Tab. 3.6 przedstawia możliwe usługi bezpieczeństwa wraz z realizującymi je mechanizmami bezpieczeństwa dla omawianego protokołu SSL Handshake Protocol. Mechanizmy tam zawarte opisane są w rozdziale 2.2.2.

W drugim kroku, ustalamy wartości parametrów dla poszczególnych

mechanizmów bezpieczeństwa, zawartych w tabeli bezpieczeństwa (tab. 3.6). Wartości przedstawione w tab. 3.6 zostały wyznaczone na podstawie intuicji autora.

Trzeci krok pierwszej fazy schematu postępowania polega na utworzeniu grafów bezpieczeństwa dla możliwych do zastosowania w danym przypadku usług bezpieczeństwa. W rozpatrywanym przypadku będą to grafy dla usług integralności, poufności oraz autoryzacji. Na rys. 3.26 przedstawiony jest graf dla usługi integralności, na rys. 3.27 dla usługi poufności a na rys. 3.28 dla usługi autoryzacji. Poniżej grafów znajdują się opisy do poszczególnych wierzchołków grafów. Wierzchołki te charakteryzowane są przez odpowiednie parametry (rozdział 3.3.1). W ostatnim czwartym kroku pierwszej fazy schematu postępowania, przyporządkowywane są wartości do tych parametrów. W opisywanym przypadku parametry te zostały dobrane na drodze intuicji autora.




Rys. 3.26 Graf dla usługi integralności dla protokołu SSL Handshake Protocol

**1. Integralność**

1.1 Kryptograficzna suma kontrolna (MAC) *(LZ,LK,LP= dziedziczenie)*

1.1.1 Zarządzanie kluczami kryptograficznymi *(LZ,LK,LP = dziedziczenie)*

1.1.1.1 Moduły kryptograficzne (min. poziom 2) [33] (LZ=80%, LK=70%, LP=80%, C=0,05, M=0,01)

1.1.1.2 Moduły kryptograficzne (min. poziom 3) [33] (LZ=80%, LK=80%, LP=90%, C=0,05, M=0,02)

1.1.2 Porty i interfejsy modułów kryptograficznych *(LZ,LK,LP = dziedziczenie)*

1.1.2.1 Moduły kryptograficzne (min. poziom 2) [33] (LZ=70%, LK=50%, LP=80%)

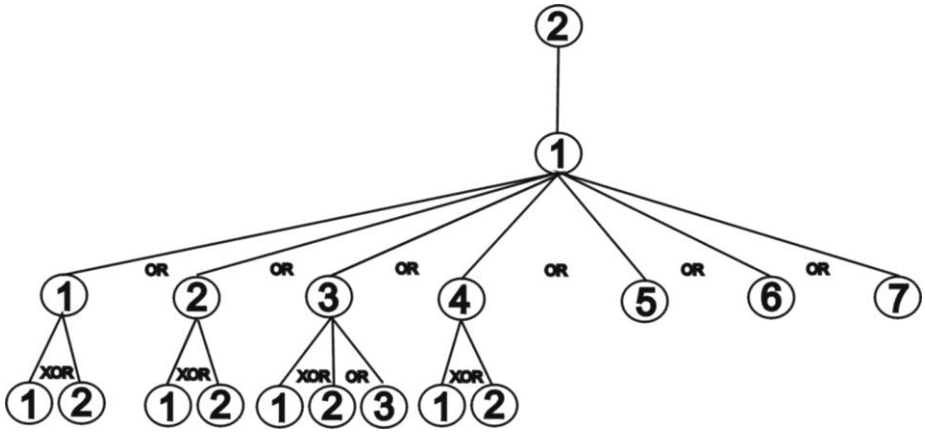
1.1.2.2 Moduły kryptograficzne (min. poziom 3) [33] (LZ=70%, LK=70%, LP=80%)

1.1.3 Specyfikacja modułów kryptograficznych *(LZ,LK,LP = dziedziczenie)*

1.1.3.1 Moduły kryptograficzne (min. poziom 2) [33] (LZ=70%, LK=50%, LP=80%)

`

1.1.3.2 Moduły kryptograficzne (min. poziom 3) [33] (LZ=70%, LK=70%, LP=80%)
1.1.3.3 Zwiększenie długości kluczy (LZ=10%, LK=60%, LP=40%) (LK=+10%, LP=+10%)
1.1.4 Generowanie kluczy *(LZ,LK,LP= dziedziczenie* )
1.1.4.1 Moduły kryptograficzne (min. poziom 2) [20], Techniki bezpieczeństwa
(min. EAL 3) [33] (LZ=80%, LK=70%, LP=80%)
1.1.4.2 Moduły kryptograficzne (min. poziom 3) [20], Techniki bezpieczeństwa
(min. EAL 4) [33], (LZ=80%, LK=80%, LP=90%, M=0,01)
1.1.5 Rozpowszechnianie kluczy (LZ=80%, LK=50%, LP=80%, C=0,02)
1.1.6 Użycie kluczy (LZ=80%, LK=80%, LP=50%)
1.1.7 Zakończenie cyklu kluczy (LZ=30%, LK=80%, LP=50%, C=0,01)
1.1.8 Wewnętrzny Audyt (LZ=10%, LK=60%, LP=40%, C=0,01, M=0,03) (LK=+5%, LP=+5%)




Rys. 3.27 Graf dla usługi poufności dla protokołu SSL Handshake Protocol.

2. Poufność
2.1 Szyfrowanie *(LZ,LK,LP= dziedziczenie)* Szyfrowanie *(LZ,LK,LP= dziedziczenie)*
2.1.1 Zarządzanie kluczami kryptograficznymi *(LZ,LK,LP = dziedziczenie)*
2.1.1.1 Moduły kryptograficzne (min. poziom 2) [33] (LZ=80%, LK=70%, LP=80%, C=0,05, M=0,01)
2.1.1.2 Moduły kryptograficzne (min. poziom 3) [33] (LZ=80%, LK=80%, LP=90%, C=0,05, M=0,02)
2.1.2 Porty i interfejsy modułów kryptograficznych *(LZ,LK,LP = dziedziczenie)*
2.1.2.1 Moduły kryptograficzne (min. poziom 2) [33] (LZ=70%, LK=50%, LP=80%)

2.1.2.2 Moduły kryptograficzne (min. poziom 3) [33] (LZ=70%, LK=70%, LP=80%)

2.1.3 Specyfikacja modułów kryptograficznych *(LZ,LK,LP = dziedziczenie)*

2.1.3.1 Moduły kryptograficzne (min. poziom 2) [33] (LZ=70%, LK=50%, LP=80%)

2.1.3.2 Moduły kryptograficzne (min. poziom 3) [33] (LZ=70%, LK=70%, LP=80%)

2.1.3.3 Zwiększenie długości kluczy (LZ=10%, LK=60%, LP=40%) (LK=+10%, LP=+10%)

2.1.4 Generowanie kluczy *(LZ,LK,LP= dziedziczenie* )

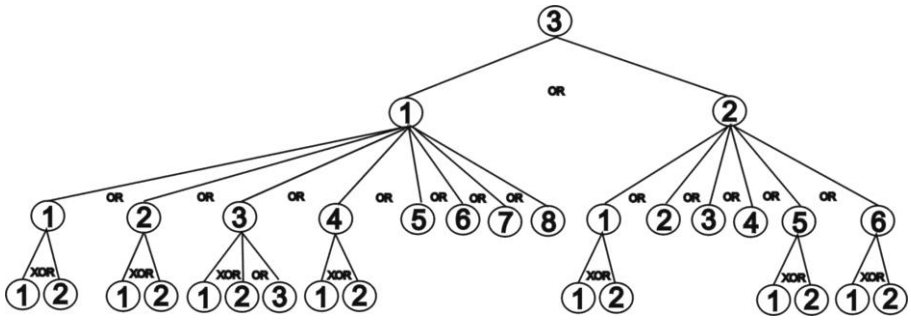
2.1.4.1 Moduły kryptograficzne (min. poziom 2) [20], Techniki bezpieczeństwa
(min. EAL 3) [33] (LZ=80%, LK=70%, LP=80%)

2.1.4.2 Moduły kryptograficzne (min. poziom 3) [20], Techniki bezpieczeństwa
(min. EAL 4) [33], (LZ=80%, LK=80%, LP=90%, M=0,01)

2.1.5 Rozpowszechnianie kluczy (LZ=80%, LK=50%, LP=80%, C=0,02)

2.1.6 Użycie kluczy (LZ=80%, LK=80%, LP=50%)

2.1.7 Zakończenie cyklu kluczy (LZ=30%, LK=80%, LP=50%, C=0,01)




Rys. 3.28 Graf dla usługi autoryzacji dla protokołu SSL Handshake Protocol.

3. Autoryzacja

3.1 Podpis cyfrowy *(LZ,LK,LP= dziedziczenie)*

3.1.1 Zarządzanie kluczami kryptograficznymi *(LZ,LK,LP = dziedziczenie)*

3.1.1.1 Moduły kryptograficzne (min. poziom 2) [33] (LZ=80%, LK=70%, LP=80%, C=0,05, M=0,01)

3.1.1.2 Moduły kryptograficzne (min. poziom 3) [33] (LZ=80%, LK=80%, LP=90%, C=0,05, M=0,02)

3.1.2 Porty i interfejsy modułów kryptograficznych *(LZ,LK,LP = dziedziczenie)*

3.1.2.1 Moduły kryptograficzne (min. poziom 2) [33] (LZ=70%, LK=50%, LP=80%)

3.1.2.2 Moduły kryptograficzne (min. poziom 3) [33] (LZ=70%, LK=70%, LP=80%)

3.1.3 Specyfikacja modułów kryptograficznych *(LZ,LK,LP = dziedziczenie)*

`

3.1.3.1 Moduły kryptograficzne (min. poziom 2) [33] (LZ=70%, LK=50%, LP=80%)
3.1.3.2 Moduły kryptograficzne (min. poziom 3) [33] (LZ=70%, LK=70%, LP=80%)
3.1.3.3 Zwiększenie długości kluczy (LZ=10%, LK=60%, LP=40%) (LK=+10%, LP=+10%)
3.1.4 Generowanie kluczy *(LZ,LK,LP= dziedziczenie* )
3.1.4.1 Moduły kryptograficzne (min. poziom 2) [20], Techniki bezpieczeństwa
(min. EAL 3) [33] (LZ=80%, LK=70%, LP=80%)
3.1.4.2 Moduły kryptograficzne (min. poziom 3) [20], Techniki bezpieczeństwa
(min. EAL 4) [33], (LZ=80%, LK=80%, LP=90%, M=0,01)
3.1.5 Rozpowszechnianie kluczy (LZ=80%, LK=50%, LP=80%, C=0,02)
3.1.6 Użycie kluczy (LZ=80%, LK=80%, LP=50%)
3.1.7 Zakończenie cyklu kluczy (LZ=30%, LK=80%, LP=50%, C=0,01)
3.1.8 Wewnętrzny Audyt (LZ=10%, LK=60%, LP=40%, C=0,01, M=0,03)(LK=+5%, LP=+5%)
3.2 Zarządzanie certyfikatami *(LZ,LK,LP= dziedziczenie)*
3.2.1 Rejestracja podmiotu *(LZ,LK,LP= dziedziczenie)*
3.2.1.1 Szczegółowa weryfikacja strony ubiegającej się o certyfikat (LZ=70%, LK=30%, LP=90%, C=0,02)
3.2.1.2 Podstawowa weryfikacja stron ubiegających się o certyfikat (LZ=70%, LK=20%, LP=70%, C=0,02, M=0,01)
3.2.2 Uaktualnienie certyfikatu (LZ=70%, LK=50%, LP=30%, C=0,02)
3.2.3 Generowanie certyfikatu (LZ=70%, LK=80%, LP=80%, M=0,01)
3.2.4 Wewnętrzny Audyt (LZ=10%, LK=60%, LP=40%, C=0,01, M=0,03)(LK=+5%, LP=+5%)
3.2.5 Rozgłaszanie certyfikatu *(LZ,LK,LP= dziedziczenie)*
3.2.5.1 Weryfikacja certyfikatów jest możliwa zgodnie z warunkami ustalonymi przez dany C.A. (LZ=30%, LK=60%, LP=30%, C=0,03, M=0,01)
3.2.5.2 Weryfikacja certyfikatów jest możliwa 24h na dobę, 7 dni w tygodniu
(LZ=30%, LK=80%, LP=30%, C=0,03, M=0,02)
3.2.6 Zawieszenie i odwołanie certyfikatu *(LZ,LK,LP= dziedziczenie)*
3.2.6.1 Odwołanie certyfikatu oraz zmodyfikowanie list certyfikatów (CRL) w ciągu 72h od uzyskania stosownego żądania (LZ=30%, LK=60%, LP=40%, C=0,01)
3.2.6.2 Odwołanie certyfikatu oraz zmodyfikowanie list certyfikatów (CRL) w ciągu 24h od uzyskania stosownego żądania *(*LZ=30%, LK=80%, LP=40%, C=0,01, M=0,01*)*

## 3.7.3. Definiowanie protokołu SSL Handshake Protocol

Druga faza schematu postępowania dla przedstawianej metodologii skalowanego bezpieczeństwa polega na zdefiniowaniu protokołu kryptograficznego (rozdział 3.6). Ta czynność jest wykonywana w dwóch

krokach. W pierwszym wybierany jest protokół kryptograficzny realizujący dany proces elektroniczny a w drugim wybrany protokół dzielony jest na osobne podprotokoły, a te następnie na pojedyncze kroki.

W rozpatrywanym przypadku model skalowalności będzie zastosowany do protokołu SSL Handshake Protocol, który w skrócie został omówiony w rozdziale 3.7.1. W kroku drugim należy podzielić ten protokół na podprotokoły, a następnie na pojedyncze kroki. Rozpatrywany protokół nie zawiera w sobie osobnych podprotokołów, natomiast warto przypomnieć, że sam jest podprotokołem protokołu SSL v.3.00 [82]. W kroku drugim, omawianej fazy schematu postępowania, należy podzielić protokół SSL Handshake Protocol na pojedyncze kroki. Ten podział jest przedstawiona poniżej.

**Krok 1**

W pierwszym kroku strona klienta przesyła w formie jawnej wiadomość $M_K$.

**Krok 2**

Strona serwera otrzymuje wiadomość wysłaną przez stronę klienta $M_K$, a następnie również w formie jawnej, wysyła odpowiedz do klienta, czyli $M_S$. Razem z wiadomością $M_S$ przesyłany jest klucz publiczny serwera wraz z przypisanym do niego certyfikatem $PK_S$.

**Krok 3**

W kroku trzecim przez stronę klienta weryfikowany jest klucz publiczny otrzymany od serwera $PK_S$. Po pozytywnej weryfikacji na podstawie otrzymanych danych, które zostały określone przez stronę serwera w wiadomości $M_S$, generowane są odpowiednie klucze $K_{KS}$, które następnie posłużą do utworzenia poufnego połączenia między komunikującymi się stronami.

**Krok 4**

W ostatnim kroku utworzone klucze $K_{KS}$ są szyfrowane za pomocą otrzymanego klucza publicznego serwera $PK_S$, a następnie w formie zaszyfrowanej są przesyłane do serwera.

### 3.7.4. Ustalenie parametrów modelu skalowanego bezpieczeństwa dla rozpatrywanej wersji protokołu SSL Handshake Protocol

Kolejna, trzecia faza schematu postępowania polega na ustaleniu parametrów modelu skalowanego bezpieczeństwa dla rozpatrywanej wersji protokołu. Jak opisano w rozdziale 3.6 trzecia faza składa się z sześciu kroków.

W pierwszym kroku trzeciej fazy postępowania definiujemy wymagane usługi bezpieczeństwa dla pojedynczych kroków rozpatrywanego podprotokołu. Podział na kroki dla danego przypadku zostały przedstawiony w rozdziale 3.7.3. Wybór usług bezpieczeństwa został zapisany w tab. 3.7.

Tab. 3.7 Tabela prezentująca wymagane usług bezpieczeństwa dla

`

poszczególnych
kroków protokołu SSL Handshake Protocol.

| | Kroki podprotokołu | | | | |
|---|---|---|---|---|---|
| **Usługi bezpieczeństwa** | | **Krok 1** | **Krok 2** | **Krok 3** | **Krok 4** |
| | **I** | TAK | TAK | TAK | TAK |
| | **C** | NIE | NIE | TAK | TAK |
| | **Au** | NIE | NIE | TAK | NIE |

W kolejnym kroku przydzielamy mechanizmy bezpieczeństwa realizujące wybrane usługi bezpieczeństwa dla wszystkich wyodrębnionych kroków. Dla rozpatrywanego przypadku możliwe do wybrania elementy bezpieczeństwa zostały przedstawione w tab. 3.6. Na tym etapie realizacji metodologii skalowanego bezpieczeństwa można wprowadzić pierwsze rozróżnienie w wersjach realizowanego protokołu, które będzie polegało na doborze różnych mechanizmów bezpieczeństwa do realizacji tych samych kroków. Dla omawianego protokołu SSL Handshake Protocol wprowadzono dwie wersje protokołu. Pierwsza charakteryzująca się wyborem podstawowych mechanizmów bezpieczeństwa i druga, która zakłada podwyższone środki ochrony informacji. Wybór mechanizmów bezpieczeństwa dla wersji pierwszej jest przedstawiony w tab. 3.8, a dla wersji drugiej w tab. 3.9.

Tab. 3.8 Tabela prezentująca wybrane mechanizmy bezpieczeństwa realizujących poszczególne usługi bezpieczeństwa dla konkretnych kroków protokołów SSL Handshake Protocol. w wersji 1.

| **Wersja 1** | **Kroki podprotokołu** | | | | |
|---|---|---|---|---|---|
| **Usługi bezpieczeństwa** | | **Krok 1** | **Krok 2** | **Krok 3** | **Krok 4** |
| | **I** | 1 | 1 | 1 | 1 |
| | **C** | NIE | NIE | 1 | 1 |
| | **Au** | NIE | NIE | 1 | NIE |

Tab. 3.9 Tabela prezentująca wybrane mechanizmy bezpieczeństwa

realizujących poszczególne usługi bezpieczeństwa dla konkretnych kroków protokołów SSL Handshake Protocol. w wersji 2.

| **Wersja 2** | **Kroki podprotokołu** | | | | |
|---|---|---|---|---|---|
| **Usługi bezpieczeństwa** | | **Krok 1** | **Krok 2** | **Krok 3** | **Krok 4** |
| | **I** | 1,2 | 1,2 | 1,2,4 | 1,2 |
| | **C** | NIE | NIE | 1,2 | 1,2,3 |
| | **Au** | NIE | NIE | 1,2,5 | NIE |

W trzecim kroku trzeciej fazy schematu postępowania należy określić poziom wrażliwości mechanizmów bezpieczeństwa (rozdział 3.2.1). W rozpatrywanym przypadku nie będą uwzględniane dodatkowe czynniki wpływające na bezpieczeństwo procesu elektronicznego, czyli parametr określany jako wrażliwości mechanizmów bezpieczeństwa jest równy $Z=1$.

W następnym czwarty i piątym kroku trzeciej fazy postępowania ustalamy parametry potrzebne do obliczenia prawdopodobieństwa zajścia incydentu. W tym celu w czwartym kroku wybieramy wierzchołki grafów bezpieczeństwa, utworzonych w pierwszej fazie schematu postępowania (rys. 3.26, 3.26, 3.28), które odpowiadają wcześniej wybranym, z tabeli bezpieczeństwa (tab. 3.6), mechanizmom bezpieczeństwa (tab. 3.8, 3.9). Wybór dokonywany jest dla wszystkich wymaganych usług bezpieczeństwa oraz dla wszystkich kroków podprotokołu. Poniżej przedstawiono dokonany wybór dla dwóch wersji protokołu SSL Handshake Protocol.

***Wersja 1 (tab. 3.8)***

**Krok 1**

Integralność

Wierzchołki = 1.1 = 1.1.1 = 1.1.1.1 = 1.1.2 = 1.1.2.1 = 1.1.3 = 1.1.3.1 =1.1.6 =1

$F_{BOOL}$= (1.1.1.1 $\oplus$ 1.1.1.2.) $\vee$ (1.1.2.1 $\oplus$ 1.1.2.2) $\vee$ (1.1.3.1 $\oplus$ 1.1.3.2) $\vee$ 1.1.6

**Krok 2**

Integralność

Wierzchołki = 1.1 = 1.1.1 = 1.1.1.1 = 1.1.2 = 1.1.2.1 = 1.1.3 = 1.1.3.1 =1.1.6 = 1

$F_{BOOL}$= (1.1.1.1 $\oplus$ 1.1.1.2.) $\vee$ (1.1.2.1 $\oplus$ 1.1.2.2) $\vee$ (1.1.3.1 $\oplus$ 1.1.3.2) $\vee$ 1.1.6

**Krok 3**

Integralność

`

Wierzchołki = 1.1 = 1.1.1 = 1.1.1.1 = 1.1.2 = 1.1.2.1 = 1.1.3 = 1.1.3.1 = 1.1.6 =1
$F_{BOOL}$= (1.1.1.1⊕1.1.1.2.) ∨ (1.1.2.1⊕1.1.2.2) ∨ (1.1.3.1⊕1.1.3.2) ∨ 1.1.6

Poufność

Wierzchołki = 2.1 = 2.1.1 = 2.1.1.1 = 2.1.2 = 2.1.2.1 = 2.1.3 = 2.1.3.1 = 2.1.4. = 2.1.4.1 = 2.1.4 = 1
$F_{BOOL}$= (2.1.1.1⊕2.1.1.2.) ∨ (2.1.2.1⊕2.1.2.2) ∨ (2.1.3.1⊕2.1.3.2) ∨ (2.1.4.1⊕2.1.4.2) ∨ 2.1.4

Autoryzacja

Wierzchołki = 3.1 = 3.1.1 = 3.1.1.1 = 3.1.2 = 3.1.2.1 = 3.1.3 = 3.1.3.1 = 3.1.6 = 3.2 = 3.2.5 = 3.2.5.1 = 1
$F_{BOOL}$= (3.1.1.1⊕3.1.1.2.) ∨ (3.1.2.1⊕3.1.2.2) ∨ (3.1.3.1⊕3.1.3.2) ∨ 3.1.6 ∨ (3.2.5.1⊕3.2.5.2)

**Krok 4**

Integralność

Wierzchołki = 1.1 = 1.1.1 = 1.1.1.1 = 1.1.2 = 1.1.2.1 = 1.1.3. = 1.1.3.1 = 1.1.6 =1
$F_{BOOL}$= (1.1.1.1⊕1.1.1.2.) ∨ (1.1.2.1⊕1.1.2.2) ∨ (1.1.3.1⊕1.1.3.2) ∨ 1.1.6

Poufność

Wierzchołki = 2.1 = 2.1.1 = 2.1.1.1 = 2.1.2 = 2.1.2.1 = 2.1.3 = 2.1.3.1 = 2.1.5 = 2.1.6 = 1
$F_{BOOL}$= (2.1.1.1⊕2.1.1.2.) ∨ (2.1.2.1⊕2.1.2.2) ∨ (2.1.3.1⊕2.1.3.2) ∨ 2.1.5 ∨ 2.1.6

***Wersja 2 (tab. 3.9)***

**Krok 1**

Integralność

Wierzchołki = 1.1 = 1.1.1 = 1.1.1.2 = 1.1.2 = 1.1.2.2 = 1.1.3 = 1.1.3.2 = 1.1.6 =1
$F_{BOOL}$= (1.1.1.1⊕1.1.1.2.) ∨ (1.1.2.1⊕1.1.2.2) ∨ (1.1.3.1⊕1.1.3.2) ∨ 1.1.6

**Krok 2**

Integralność

Wierzchołki = 1.1 = 1.1.1 = 1.1.1.2 = 1.1.2 = 1.1.2.2 = 1.1.3 = 1.1.3.2 =1.1.6 =1
$F_{BOOL}$= (1.1.1.1⊕1.1.1.2.) ∨ (1.1.2.1⊕1.1.2.2) ∨ (1.1.3.1⊕1.1.3.2) ∨ 1.1.6

**Krok 3**

Integralność

Wierzchołki = 1.1 = 1.1.1 = 1.1.1.2 = 1.1.2 = 1.1.2.2 = 1.1.3 = 1.1.3.2 = 1.1.6 = 1.1.8 = 1
$F_{BOOL}$= (1.1.1.1⊕1.1.1.2.) ∨ (1.1.2.1⊕1.1.2.2) ∨ (1.1.3.1⊕1.1.3.2) ∨ 1.1.6 ∨ 1.1.8

Poufność

Wierzchołki = 2.1 = 2.1.1 = 2.1.1.2 = 2.1.2 = 2.1.2.2 = 2.1.3 = 2.1.3.2 = 2.1.4. = 2.1.4.2 = 2.1.4 = 1

$F_{BOOL}$= (2.1.1.1 ⊕ 2.1.1.2.) ∨ (2.1.2.1 ⊕ 2.1.2.2) ∨ (2.1.3.1 ⊕ 2.1.3.2) ∨ (2.1.4.1 ⊕ 2.1.4.2) ∨ 2.1.4

Autoryzacja

Wierzchołki = 3.1 = 3.1.1 = 3.1.1.2 = 3.1.2 = 3.1.2.2 = 3.1.3 = 3.1.3.2 = 3.1.6 = 3.1.8 = 3.2 = 3.2.5 = 3.2.5.1 = 3.2.4 = 1

$F_{BOOL}$= (3.1.1.1 ⊕ 3.1.1.2.) ∨ (3.1.2.1 ⊕ 3.1.2.2) ∨ (3.1.3.1 ⊕ 3.1.3.2) ∨ 3.1.6 ∨ 3.1.8 ∨ (3.2.5.1 ⊕ 3.2.5.2) ∨ 3.2.4

**Krok 4**

Integralność

Wierzchołki = 1.1 = 1.1.1 = 1.1.1.2 = 1.1.2 = 1.1.2.2 = 1.1.3 = 1.1.3.2 = 1.1.6 = 1

$F_{BOOL}$= (1.1.1.1 ⊕ 1.1.1.2.) ∨ (1.1.2.1 ⊕ 1.1.2.2) ∨ (1.1.3.1 ⊕ 1.1.3.2) ∨ 1.1.6

Poufność

Wierzchołki = 2.1 = 2.1.1 = 2.1.1.2 = 2.1.2 = 2.1.2.2 = 2.1.3 = 2.1.3.2 = 2.1.3.3 = 2.1.4. = 2.1.4.2 = 2.1.4 = 1

$F_{BOOL}$= (2.1.1.1 ⊕ 2.1.1.2.) ∨ (2.1.2.1 ⊕ 2.1.2.2) ∨ [(2.1.3.1 ⊕ 2.1.3.2) ∨ 2.1.3.3] ∨ (2.1.4.1 ⊕ 2.1.4.2) ∨ 2.1.4

W następnym, piątym kroku ustalane są dalsze parametry potrzebne do obliczenia prawdopodobieństwa zajścia incydentu (rozdział 3.3.1). W rozpatrywanym przypadku przyjęto, że w procesie elektroniczny można zdobyć duże zasoby, czyli parametr *PP*=0,08, rodzaj instytucji realizujący proces elektroniczny, niech będzie o podwyższonym ryzyku (np. bank), czyli *I*=0,08, natomiast hipotetyczne ryzyko poniesione przez atakującego w wyniku wykrycia włamania niech będzie niskie, czyli *H*=0,01. Innymi parametrami, które należy w tym kroku określić, jest potencjalne przygotowanie atakujących pod względem wiedzy ($\omega_{LK}$) oraz poniesionych kosztów ($\omega_{LP}$). W rozpatrywanym przypadku ustaliliśmy, że napastnicy mają średnią wiedzę, czyli $\omega_{LK}$ = 0,6 oraz mogą ponieść średnie koszty finansowe, czyli $\omega_{LP}$ = 0,5. W kroku piątym należy również określić ewentualną uwzględnianą poprawkę do całkowitej wartości prawdopodobieństwa zajścia incydentu. Jej wartość jest zależna między innymi od ilości cząstkowych prawdopodobieństw, które zostaną uwzględnione w poprawce. W tym kroku należy tę liczbę określić, czyli podać parametr *N* (formuła (3.6)). W rozpatrywanym przypadku ustalono, że wartość parametru *N=2*. To zagadnienie jest szczegółowo opisane w rozdziale 3.3.3.

Ostatni, szósty krok trzeciej fazy schematu postępowania polega na zdefiniowaniu parametrów określających wpływ udanego ataku na system. W tym celu określane są parametry opisujące maksymalne zasoby zdobyte podczas udanego ataku (*LZ*), finansowe straty podczas udanego ataku (*F*), straty

`

finansowe konieczne do usunięcia awarii, które zostały spowodowane udanym atakiem ($\alpha$) oraz straty poniesione w wyniku spadku reputacji firmy ($\beta$).

Tak jak podano w rozdziale 3.6 w tym miejscu można wprowadzić kolejne rozróżnienie wersji protokołu. W rozpatrywanym przypadku wprowadzono dwie wersje. Pierwsza będzie aplikacją, która przy pomocy protokołu SSL v.3.00 będzie łączyła się z witryną banku internetowego a następnie dokona przelewu na duża kwotę pieniędzy np. 100000 PLN. Druga wersja aplikacji również będzie łączyła się z witryną banku i dokonywała przelewu, ale tym razem kwota będzie znacznie niższa, czyli 1000 PLN. W pierwszym przypadku aplikacja będzie procesem o dużym wpływie udanego ataku na system. Natomiast wersja druga będzie miała dużo mniejszy wpływ udanego ataku na system. W wersji drugiej parametry określające finansowe straty podczas udanego ataku (*F*) oraz straty finansowe konieczne do usunięcia awarii, które zostały spowodowane udanym atakiem ($\alpha$) zostały znacznie obniżone w stosunku do wersji pierwszej. Pierwsza wersja będzie nazywana wersją A, a druga wersją B. W tab. 3.10 przedstawiono ustalone wartości wspomnianych parametrów. Definiowanie parametrów określających wpływ udanego ataku na system jest ostatnim krokiem trzeciej fazy schematu postępowania dla prezentowanej metodologii skalowanego bezpieczeństwa.

Tab. 3.10 Tabela prezentująca wybrane parametry charakteryzujące wpływ udanego ataku na system dla poszczególne usługi bezpieczeństwa oraz konkretnych kroków protokołu SSL Handshake Protocol. w dwóch wersjach A i B.

| | **Wersja A** | | | | **Wersja B** | | | |
|---|---|---|---|---|---|---|---|---|
| | ***LZ*** | ***F*** | $\alpha$ | $\beta$ | ***LZ*** | ***F*** | $\alpha$ | $\beta$ |
| *Krok 1* | | | | | | | | |
| **I** | 0,8 | 0,6 | 0,5 | 0,5 | 0,8 | 0,15 | 0,1 | 0,2 |
| *Krok 2* | | | | | | | | |
| **I** | 0,8 | 0,8 | 0,5 | 0,7 | 0,8 | 0,15 | 0,1 | 0,3 |
| *Krok 3* | | | | | | | | |
| **I** | 0,8 | 0,5 | 0,5 | 0,5 | 0,8 | 0,15 | 0,1 | 0,2 |
| **C** | 0,8 | 0,9 | 0,9 | 0,7 | 0,8 | 0,25 | 0,1 | 0,35 |
| **Au** | 0,8 | 0,5 | 0,4 | 0,3 | 0,8 | 0,2 | 0,1 | 0,1 |
| *Krok 4* | | | | | | | | |
| **I** | 0,8 | 0,5 | 0,5 | 0,6 | 0,8 | 0,15 | 0,1 | 0,25 |
| **C** | 0,8 | 0,9 | 0,8 | 0,5 | 0,8 | 0,25 | 0,1 | 0,15 |

### 3.7.5. Obliczanie poziomu bezpieczeństwa dla rozpatrywanej wersji protokołu SSL Handshake Protocol

Kiedy wszystkie parametry opisujące model skalowanego bezpieczeństwa

dla danej wersji protokołu kryptograficznego zostały zdefiniowane, wówczas można przejść do ostatniej, czwartej fazy schematu postępowania, czyli obliczenie poziomu bezpieczeństwa dla wszystkich wersji rozpatrywanego protokołu. Poziom bezpieczeństwa jest obliczany według formuły (3.10) (rozdział 3.5). Formuła ta jest funkcją trzech czynników (parametrów): poziomu zabezpieczeń ($L^Z$) (rozdział 3.2), prawdopodobieństwa zajścia incydentu ($P$) (rozdział 3.3) oraz wpływu udanego ataku na system ($\omega$) (rozdział 3.4). W celu obliczenia poziomu bezpieczeństwa dla danej wersji protokołu, należy obliczyć czynniki wchodzące w skład formuły (3.10), które to następnie posłużą do obliczenia końcowej wartości poziomu bezpieczeństwa.

W bieżącym rozdziale przedstawiono obliczone poziomy bezpieczeństwa dla wszystkich wyodrębnionych wersji rozpatrywanego protokołu SSL Handshake Protocol. Jak wspomniano wyżej, przed obliczeniem poziomu bezpieczeństwa należy obliczyć czynniki wchodzące w skład formuły (3.10). Obliczenia wykonywane są indywidualnie dla wszystkich kroków wchodzących w skład protokołu SSL Handshake Protocol oraz dla wszystkich usług bezpieczeństwa wymaganych w poszczególnych krokach.

W rozpatrywanym przypadku zdefiniowano dwa rozróżnienia protokołu SSL Handshake Protocol. Pierwsze dotyczy użytych mechanizmów bezpieczeństwa. Zdefiniowano wersję pierwszą (tab. 3.8), która zakłada użycie podstawowych mechanizmów bezpieczeństwa oraz wersję drugą (tab. 3.9), która zakłada użycie bardziej zaawansowanych mechanizmów bezpieczeństwa. Druga modyfikacja polega na wprowadzeniu różnego wpływu udanego ataku na system dla rozpatrywanego protokołu SSL Handshake Protocol. W tym celu utworzono wersję A, która zakłada, że wpływ udanego ataku na system jest wysoki oraz wersję B, która zakłada, że wpływ udanego ataku na system jest znacznie mniejszy niż w wersji A (tab. 3.10).

W tab. 3.11 i 3.12 przedstawiono, otrzymane wartości wspomnianych czynników wchodzących w skład formuły (3.10) oraz końcową wartość obliczonego poziomu bezpieczeństwa ($F_S$). Obliczenia zostały wykonane dla wszystkich zdefiniowanych wersji protokołu SSL Handshake Protocol.

***Wersja 1***

Tab. 3.11 Obliczone wartości poziomu bezpieczeństwa dla wersji 1 protokołu SSL Handshake Protocol wraz z trzema czynnikami wchodzącymi w skład formuły (3.10), czyli poziomu zabezpieczeń ($L^Z$), prawdopodobieństwa zajścia

`

incydentu ($P$) oraz wpływu udanego ataku na system ($\omega$).

| | **wersja A** | | | **wersja B** | | |
|---|---|---|---|---|---|---|
| | $P$ | $\omega$ | $L^Z$ | $P$ | $\omega$ | $L^Z$ |
| *Krok 1* | | | | | | |
| **I** | 0,673 | 0,426667 | 0,6 | 0,673 | 0,12 | 0,6 |
| *Krok 2* | | | | | | |
| **I** | 0,673 | 0,533333 | 0,6 | 0,673 | 0,146667 | 0,6 |
| *Krok 3* | | | | | | |
| **I** | 0,673 | 0,4 | 0,6 | 0,673 | 0,12 | 0,6 |
| **C** | 0,64 | 0,666667 | 0,6 | 0,64 | 0,186667 | 0,6 |
| **Au** | 0,67 | 0,32 | 0,5 | 0,67 | 0,106667 | 0,5 |
| *Krok 4* | | | | | | |
| **I** | 0,673 | 0,426667 | 0,6 | 0,673 | 0,133333 | 0,6 |
| **C** | 0,6865 | 0,586667 | 0,6 | 0,6865 | 0,133333 | 0,6 |
| $\mathbf{F_S}$ | 0,095015 | | | 0,157667 | | |

***Wersja 2***

Tab. 3.12 Obliczone wartości poziomu bezpieczeństwa dla wersji 2 protokołu SSL Handshake Protocol wraz z trzema czynnikami wchodzącymi w skład formuły (3.10), czyli poziomu zabezpieczeń ($L^Z$), prawdopodobieństwa zajścia incydentu ($P$) oraz wpływu udanego ataku na system ($\omega$).

| | **wersja A** | | | **wersja B** | | |
|---|---|---|---|---|---|---|
| | $P$ | $\omega$ | $L^Z$ | $P$ | $\omega$ | $L^Z$ |
| *Krok 1* | | | | | | |
| **I** | 0,648475 | 0,426667 | 0,7 | 0,648475 | 0,12 | 0,7 |
| *Krok 2* | | | | | | |
| **I** | 0,648475 | 0,533333 | 0,7 | 0,648475 | 0,146667 | 0,7 |
| *Krok 3* | | | | | | |
| **I** | 0,614175 | 0,4 | 0,8 | 0,614175 | 0,12 | 0,8 |
| **C** | 0,583975 | 0,666667 | 0,7 | 0,583975 | 0,186667 | 0,7 |
| **Au** | 0,614175 | 0,32 | 0,75 | 0,614175 | 0,106667 | 0,75 |
| *Krok 4* | | | | | | |
| **I** | 0,648475 | 0,426667 | 0,7 | 0,648475 | 0,133333 | 0,7 |
| **C** | 0,564625 | 0,586667 | 1 | 0,564625 | 0,133333 | 1 |
| $\mathbf{F_S}$ | 0,150855 | | | 0,254869 | | |

Analizę otrzymanych wyników dla rozpatrywanego przypadku protokołu SSL Handshake Protocol rozpoczniemy od uzyskanych wartości prawdopodobieństwa zajścia incydentu ($P$). Jest sprawą oczywistą, że w obrębie

poszczególnej rozpatrywanej wersji protokołu, np. wersji 1 (tab. 3.11), wartości parametru *P* dla wersji A i B oraz dla odpowiednich kroków a w ich obrębie konkretnych usług bezpieczeństwa są identyczne. Jest to spowodowane tym, że naszym założeniem jest to, że wersje A i B różnią się jedynie wpływem udanego ataku na system ($\omega$ ).

Przeprowadzając dalszą analizę widać, że dla poszczególnych wersji rozpatrywanego protokołu np. wersji 1 otrzymane wartości prawdopodobieństwa zajścia incydentu (*P*) dla wszystkich kroków oraz założonych w nich usług bezpieczeństwa, przyjmują przybliżoną wartość. Jest to spowodowane tym, że w każdym kroku rozpatrywanego protokołu używane są podobne, podstawowe mechanizmy bezpieczeństwa (tab. 3.8), które wykorzystują podobne moduły kryptograficzne. Wraz z każdorazowym wykorzystywaniem modułów kryptograficznych system musi spełnić odpowiednie wymogi [33], a w rozpatrywanym przypadku przyjęto (rozdział 3.7.2), że właśnie użycie modułów kryptograficznych ma największy wkład do prawdopodobieństwa zajścia zagrożenia.

W obydwu wersjach (wersja 1 i 2) rozpatrywanego protokołu, prawdopodobieństwo zajścia incydentu (*P*) dla poszczególnych kroków protokołu przyjmuje średnie wartości. Jest to w dużym stopniu spowodowane faktem, że w rozpatrywanym przypadku zdolność atakującego pod względem wiedzy jak i poniesionych kosztów jest również na średnim poziomie i wynosi odpowiednio $\omega_{LK}$ = 0,6 i $\omega_{LP}$ = 0,5. Porównując uzyskane wartości dla dwóch wersji protokołu widać, że wraz ze zwiększeniem zastosowanych mechanizmów bezpieczeństwa (wersja 2) wartość prawdopodobieństwa zajścia incydentu zmienia się nieznacznie. Jest to spowodowane tym, że dodatkowe mechanizmy bezpieczeństwa oprócz wprowadzenia nowych zabezpieczeń stanowią nowe zagrożenie dla systemu.

Kolejnym parametrem, który zostanie rozważony, jest parametr charakteryzujący wpływ udanego ataku na system ($\omega$ ). Analizując otrzymane wyniki dla wersji 1 (tab. 3.11) omawianego protokołu, widać, że wraz ze zmniejszeniem parametrów określających wpływ udanego ataku na system, czyli parametrów *F* i $\alpha$ (wersja B) ostateczna wartość parametru określającego wpływ udanego ataku na system ($\omega$ ) przyjmuje mniejsze wartości. Taką samą tendencję odzwierciedla wersja 2 (tab. 3.12) rozpatrywanego protokołu.

Ostatnim obliczanym parametrem jest poziom zabezpieczeń ($L^Z$). Wartość tego parametru jest uzależniona od wybrany mechanizmów bezpieczeństwa (tab. 3.8, 3.9). Podobnie jak w przypadku parametru określającego prawdopodobieństwo zajścia incydentu (*P*) jest sprawą oczywistą, że w obrębie poszczególnej rozpatrywanej wersji protokołu, np. wersji 1 (tab. 3.11) jego wartość dla wersji A i B oraz dla odpowiednich kroków a w ich obrębie konkretnych usług bezpieczeństwa jest identyczna. Jest to spowodowany tym, że naszym założeniem jest to, że wersje A i B różnią się jedynie wpływem

`

udanego ataku na system ($\omega$ ).

Istotą prezentowanego w tej pracy modelu skalowalności jest określenie poziomu bezpieczeństwa ($F_S$) dla poszczególnych wersji protokołu. Analizując wersję 1 rozpatrywanego protokołu widać, że wraz ze zmniejszeniem wpływu udanego ataku na system uzyskiwany poziom bezpieczeństwa realizowanego procesu elektronicznego rośnie. Dla wersji A przyjmuje on wartość $F_S$=0,095015 a dla wersji B przyjmuje wartość $F_S$=0,157667.

Podobne wyniki zostały uzyskane w przypadku, gdy w kolejnej wersji protokołu zostały użyte dodatkowe mechanizmy bezpieczeństwa (wersja 2). W tym przypadku również wraz ze zmniejszeniem wpływu udanego ataku na system uzyskiwany poziom bezpieczeństwa realizowanego procesu elektronicznego rośnie. Dla wersji A przyjmuje on wartość $F_S$=0,150855, a dla wersji B przyjmuje wartość $F_S$=0,254869.

Istotnym spostrzeżeniem jest to, że zmieniając charakter realizowanego procesu elektronicznego, w rozpatrywanym przypadku było to związane ze zmniejszeniem kwoty przelewu dokonywanego za pośrednictwem aplikacji internetowej wykorzystującej protokół SSL v.3.00, można zrezygnować z niektórych użytych mechanizmy bezpieczeństwa, zachowując jednocześnie określony poziom bezpieczeństwa. Na potwierdzenie tego spostrzeżenia przedstawiono następujące rozumowanie. Analiza będzie dotyczyła tab. 3.12. Jeżeli w rozpatrywanym protokole zastosowano zwiększone mechanizmy bezpieczeństwa (wersja 2) i gdy wpływ udanego ataku na system jest duży (wersja A), wówczas uzyskany poziom bezpieczeństwa, który gwarantuje bezpieczne przeprowadzenie procesu jest równy $F_S$=0,150855. Warunkiem koniecznym, żeby inne wersje rozpatrywanego protokołu, spełniały założone wymogi bezpieczeństwa jest uzyskanie poziomu bezpieczeństwa, który jest większy lub równy od obliczonego, czyli $F_S \geq 0{,}150855$. Warto zwrócić uwagę na otrzymane poziomy bezpieczeństwa dla wersji 1 rozpatrywanego protokołu (tab. 3.11). Jeżeli dla danego protokołu zmniejszymy wpływ udanego ataku na system, czyli w rozpatrywanym przypadku wersja B, wówczas otrzymany poziom bezpieczeństwa będzie równy $F_S$=0,157667, czyli większy od obliczonego w wersji 2. Jak pokazano uzyskany poziom bezpieczeństwa jest większy, dlatego ta wersja podprotokołu spełnia założone wymogi bezpieczeństwa. Istotnym spostrzeżeniem jest to, że w spełniającej wymogi wersji 1 użyto mniej mechanizmów bezpieczeństwa niż w wersji 2. Dzięki zmniejszeniu nadmiarowych środków ochrony informacji można wprowadzić dodatkową optymalizacje procesu elektronicznego, która poprawia jego wydajność, dostępność a w rezultacie bezpieczeństwo.

# Rozdział 4

## Optymalizacja protokołu elektronicznego przetargu z wykorzystaniem mechanizmu skalowanego bezpieczeństwa

W bieżącym rozdziale przedstawiono optymalizację wydajności, dostępności, a w rezultacie - bezpieczeństwa nowego protokołu kryptograficznego realizującego elektroniczny przetarg. Do tego celu wykorzystano zaprezentowany w rozdziale 3 mechanizm skalowanego bezpieczeństwa.

Na początku rozdziału przedstawiono analizę wymagań, jakie musi spełniać elektroniczna wersja przetargu, oraz możliwości ich realizacji. Następnie zaprezentowano nowy protokół kryptograficzny realizujący elektroniczny przetarg [46] wraz z omówieniem jego cech charakterystycznych. Ostatecznym elementem zaprezentowanym w bieżącym rozdziale jest wykonanie wspomnianej optymalizacji dla tego protokołu. W protokole opisanym w pracy [46] oraz analizowanym w książce został znaleziony atak z człowiekiem pośrodku (ang. man in the middle), szczegóły tego ataku oraz jego korekta zostały przedstawione w pracy [97].

## 4.1. Założenia dla prezentowanej nowej wersji elektronicznego przetargu

Usługi realizowane przez instytucje administracji publicznej lub inne organizacje muszą spełniać szereg założeń, które gwarantują poprawność przeprowadzenia danego procesu. Elektroniczne formy tradycyjnych usług również muszą spełniać określone właściwości. Oprócz wymogów koniecznych można wprowadzać dodatkowe funkcjonalności, które są indywidualnym rozwiązaniem danego przypadku. W analizowanej nowej wersji elektronicznego przetargu [46] założono, że powinien on spełniać wymogi przedstawione poniżej (realizowane metodami kryptograficznymi).

**Niezaprzeczalność uczestników**

E-przetarg mogą ogłaszać jedynie upoważnione osoby. Oferty przetargowe mogą składać również tylko uprawnione osoby.

**Integralność danych**

Zarówno treść przesłanych ofert jak i końcowe wyniki e-przetargu nie mogą być zmienione.

**Niezaprzeczalność ofert**

Oferent, który wygrał e-przetarg nie może wyprzeć się treści swojej oferty oraz faktu jej złożenia.

**Poufność ofert**

Nikt nie może ustalić treści przesłanych ofert przed czasem zakończenia e-przetargu.

**Anonimowość wygrywającego oferenta**

Oferent, który wygrał przetarg nie jest publicznie ujawniony.

**Publiczna weryfikacja**

Każdy może sprawdzić, która oferta wygrała e-przetarg. Uczestnicy e-przetargu mogą sprawdzić czy ich oferty były wzięte pod uwagę.

**Wybór wielokryterialny**

Osoba ogłaszająca przetarg może przedstawić jego warunki w postaci zestawienia wielu czynników.

Wymienione usługi ochrony informacji są zrealizowane za pomocą różnych mechanizmów bezpieczeństwa. Przykładowe ich zestawienie zawarte jest w tab. 3.1.

## 4.2. Typy aukcji Internetowych

Do najpopularniejszych rozwiązań z dziedziny handlu elektronicznego zalicza się aukcje internetowe. Aukcja internetowa jest rozumiana jako proces licytacji danego towaru wystawionego na sprzedaż w serwisie aukcyjnym [24]. Rozróżniamy rożne typy aukcji internetowych, najpopularniejsze to: *klasyczna (ang. English), przetargowa (ang. 1-st Price Sealed-Bid), Vickrey* oraz *holenderska (ang. Dutch).*

Typ *aukcji klasycznej* jest najbardziej rozpowszechniony. Polega on na tym, że cena za dany towar jest licytowana i rośnie do czasu, kiedy pozostanie tylko jedna osoba biorąca udział w licytacji, podczas gdy inne się wycofają.

Typ *aukcji przetargowej* polega na tym, że każdy oferent niezależnie deklaruje swoją cenę za dany towar. Osoba, która zadeklaruje najwyższą sumę wygrywa towar i jest zobowiązana zapłacić cenę przedstawioną przez siebie.

Typ aukcji *Vickrey,* inaczej zwany 2-*nd Price Sealed-Bid,* jest podobny do poprzedniego modelu. Różnica polega na tym, że aukcję wygrywa osoba, która zadeklarowała najwyższa kwotę za dany towar, ale płaci cenę drugą najwyższą w kolejności.

Typ *aukcji holenderskiej* polega na tym, że licytacja prowadzona jest z najwyższej możliwej ceny, ale w odwrotnym kierunku, czyli każda licytowana oferta jest niższa od aktualnej. Taka aukcja zostanie zakończona, gdy dowolny oferent zatrzyma ją przy konkretnej wartości, co jest równoważne z wygraniem aukcji z ceną, przy której oferent zatrzymał licytację.

Każdy z wymienionych typów aukcji internetowej posiada swoją charakterystykę i w zależności od wymagań konkretnego przypadku dobierany jest jej odpowiedni typ. Dla przykładu najpopularniejszy polski serwis aukcyjny (www.allegro.pl), polega na podbijaniu ceny wyjściowej przez strony biorące udział w licytacji aż do momentu, gdy minie z góry ustalony czas. Oczywiście wygrywa strona, która zaoferowała najwyższą cenę. Taką charakterystykę posiada klasyczny typ aukcji.

Kolejnym przykładem aukcji internetowej jest elektroniczny przetarg. W tym przypadku nie ma tradycyjnej licytacji, a zainteresowani danym towarem składają swoją ofertę z ceną, jaką są w stanie zapłacić. Zwycięża ten, kto zaoferuje najwyższą cenę. W takim przypadku aukcja internetowa spełnia warunki typu aukcji przetargowej (http://www.e-przetarg.pl/).

Aukcje internetowe realizowane są na podstawie protokołów kryptograficznych, które opisują poszczególne kroki postępowania uczestników. Każdy typ aukcji internetowej może bazować na różnych protokołach kryptograficznych, które są dobierane w zależności od konkretnych wymagań formy elektronicznego przetargu.

`

## 4.3. Protokoły kryptograficzne realizujące aukcje przetargowe

W bieżącym rozdziale przedstawiono analizę literatury dotyczącej protokołów kryptograficznych realizujących aukcje przetargowe. Przeprowadzona analiza skoncentrowana jest na głównych cechach charakterystycznych protokołów kryptograficznych, realizujących aukcje przetargową. Dodatkowo odniesiono przedstawioną analizę do założeń nowej wersji e-przetargu (rozdział 4.1).

Na podstawie typu *aukcji przetargowej* powstało wiele protokołów kryptograficznych [5, 28, 29, 41, 43, 85, 90]. W przypadku elektronicznego przetargu warto zwrócić uwagę na niektóre cechy, charakteryzujące wspomniany typ aukcji.

**Wymagania komunikacyjne i obliczeniowe**

Wszelkie operacje opisane w ramach protokołu kryptograficznego wykonywane są w odrębnych fazach. Mogą one opierać się na krokach komunikacyjnych, czyli przesyłaniu informacji pomiędzy uczestnikami danego protokołu. Innym działaniem jest wykonywanie szeregu obliczeń, które potrzebują odpowiedniej mocy obliczeniowej. Zazwyczaj obydwie metody łączone są ze sobą, a istotną różnicą wśród protokołów kryptograficznych jest stosunek wykonanych obliczeń do liczby potrzebnych połączeń między uczestnikami.

Zdefiniowane założenia dla elektronicznego przetargu (rozdział 4.1) nie określają specjalnych wymagań komunikacyjnych i obliczeniowych, dlatego w rozpatrywanym przypadku stosunek tych metod nie jest czynnikiem szczególnej uwagi.

**Warunki przetargu**

Kolejnym istotnym elementem są możliwe do określenia warunki przetargu. W istniejących protokołach kryptograficznych [28, 85, 90], warunki mogą być określane jedynie na podstawie jednego kryterium wyboru, czyli np. poziomu ceny. Jest to duże ograniczenie realizacji potencjalnych elektronicznych przetargów, ponieważ w rzeczywistości organizowane są takie, których wybór nie ogranicza się jedynie do określenia ceny, lecz są wyborem wielokryterialnym. Dla przykładu można przedstawić przetarg, który ma na celu zakup komputerów. Przy takim przetargu, oprócz czynnika związanego z ceną, istotny może być również okres gwarancji na komputery lub czas dostarczenia sprzętu. W takiej sytuacji otrzymanie ofert określających wszystkie wspomniane czynniki pozwoli dokonać precyzyjniejszego wyboru.

Zdefiniowane założenia dla nowej wersji elektronicznego przetargu (rozdział 4.1) zakładają, że warunki przetargu mogą być sformułowane w postaci wielokryterialnych wymogów. Aktualnie istniejące protokoły kryptograficzne realizujące aukcje przetargowe nie pozwalają wprowadzić takiej funkcjonalności.

**Wymagania odnośnie uczestników przetargu**

W aukcjach przetargowych głównymi uczestnikami są aukcjoner lub aukcjonerzy oraz oferenci. Zadania aukcjonerów są różne w zależności od konkretnego protokołu, kontrolują oni wszystkie fazy protokołu. Oferenci

są uczestnikami, którzy licytują daną ofertę. Ważnym elementem jest umożliwienie wzięcia udziału oferentów w aukcji. W większości protokołów do tego aspektu nie przywiązuje się dużej wagi. Do tego celu stosowane są podstawowe metody autoryzacji, jakimi mogą być login i hasło [28, 85] czy przydzielane przez specjalne podprotokoły numery autoryzacyjne [90].

Założenia dla protokołu kryptograficznego realizującego elektroniczną formę przetargu (rozdział 4.1) zakładają, że w aukcji przetargowej mogą wziąć udział jedynie upoważnione osoby. Możliwość wzięcia udziału w elektronicznym przetargu jest regulowana przez prawo kraju, w którym odbywa się przetarg. W przypadku Polski są one bardzo wymagające i określone przez ustawę o zamówieniach publicznych [14]. Weryfikacja koniecznych wymogów, które potrzebne są do wzięcia udziału w przetargu, nie może być wykonana na podstawie podstawowych metod autoryzacji.

**Stosowane techniki ochrony informacji w stosunku do zagwarantowania poufności składanych ofert**

W aktualnych pracach uzyskanie żądanego poziomu poufności dla składanych ofert bazuje na dwóch technikach kryptograficznych. Pierwsza [28, 29, 41] opiera swój mechanizm na schemacie progowym. W tej metodzie potrzebujemy kilku aukcjonerów, do których oferenci przesyłają swoje części oferty. Główny aukcjoner łączy wszystkie części i wyznacza cenę końcową bez ujawniania wszystkim oferentom pojedynczych ofert. Niebezpieczeństwo tej techniki tkwi w ewentualnych konszachtach miedzy aukcjonerami, co w rzeczywistości może doprowadzić do wcześniejszego ujawnienia składowych cen lub nie ujawnienia ostatecznej oferty. Druga [5, 43] wyklucza możliwość konszachtów między aukcjonerami. Zostało to uzyskane dzięki zastosowaniu zaufanej "*trzeciej strony*". W tej metodzie zastrzeżenie może budzić wiarygodność samej "*trzeciej strony*".

W rozpatrywanym protokole kryptograficznym dla e-przetargu poufność składanych ofert jest gwarantowane za pomocą obydwu wspomnianych metod, czyli zarówno modelu progowego jak i zaufanej trzeciej strony (TTP). Zastosowanie jednocześnie dwóch metod pozwala zwiększyć poziom poufności składanych ofert.

Przedstawiona analiza charakteryzująca protokoły kryptograficzne realizujące aukcje przetargowe wskazuje na pewne niedostatki tych protokołów. Braki te dotyczą możliwego wyboru warunków przetargu oraz wymagań odnośnie uczestników biorących udział w przetargu. W pracy przedstawiono nowy protokół kryptograficzny realizujący elektroniczny przetarg [46], który będzie spełniał założenia przedstawione w rozdziale 4.1 oraz wyeliminuje wspomniane braki.

## 4.4. Model nowego protokołu kryptograficznego realizującego e-przetarg

Nowy protokół kryptograficzny realizujący elektroniczny przetargu [46] składa się z czterech podprotokołów: *certyfikacji, zgłoszenia przetargu,*

`

*zgłoszenia oferty oraz wyboru oferty*. W protokole bierze udział *n* oferentów *($O_1$, ..... ,$O_n$)*, zaufana trzecia strona, czyli *GAP* (Główna Agencja Przetargowa) oraz firma chcąca ogłosić przetarg *F*.

Pierwszym krokiem protokołu jest weryfikacja przez *GAP* uczestników biorących udział w e-przetargu, czyli oferentów $O_n$ oraz firmy *F* chcącej ogłosić przetarg (*podprotokół certyfikacji*). Kolejnym krokiem jest zgłoszenie do *GAP* przetargu przez zweryfikowaną firmę *F*. *GAP* publikuje warunki zgłoszonego przetargu, podając w nim wszelkie wymogi zgłoszone przez *F (podprotokół zgłoszenia przetargu)*. W następnym kroku osoba chcąca wziąć udział w przetargu, po wcześniejszej weryfikacji, przesyła swoją ofertę do *GAP (podprotokół zgłoszenia oferty)*. Ostatni podprotokół wykonywany jest po terminie zgłaszania ofert. Firma *F* oraz oferenci $O_n$, przesyłają wówczas do *GAP* swoje części sekretu potrzebne do odczytania ofert. Po odszyfrowaniu zostaną one przesłane do firmy *F*, gdzie zostanie wybrana zwycięska oferta. W tym samym podprotokole firma *F* wysyła informacje o wybranej ofercie do *GAP*, po czym zostaje ona podana do publicznej wiadomości *(podprotokół wyboru oferty)*.

Komunikacja pomiędzy uczestnikami protokołu jest bezpieczna. Uzyskujemy to dzięki zastosowaniu kryptografii z kluczem publicznym (każdy uczestnik protokołu posiada swój klucz prywatny (SK) oraz klucz publiczny (PK)). Stosowane klucze nie są stałe, ich ważność kończy się wraz z ważnością numeru rejestracyjnego, uzyskanego w podprotokole certyfikacji.

Oferty przesłane przez oferentów $O_n$, są szyfrowane kluczem publicznym danego przetargu. Odczytać je można posiadając klucz prywatny, który w podprotokole zgłoszenia przetargu zostaje podzielony na części za pomocą odpowiedniego progowego bezpiecznego schematu podziału sekretu. W protokole użyto również generatora liczb pseudolosowych (PRNG) [39, 6]. Stosuje się go do tworzenie numerów identyfikacyjnych uczestników przetargu jak i numerów samych przetargów.

Przetarg kończy się po ustalonym terminie. Do określenia tej chwili służą znaczniki czasu (*T*).

### 4.4.1. Podprotokół certyfikacji

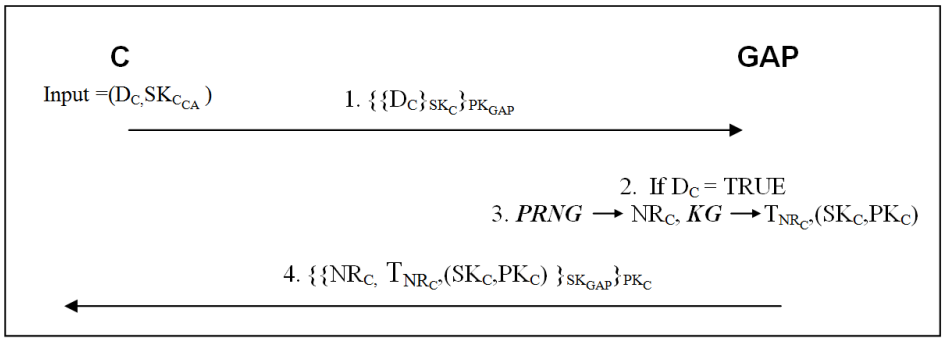
Możliwość wzięcia udziału w e-przetargu musi być poprzedzona uzyskaniem odpowiednich uprawnień.

Osoba ubiegająca się o certyfikat, czyli firma, która chce ogłosić przetarg lub oferent powinna posiadać stosowne dokumenty $D_C$ oraz klucz prywatny $SK_{C_{CA}}$ uzyskany w jednej z wcześniej wskazanych centrów autoryzacji (CA). Osoba ubiegająca się o certyfikat podpisuje cyfrowo wspomniane dokumenty

za pomocą $SK_{C_{CA}}$, później szyfruje za pomocą klucza publicznego $PK_{GAP}$, a następnie przesyła do *GAP*[2].

*GAP* odszyfrowuje dokumenty, które następnie weryfikuje. Po pozytywnej weryfikacji generuje za pomocą generatora liczb pseudolosowych (PRNG) unikalny numer rejestracyjny dla danej osoby $NR_C$. Numer rejestracyjny jest ważny przez określony czas, w tym celu generowany jest znacznik czasu numeru rejestracyjnego $T_{NR_C}$. *GAP* generuje również (KG) klucze prywatny ($SK_C$) i publiczny ($PK_C$) dla danego podmiotu, które będą używane w kolejnych podprotokołach. Ważność tych kluczy kończy się wraz z przekroczeniem czasu wskazywanego przez $T_{NR_C}$. Wygenerowane dane podpisuje się cyfrowo, szyfruje się za pomocą klucza publicznego *C* a następnie przesyła do *C*.

Graf przedstawiający w sposób schematyczny kroki podprotokołu certyfikacji przedstawiony jest na rys. 4.1.




Rys. 4.1 Graf podprotokołu certyfikacji.

### 4.4.2. Podprotokół zgłoszenia przetargu

Przetarg może być zgłoszony przez dowolną osobę, która wcześniej w podprotokole certyfikacji uzyskała odpowiednie uprawnienia. Taka osoba, oznaczona jako *F*, powinna posiadać numer rejestracyjny $NR_F$, jego znacznik czasu $T_{NR_F}$ , klucz prywatny $SK_F$ oraz warunki zgłaszanego przetargu $WP_F$. Następnie *F* generuje za pomocą generatora liczb pseudolosowych (PRNG) swój indywidualny numer $N_F$.

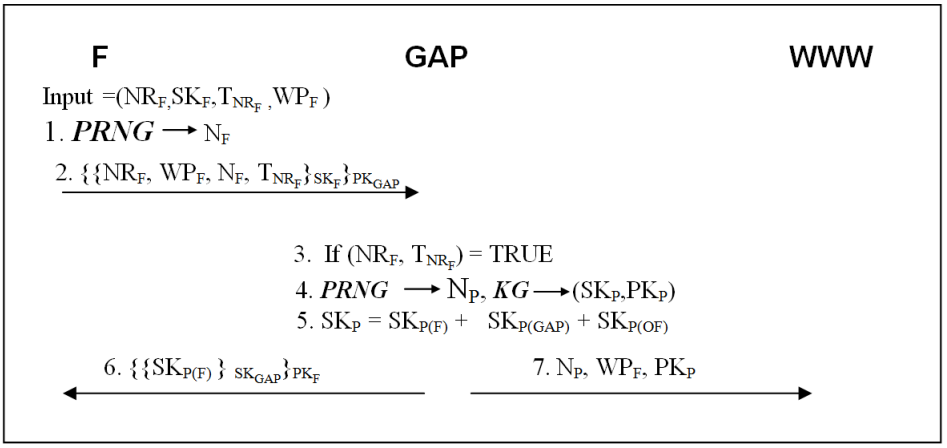
W pierwszym kroku *F* przesyła do *GAP* podpisane cyfrowo ($SK_F$) oraz zaszyfrowane ($PK_{GAP}$) następujące informacje: swój numer rejestracyjny ($NR_F$), jego znacznik czasu ($T_{NR_F}$), warunki przetargu ($WP_F$) oraz swój indywidualny

[2] Szyfrowaniu danych kluczem publicznym rozumiane jest jako szyfrowanie klucza sesyjnego, podczas gdy dane szyfrowane są szyfrem symetrycznym (schematu hybrydowy) [99]. Takie rozumowanie będzie kontynuowane w dalszej części pracy.

`

numer ($N_F$).

Główna agencja przetargowa (GAP) weryfikuje numeru rejestracyjny *F* ($NR_F$) oraz ważność jego znacznika czasu. Po pozytywnej autoryzacji GAP generuje (PNRG) indywidualny numer przetargu ($N_P$) oraz parę kluczy (KG) dla konkretnego przetargu ($SK_P$, $PK_P$). Prywatny klucz przetargu ($SK_P$) jest dzielony za pomocą progowego schematu podziału sekretu. Sekret jest podzielony na trzy części przeznaczone dla: *F* ($SK_{P(F)}$), dla *GAP* ($SK_{P(GAP)}$) oraz oferentów w przetargu ($SK_{P(OF)}$). Każda z części jest potrzebna do odtworzenia klucza prywatnego ($SK_P$). *GAP* wysyła podpisaną cyfrowo ($SK_{GAP}$) oraz zaszyfrowaną ($PK_F$) część sekretu przeznaczoną dla *F* ($SK_{P(F)}$).




Rys 5.2 Graf podprotokołu zgłoszenia przetargu.

*GAP* podaje do wiadomości publicznej, np. na stronie *WWW*, numer przetargu ($N_P$), jego warunki ($WP_F$) oraz jego klucz publiczny ($PK_P$).

Graf przedstawiający w sposób schematyczny kroki podprotokołu zgłoszenia przetargu przedstawiony jest na rys. 4.2.

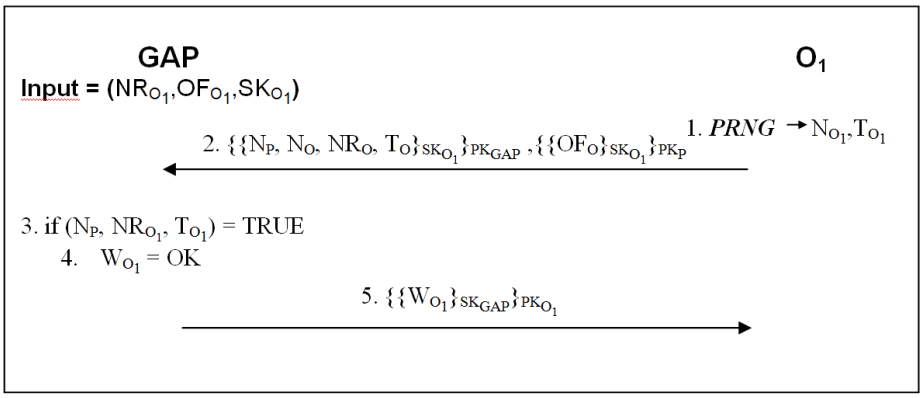
### 4.4.3. Podprotokół zgłoszenia oferty

Gdy przetarg zostanie zgłoszony i opublikowany zainteresowane strony mogą zgłaszać swoje oferty. Oferent chcąc wziąć udział w przetargu powinien posiadać wcześniej uzyskany numer rejestracyjny ($NR_{O_1}$), klucz prywatny ($SK_{O_1}$) oraz swoją ofertę ($OF_{O_1}$). Następnie oferent $O_1$ generuje (PRNG) swój numer indywidualny ($N_{O_1}$) oraz znaczy swoją ofertę znacznikiem czasu ($T_{O_1}$). Kolejny krok polega na przesłaniu do *GAP* podpisanych cyfrowo ($SK_{O_1}$) oraz zaszyfrowanych ($PK_{GAP}$) następujących informacji: $N_P$, $N_O$, $NR_O$, $T_O$.

Oferta ($OF_{O_1}$) jest również podpisywana cyfrowo ($SK_{O_1}$), ale szyfrowana jest za pomocą klucza publicznego danego przetargu ($PK_P$), później jest przesyłana do *GAP*. Jeżeli przesłane dane są poprawne, to wówczas *GAP* przesyła do $O_1$ potwierdzenie zgłoszenia oferty ($W_{O_1}$). Potwierdzenie jest podpisane cyfrowo

przez *GAP* ($SK_{GAP}$) oraz zaszyfrowane ($PK_{O_1}$).

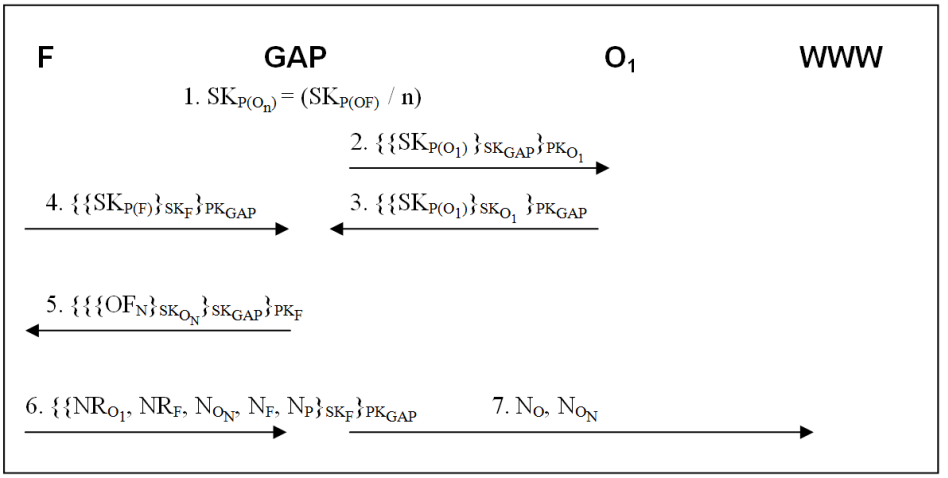
Graf przedstawiający w sposób schematyczny kroki podprotokołu zgłoszenia oferty przedstawiony jest na rys. 4.3.




Rys. 4.3 Graf podprotokołu zgłoszenia oferty.

### 4.4.4. Podprotokół wyboru oferty

Ostatni podprotokół wykonywany jest po upływie czasu przeznaczonego na składanie ofert. Czas ten opublikowany jest wraz z innymi warunkami przetargu ($WP_F$).




Rys. 4.4 Graf podprotokołu wyboru oferty.

*GAP*, znając liczbę oferentów, którzy przesłali swoje oferty (n), dzieli wcześniej podzieloną część głównego sekretu przetargu ($SK_{P(OF)}$) na *n* mniejszych części. Stosuje do tego bezpieczny system progowy podziału sekretu o charakterystyce (2,*n*). Utworzone części podpisuje cyfrowo ($SK_{O_1}$),

szyfruje ($PK_{O_1}$) i przesyła do wszystkich oferentów $O_n$.

W następnym kroku firma *F* oraz oferenci $O_n$ przesyłają podpisane cyfrowo oraz zaszyfrowane swoje części sekretu do *GAP*, gdzie zostaną one złożone w główny sekret przetargu ($SK_P$). *GAP* mając cały sekret danego przetargu może odszyfrować wszystkie nadesłane oferty ($OF_N$). Po tej czynności przesyła wszystkie oferty podpisane cyfrowo przez oferentów do firmy *F* ogłaszającej przetarg. Wszystkie oferty są wcześniej podpisane cyfrowo ($SK_{GAP}$) oraz zaszyfrowane ($PK_F$).

Firma *F* po otrzymaniu ofert wybiera najlepszą i wyniki przesyła do *GAP* w celu ogłoszenia zwycięzcy. Informacje przesłane to: numer rejestracyjny oferenta, który wygrał przetarg ($NR_{O_1}$), numer rejestracyjny firmy ($NR_F$), numery indywidualne wszystkich oferentów, których oferty były wzięte pod uwagę ($N_{O_N}$), swój numer indywidualny ($N_F$) oraz numer przetargu ($NI_P$). Wymienione informacje są podpisane cyfrowo ($SK_F$) oraz zaszyfrowane ($PK_{GAP}$).

*GAP* po otrzymaniu informacji publikuje numer indywidualny ($N_{O_1}$) oferenta, którego oferta została wybrana. Do wiadomości publicznej podawane są również wszystkie numery indywidualne oferentów, których oferty były rozpatrywane ($N_{O_N}$).

Graf przedstawiający w sposób schematyczny kroki podprotokołu wyboru oferty przedstawiony jest na rys. 4.4.

## 4.5. Analiza realizacji założeń dla nowego protokołu e-przetargu

W bieżącym rozdziale omówiono realizacje założeń dla nowego protokołu kryptograficznego e-przetargu (rozdział 4.1).

**Niezaprzeczalność uczestników**

Podprotokół certyfikacji jest odpowiedzialny za główną weryfikacje uczestników. *GAP* jako zaufana trzecia strona sprawdza wymagane dokumenty i przydziela prawo zgłaszania własnego przetargu lub prawo wzięcia udziału w przetargu. Przydzielany indywidualny numer rejestracyjny jest konieczny, żeby wziąć udział w pozostałych podprotokołach. Do tego celu wykorzystano podpis cyfrowy, szyfrowanie danych, generator liczb pseudolosowych.

**Integralność danych**

Oferty przesłane przez oferentów są podpisywane cyfrowo za pomocą kluczy prywatnych otrzymanych przez każdego oferenta po pozytywnej weryfikacji w podprotokole certyfikacji. Wyniki przetargu również są podpisywane cyfrowo przez firmę, która ogłosiła przetarg. Ona również posiada klucz prywatny uzyskany w podprotokole certyfikacji. Do tego celu wykorzystano podpis cyfrowy, szyfrowanie danych, generator liczb pseudolosowych.

**Niezaprzeczalność ofert**

Oferent nie może wyprzeć się treści złożonej oferty, ponieważ zanim zostanie ona zaszyfrowana za pomocą klucza publicznego przetargu musi być przez niego cyfrowo podpisana. Fakt złożenia oferty przez oferenta jest

odnotowywany przez *GAP*, która każdą poprawną ofertę archiwizuje. Do tego celu wykorzystano podpis cyfrowy, szyfrowanie danych, generator liczb pseudolosowych, znakowanie czasem, bezpieczne przechowywania danych.

**Poufność ofert**

Oferty przesyłane przez oferentów są zaszyfrowane za pomocą klucza publicznego przetargu. Klucz prywatny przetargu jest podzielony przy użyciu bezpiecznego schematu progowego na trzy części, z których każda jest potrzebna do powtórnego złożenia całego sekretu. Jedna część pozostaje w *GAP*, druga jest przesyłana do firmy *F* ogłaszającej przetarg, a trzecia jest przeznaczona dla oferentów biorących udział w przetargu. Wspomniana trzecia część jest w podprotokole wyboru oferty dzielona według schematu (2,*n*), czyli sekret dzielimy na *n* części, ale tylko dwie są potrzebne do powtórnego złożenia sekretu. Wybrano schemat (2,*n*), ponieważ żeby przetarg był ważny potrzebujemy minimum dwóch ofert. Do tego celu wykorzystano podpis cyfrowy, szyfrowanie danych, generator liczb pseudolosowych, bezpieczny schematu podziału sekretu.

**Anonimowość wygrywającego oferenta**

Po wybraniu wygranej oferty do publicznej wiadomości podawany jest jedynie indywidualny numer danego oferenta. Ten numer jest znany tylko przez właściciela danego numeru. Do tego celu wykorzystano indywidualne numery rejestracyjne.

**Publiczna weryfikacja**

Po rozstrzygnięciu przetargu do publicznej wiadomości są podawane wszystkie numery indywidualne oferentów a wyróżnieniem numeru, który wygrał przetarg. Każdy uczestnik może sprawdzić czy jego numer znajduje się na liście co jest równoważne z faktem wzięcia pod uwagę jego oferty. Do tego celu wykorzystano indywidualne numery rejestracyjne.

**Wybór wielokryterialny**

Warunki przetargu przesyłane są do *GAP* w postaci niezależnego dokumentu. Dokument ten nie zakłada z góry ustalonych możliwości wyboru warunków przetargu, tylko w całości jest określany przez stronę zgłaszającą przetarg. Dzięki takiemu rozwiązaniu warunki ogłaszanego przetargu mogą przyjąć dowolną formę, czyli również postać wielokryterialnych wymogów. Do tego celu wykorzystano niezależne dokumenty zawierając warunki przetargu.

W bieżącym rozdziale przedstawiono nowy protokół kryptograficzny realizujący elektroniczny przetarg [46], który spełnia założenia przedstawione w rozdziale 4.1. Dodatkowe funkcjonalności, które wniósł opisany protokół dotyczą zwiększenia możliwości wyboru warunków przetargu oraz zwiększenia metod weryfikacji uczestników biorących udział w przetargu.

## 4.6. Centrum certyfikacji – element krytyczny infrastruktury systemu dla nowej wersji e-przetargu

Użyte w nowej wersji e-przetargu usługi bezpieczeństwa uzależnione

`

są w dużej mierze od Centrum Certyfikacji, pełniącego rolę zaufanej trzeciej strony (TTP), która oferuje usługi kompletne, ujednolicające poziom bezpieczeństwa. W opisywanym przypadku rolę pełni *GAP*, która przydziela numery certyfikujące (CA), tworzy znaczniki czasu (TSA), dzieli i następnie odtwarza sekret za pomocą wybranego schematu podziału sekretu oraz może pełnić inne funkcje, w których zaufanie jest kluczowym elementem. Analizując funkcje, jakie pełni zaufana trzecia strona można stwierdzić, że jest to element krytyczny całej infrastruktury systemu [47].

Bezpieczeństwo zaufanej trzeciej strony (TTP) można uzyskać stosując się do norm, które określają warunki jakie powinien spełniać dany system. W opisywanym przypadku TTP pełni potrójną rolę, czyli rolę centrum autoryzacji(CA), centrum znakowania czasem (TSA) oraz dzieli dowolny sekret bezpiecznym schematem podziału sekretu. Specyfikacje dotycząca CA oraz TSA przedstawione przez Europejski Instytut do Spraw Standardów Telekomunikacyjnych ETSI [16, 17] są merytorycznie zbliżone. Zawarte tam wymogi można podzielić na trzy główne zagadnienia: z*arządzanie kluczami, zarządzanie certyfikatami, zarządzanie samym urzędem.*

Zarządzania kluczami dotyczy zagadnień związanych z generowaniem kluczy, przechowywaniem kluczy oraz ich kopii, rozpowszechnianiem kluczy publicznych, użyciem kluczy, zakończeniem „cyklu życia" kluczy oraz sprzętowych urządzeń kryptograficznych.

Zarządzanie certyfikatami opisuje rejestracje podmiotów, generowanie certyfikatów, uaktualnienie certyfikatów, rozgłaszanie certyfikatów oraz zawieszenie i odwoływanie certyfikatów.

Zarządzanie urzędem obejmuje zagadnienia zarządzania bezpieczeństwem, ochrony zasobów urzędu, zabezpieczeń fizycznych oraz bezpieczeństwa całej infrastruktury, bezpieczeństwa personelu, zarządzania dostępem do systemów, wyboru wiarygodnych systemów i aplikacji, wymogów awaryjnych na wypadek nadużyć i ataków zewnętrznych, archiwizacji danych dotyczących certyfikatów oraz czynności związane z zakończeniem działania urzędu.

Bezpieczne schematy podziału sekretu nie są jeszcze znormalizowane. Istnieją natomiast algorytmy o podwyższonym bezpieczeństwie [53], za pomocą których możemy zrealizować wspomnianą operację.

### 4.6.1. Zagadnienia kryptograficzne

W przedstawionym przypadku e-przetargu kluczową rolę pełnią moduły kryptograficzne. Wybór konkretnych algorytmów kryptograficznych oraz szczegółów związanych z ich zastosowaniem należy uzależnić od poziomu bezpieczeństwa, jaki ma być zachowany w danym e-urzędzie. Takie założenia ustalamy podczas pierwotnej fazy tworzenia bezpiecznej infrastruktury, czyli projektując konkretną politykę bezpieczeństwa. Poziomy bezpieczeństwa modułów kryptograficznych opracowane przez organizację ISO/IEC [33] zostały podzielone na różne grupy.

W przypadku elektronicznego przetargu możemy mówić o najwyższym

poziomie ochrony. Szczególną uwagę należy zwrócić na zaufaną trzecią stronę, czyli Główną Agencje Przetargową. Wspomniany element jest krytyczny dla całej infrastruktury, dlatego powinien spełniać najwyższy poziom bezpieczeństwa.

Zagadnienia zawarte w normach ISO/IEC [33] są bardzo obszerne. W przypadku tworzonego protokołu kryptograficznego dla e-przetargu skupiono się na kilku głównych: specyfikacja modułów kryptograficznych, porty i interfejsy modułów kryptograficznych, model dopuszczalnych stanów, zarządzanie kluczami kryptograficznymi i wewnętrzny audyt.

### 4.6.2. Specyfikacja modułów kryptograficznych

W elektronicznym przetargu użyto wielu mechanizmów kryptograficznych. Chcąc zachować odpowiedni poziom bezpieczeństwa należy stosować potwierdzone algorytmy kryptograficzne.

Bezpieczna komunikacja między stronami uczestniczącymi w elektronicznym przetargu, w tym głównie z *GAP*, odbywa się za pomocą schematów hybrydowych. Do tego rodzaju szyfrowania używamy dwóch rodzajów operacji. Pierwszym jest mechanizm kopertowania (enkapsulacji) klucza (KEM) polegający na bezpiecznym przekazaniu klucza sesyjnego, a drugim mechanizm kopertowania danych (DEM), czyli przesłania danych zaszyfrowanych z wykorzystaniem przekazanego wcześniej klucza sesyjnego.

Pierwsza operacja wykonywana jest za pomocą szyfrów asymetrycznych [36] przy użyciu różnych modeli [81]. Do tego rodzaju szyfrowania możemy zastosować szyfry RSA [73], ElGamala [15] oraz innych zbudowanych na ich podstawie.

W drugiej operacji do szyfrowania danych używamy szyfrów symetrycznych [37]. W tej grupie szyfrów znajdują się szyfry o dwóch długościach kluczy: 64 i 128-bitowe. Z grupy szyfrów z kluczem 64-bitowym możemy wybrać np. szyfry DES [19] i IDEA [54], natomiast z 128-bitowym np. AES [21] lub Camellia [3].

Zaufana trzecia strona przesyłając dokumenty do innych uczestników przetargu wcześniej je podpisuje. Do tego celu możemy użyć np. wspominanego algorytmu RSA w trybie podpisu lub DSA [38].

Schematy podziału sekretu można zrealizować na podstawie modelu Shamira [80]. W przypadku elektronicznego przetargu możemy użyć automatycznego schematu podziału sekretu [53].

### 4.6.3. Porty i interfejsy modułów kryptograficznych

Informacje przekazywane między uczestnikami e-przetargu początkowo są szyfrowane, a następnie poprzez fizyczne porty oraz logiczne interfejsy kierowane są do miejsca przeznaczenia. Porty oraz interfejsy, do których kierowane są informacje powinny być jasno określone, zarówno dla danych wchodzących jak i wychodzących. Ponadto, zgodnie z najwyższym poziomem bezpieczeństwa, musimy stworzyć dwa niezależne połączenia fizyczne oraz

logiczne, którymi przesyłane będą dane. W jednym kanale będą przesyłane wszelkie informacje jawne, natomiast w drugim wyłączenie dane zaszyfrowane.

### 4.6.4. Model dopuszczalnych stanów

Operacje wykonywane przy użyciu modułów kryptograficznych powinny być opisane za pomocą szczegółowego, kompletnego modelu zawierającego wszystkie przewidywane stany w jakich może znaleźć się TTP. Model powinien zawierać następujące elementy:

- wszelkie możliwe stany, poprawne jak i błędne, modułów kryptograficznych;
- opis transakcji pomiędzy poszczególnymi stanami;
- możliwe stany danych wejściowych, które powodują transakcje pomiędzy stanami;
- możliwe stany danych wyjściowych, które zostały spowodowane wcześniejszymi transakcjami.

W przypadku e-przetargu główne stany uczestników przetargu zostały opisane we wspominanym protokole kryptograficznym. Stany pośrednie określa się podczas konkretnej implementacji, gdyż zależą one od indywidualnych wyborów algorytmów i rozwiązań technicznych.

### 4.6.5. Zarządzanie kluczami kryptograficznymi

Proces zarządzania kluczami kryptograficznymi jest cyklem (obejmującym czas życia klucza) składającym się z elementów, które zostały wyszczególnione podczas opisywania poziomów bezpieczeństwa.

**Generator liczb pseudolosowych** używany jest do generowania ciągów pseudolosowych, które wykorzystywane są w innych modułach kryptograficznych. W opisywanym przypadku warto zastosować potwierdzone generatory, spełniające odpowiednie normy [39]. Takim generatorem jest np. BBS (ang. Blum-Blum-Shub) [6], dla którego udowodniono mocną pseudolosowość generowanych przez niego ciągów [60]. Dane wychodzące z generatora liczb pseudolosowych powinny być weryfikowane za pomocą testu ciągłości, którego opis zostanie przedstawiony w dalszej części pracy.

**Generator kluczy** jest zazwyczaj integralnym elementem modułów kryptograficznych. Do ich generowania używamy wcześniej wspomnianych generatorów liczb pseudolosowych, również w tym elemencie powinniśmy wybrać ich zaufane wersje. Dla algorytmów asymetrycznych generator taki musi być wyposażony dodatkowo w test pierwszości liczb [60].

**Ustanowienie kluczy** może być wykonane za pomocą metod automatycznych, manualnych lub przy wykorzystaniu obu metod. W przypadku elektronicznego przetargu istotnym elementem jest ograniczenie wykonywanych operacji, dlatego zaleca się wykorzystanie jedynie metod automatycznych. Metody kryptograficzne realizujące założenia opierają się głównie na wykorzystaniu

asymetrycznych mechanizmów. Szczegóły opisane są przez odpowiednie normy [34].

**Wejście/wyjście kluczy.** Klucze kryptograficzne są zarówno wprowadzane jak i wyprowadzane z modułów kryptograficznych. Klucze prywatne oraz publiczne przekazywane automatycznie, wcześniej są szyfrowane przy użyciu sprawdzonych algorytmów. Dla zwiększenia bezpieczeństwa proces transportu kluczy może zostać poprzedzony dodatkową autoryzacją za pomocą metod manualnych (np. smard cards/tokens).

**Przechowywanie kluczy**. Kryptograficzne klucze używane przez moduły kryptograficzne powinny być przechowywane również w innym bezpiecznym miejscu. W przypadku e-przetargu powinniśmy zadbać o wysoki stopień bezpieczeństwa, dlatego klucze nie powinny być przechowywane jako tekst jawny, a jedynie w formie zaszyfrowanej. Do przechowywanych kluczy nie może mieć dostępu nikt oprócz upoważnionych osób.

**Anulowanie kluczy.** Moduły kryptograficzne, powinny posiadać możliwość wymazywania wszystkich używanych przez siebie kluczy; wszystkie dane dotyczące generowania kluczy, jak i same klucze powinny być kasowane w chwili, gdy nie są już potrzebne.

### 4.6.6. Wewnętrzny audyt

Moduły kryptograficzne powinny być weryfikowane za pomocą testów, których pozytywne przeprowadzenie potwierdza zachowanie odpowiedniego poziomu bezpieczeństwa. Normy zalecają używania dwóch rodzajów testów [33].

Pierwszy test - test inicjalizujący jest przeprowadzany po uruchomieniu całego systemu. Sprawdza on integralność systemu oraz jego poprawne funkcjonowanie.

Drugi rodzaj testu - test warunkowy jest przeprowadzany gdy moduły kryptograficzne wykonują pewne określone czynności, np. generują klucze kryptograficzne.

**Test inicjalizujący**

Dla e-przetargu test inicjalizujący powinien zawierać testy a*lgorytmów kryptograficznych, integracji oprogramowania* oraz *krytycznych funkcji.*

Test *algorytmów kryptograficznych* przeprowadzany jest za pomocą metody *znanej odpowiedzi,* czyli na wejście algorytmu przekazujemy dane, które po przejściu przez algorytm dają pewną wartość, która jest przez nas znana. Porównując te wyniki możemy stwierdzić poprawność danego algorytmu. W przypadku e-przetargu powinniśmy sprawdzić wszelkie kryptograficzne funkcje np. funkcje szyfrujące, funkcje deszyfrujące, funkcje biorące udział w autoryzacji, generator liczb pseudolosowych itd.

Test *integracji oprogramowania* polega na sprawdzeniu autentyczności oraz integralności używanych programów. W przypadku e-przetargu do tego celu można wykorzystać algorytm podpisu cyfrowego, który zweryfikuje

`

autentyczność.
Test *funkcji krytycznych* obejmuje pozostałe operacje, które związane są z bezpiecznym funkcjonowaniem modułów kryptograficznych. Krytyczne elementy są uzależnione od konkretnych projektów, w przypadku e-przetagu takimi elementami są na przykład składniki wchodzące w skład bezpiecznego schematu podziału sekretu.

**Test warunkowy**
Testy warunkowe są wykonywane, gdy dowolna operacja kryptograficzna tego zażąda. Mogą to być testy zwartości par kluczy publiczny-prywatny (kryptografia asymetryczna), obciążenia oprogramowania, ciągłości generatora liczb pseudolosowych.
Test z*wartości par kluczy publiczny-prywatny* jest wykonywany podczas operacji KEM. Szyfrowana jest znana wiadomość kluczem publicznym, następnie deszyfrowany jest utworzony szyfrogram za pomocą klucza prywatnego i porównywane są otrzymane wartości. Innym warunkiem wykonania opisywanego testu jest weryfikacja podpisu cyfrowego, np. przez centrum autoryzacji.
Test *obciążenia oprogramowania* wykonywany jest gdy oprogramowanie wchodzące w skład modułów kryptograficznych jest mocno wykorzystywane. Przeprowadzana jest wówczas autoryzacja takiego oprogramowania np. za pomocą algorytmów podpisu cyfrowego.
Test *ciągłości generatora liczb pseudolosowych* [39] jest wykonywany, gdy moduły kryptograficzne wykorzystują generator liczb pseudolosowych. Każdorazowo, gdy generator jest wykorzystywany, przeprowadzona jest wspomniana weryfikacja poprawności ciągów.

## 4.7. Optymalizacja nowego protokołu kryptograficznego dla e-przetargu – skalowane bezpieczeństwo

W rozdziale 4.4, opisano nowy protokół kryptograficzny realizujący elektroniczny przetarg. W bieżącym rozdziale zastosowano dla tego protokołu optymalizację wydajności, dostępności a w rezultacie jego bezpieczeństwa. Do tego celu wykorzystano zaprezentowany w rozdziale 3 mechanizm skalowanego bezpieczeństwa. Dla zilustrowania metody optymalizacyjnej wybrano jeden z opisanych podprotokołów e-przetargu a konkretnie podprotokół zgłoszenia przetargu (tab. 4.2).

W rozdziale 3.6, przedstawiono schemat postępowania dla metodologii skalowanego bezpieczeństwa. Schemat ten składa się z czterech faz, czyli inicjalizacji skalowanego bezpieczeństwa, definiowania protokołu kryptograficznego, ustalenia parametrów modelu skalowanego bezpieczeństwa dla konkretnych wersji protokołu oraz obliczenia poziomu bezpieczeństwa dla danej wersji protokołu. Skrócona forma elementów wchodzących w skład poszczególnych faz postępowania dla prezentowanej metodologii skalowanego

bezpieczeństwa znajduje się w tab. 3.5.

W kolejnych rozdziałach poszczególne fazy schematu postępowania będą zastosowane dla wybranego podprotokołu zgłoszenia przetargu.

### 4.7.1. Inicjalizacja modelu skalowanego bezpieczeństwa dla podprotokołu zgłoszenia przetargu

Pierwsza faza, czyli inicjalizacja modelu skalowalności, składa się z czterech kroków. W bieżącym rozdziale dla wybranego podprotokołu zgłoszenia przetargu zostaną zastosowane wszystkie kroki przewidziane w tej fazie.

W pierwszym kroku tworzymy tabelę bezpieczeństwa, która przedstawia zestawienie możliwych usług bezpieczeństwa wraz z realizującymi je mechanizmami. W analizowanym przypadku wykorzystano już utworzoną tabelę bezpieczeństwa, która przedstawiona jest w tab. 3.1.

W drugim kroku ustalamy wartości parametrów dla poszczególnych mechanizmów bezpieczeństwa, zawartych w tabeli bezpieczeństwa (tab. 3.1). Ta czynność została już wykonana podczas tworzenia tab. 3.1.

Trzeci krok pierwszej fazy schematu postępowania polega na utworzeniu grafów bezpieczeństwa dla możliwych do zastosowania w danym przypadku usług bezpieczeństwa. W przypadku podprotokołu zgłoszenia przetargu wybrano usługi integralności, poufności, niezaprzeczalności, bezpiecznego przechowywania danych, autoryzacji stron oraz zarządzanie przywilejami. Grafy te zostały wykonane już we wcześniejszym rozdziale 3.3.2. Usługa integralności jest przedstawiona na rys. 3.2, usługa poufności na rys. 3.3, usługa niezaprzeczalności na rys. 3.4, usługa bezpiecznego przechowywania danych na rys. 3.5, usługa autoryzacji stron na rys. 3.6 oraz usługa zarządzania przywilejami na rys. 3.7.

Poniżej grafów znajdują się opisy do poszczególnych wierzchołków grafów. Wierzchołki te charakteryzowane są przez odpowiednie parametry (rozdział 3.3.1). W ostatnim czwartym kroku pierwszej fazy schematu postępowania przyporządkowywane są wartości do tych parametrów. W analizowanym przypadku wartości te zostały dobrane wcześniej i są przedstawione w rozdziale 3.3.1.

### 4.7.2. Definiowanie podprotokołu zgłoszenia przetargu

Druga faza schematu postępowania dla przedstawianej metodologii skalowanego bezpieczeństwa polega na zdefiniowaniu protokołu kryptograficznego (rozdział 3.6). Ta czynność jest wykonywana w dwóch krokach. W pierwszym wybierany jest protokół kryptograficzny realizujący dany proces elektroniczny, a w drugim wybrany protokół dzielony jest na osobne podprotokołu. Podprotokoły następnie są dzielone na pojedyncze kroki.

W rozpatrywanym przypadku model skalowalności będzie zastosowany do podprotokołu zgłoszenia przetargu, który w skrócie został omówiony w rozdziale 4.4. W kroku drugim należy podzielić ten podprotokół na

`

pojedyncze kroki. Poniżej przedstawiono podprotokół zgłoszenia przetargu podzielony na osobne kroki.

**Krok1**

W pierwszym kroku, *F* przesyła do *GAP* podpisane cyfrowo ($SK_F$) oraz zaszyfrowane ($PK_{GAP}$) następujące informacje: swój numer rejestracyjny ($NR_F$), jego znacznik czasu ($T_{NR_F}$), warunki przetargu ($WP_F$) oraz swój indywidualny numer ($N_F$).

**Krok2**

Główna agencja przetargowa (*GAP*) weryfikuje numer rejestracyjny *F* ($NR_F$) oraz ważność jego znacznika czasu. Po pozytywnej autoryzacji *GAP* generuje indywidualny numer przetargu ($N_P$) oraz parę kluczy dla konkretnego przetargu ($SK_P$, $PK_P$). Prywatny klucz przetargu ($SK_P$) jest dzielony za pomocą progowego schematu podziału sekretu. Sekret jest podzielony na trzy części przeznaczone dla *F* ( $SK_{P(F)}$), dla *GAP* ($SK_{P(GAP)}$) oraz oferentów w przetargu ($SK_{P(OF)}$). Każda z części jest potrzebna do odtworzenia klucza prywatnego ($SK_P$).

**Krok3**

*GAP* wysyła podpisaną cyfrowo ($SK_{GAP}$) oraz zaszyfrowaną ($PK_F$) część sekretu przeznaczoną dla *F* ($SK_{P(F)}$).

**Krok 4**

*GAP* podaje do wiadomości publicznej np. na stronie WWW, numer przetargu ($N_P$), jego warunki ($WP_F$) oraz jego klucz publiczny ($PK_P$).

### 4.7.3. Ustalenie parametrów modelu skalowanego bezpieczeństwa dla rozpatrywanej wersji podprotokołu zgłoszenia przetargu

Kolejna, trzecia faza schematu postępowania polega na ustaleniu parametrów modelu skalowanego bezpieczeństwa dla rozpatrywanej wersji protokołu. Jak opisano w rozdziale 3.6, trzecia faza składa się z sześciu kroków.

W pierwszym kroku trzeciej fazy postępowania definiujemy wymagane usługi bezpieczeństwa dla pojedynczych kroków rozpatrywanego podprotokołu. Podział na kroki dla danego przypadku został przedstawiony w rozdziale 4.7.2. Wybór usług bezpieczeństwa został zapisany w tab. 4.1.

Tab. 4.1 Tabela prezentująca wymagane usług bezpieczeństwa dla poszczególnych
kroków podprotokołu zgłoszenia przetargu.

| | Kroki podprotokołu | | | | |
|---|---|---|---|---|---|
| Usługi bezpieczeństwa | | Krok 1 | Krok 2 | Krok 3 | Krok 4 |
| | I | TAK | TAK | TAK | TAK |
| | C | TAK | TAK | TAK | NIE |
| | NRS | TAK | NIE | TAK | TAK |
| | SS | NIE | TAK | NIE | NIE |
| | Au | NIE | TAK | NIE | NIE |
| | MP | NIE | TAK | NIE | NIE |

Dla omawianego podprotokołu zgłoszenia przetargu wprowadzono trzy wersje protokołu. Pierwsza charakteryzująca się wyborem podstawowych mechanizmów bezpieczeństwa, druga, która zakłada podwyższone środki ochrony informacji oraz trzecia, która zakłada bardzo wysokie środki ochrony informacji. Wybór mechanizmów bezpieczeństwa dla wersji pierwszej jest przedstawiony w tab. 4.2, dla wersji drugiej w tab. 4.3, a dla wersji trzeciej w tab. 4.4.

Tab. 4.2 Tabela prezentująca wybrane mechanizmy bezpieczeństwa realizujących poszczególne usługi bezpieczeństwa dla konkretnych kroków podprotokołu zgłoszenia przetargu w wersji 1.

| Wersja 1 | Kroki podprotokołu | | | | |
|---|---|---|---|---|---|
| Usługi bezpieczeństwa | | Krok 1 | Krok 2 | Krok 3 | Krok 4 |
| | I | 1 | 2,3 | 1,2,3 | 3 |
| | C | 1 | 1,2,3,4 | 1,2,3 | NIE |
| | NRS | 1,6 | NIE | 1,3 | 4 |
| | SS | NIE | 6 | NIE | NIE |
| | Au | NIE | 1,2,4 | NIE | NIE |
| | MP | NIE | 2 | NIE | NIE |

`

Tab. 4.3 Tabela prezentująca wybrane mechanizmy bezpieczeństwa realizujących poszczególne usługi bezpieczeństwa dla konkretnych kroków podprotokołu zgłoszenia przetargu w wersji 2.

| Wersja 2 | Kroki podprotokołu | | | | |
|---|---|---|---|---|---|
| Usługi bezpieczeństwa | | Krok 1 | Krok 2 | Krok 3 | Krok 4 |
| | I | 1,2,3 | 2,3 | 1,2,3,5 | 2,3,4 |
| | C | 1,2,3 | 1,2,3,4 | 1,2,3 | NIE |
| | NRS | 1,3,4 | NIE | 1,3,4,5 | 3,4,5 |
| | SS | NIE | 6,8 | NIE | NIE |
| | Au | NIE | 1,2,4,6 | NIE | NIE |
| | MP | NIE | 2 | NIE | NIE |

Tab. 4.4 Tabela prezentująca wybrane mechanizmy bezpieczeństwa realizujących poszczególne usługi bezpieczeństwa dla konkretnych kroków podprotokołu zgłoszenia przetargu w wersji 3.

| Wersja 3 | Kroki podprotokołu | | | | |
|---|---|---|---|---|---|
| Usługi bezpieczeństwa | | Krok 1 | Krok 2 | Krok 3 | Krok 4 |
| | I | 1,2,3,5 | 2,3,4,5,6 | 1,2,3,4,5 | 2,3,4,5 |
| | C | 1,2,3,5 | 1,2,3,4,5,6 | 1,2,3 | NIE |
| | NRS | 1,3,4,5,6 | NIE | 1,3,4,5,6,8 | 3,4,5,6,7,8 |
| | SS | NIE | 1,3,4,6,8 | NIE | NIE |
| | Au | NIE | 1,2,3,4,6 | NIE | NIE |
| | MP | NIE | 2,3 | NIE | NIE |

W trzecim kroku, trzeciej fazy schematu postępowania należy określić poziom wrażliwości mechanizmów bezpieczeństwa (rozdział 3.2.1). W przypadku podprotokołu zgłoszenia przetargu zwiększono wymagany minimalny poziom zabezpieczeń. Osiągnięcie tego poziomu wiąże się z zastosowaniem podstawowego zestawu mechanizmów bezpieczeństwa. Minimalny poziom zabezpieczeń jest regulowany za pomocą parametru wrażliwości, którego charakterystyka jest przedstawiona na rys 4.1. W przypadku podprotokołu zgłoszenia przetargu ustalono wartość parametru $Z$=2.

W kolejnym czwarty i piątym kroku, trzeciej fazy postępowania, ustalamy parametry potrzebne do obliczenia prawdopodobieństwa zajścia incydentu. W tym celu, w czwartym kroku wybieramy wierzchołki grafów bezpieczeństwa, utworzonych w pierwszej fazie schematu postępowania (rys. 3.2, 3.3, 3.4, 3.5, 3.6, 3.7), które odpowiadają wcześniej wybranym, z tabeli bezpieczeństwa (tab. 3.1) mechanizmom bezpieczeństwa (tab. 4.2, 4.3, 4.4). Wybór dokonywany jest dla wszystkich wymaganych usług bezpieczeństwa oraz dla wszystkich kroków podprotokołu. Poniżej przedstawiono dokonany wybór dla trzech wersji podprotokołu zgłoszenia przetargu.

***WERSJA 1 (tab. 4.2)***

**Krok1**

Integralność

Wierzchołki = 1.1 = 1.1.1 = 1.1.1.1 = 1.1.2 = 1.1.2.1 = 1.1.3 = 1.1.3.1 =1.1.6= 1.2 = 1.2.4 = 1.2.4.1=1

$F_{BOOL}$= (1.1.1.1 ⊕ 1.1.1.2) ∨ (1.1.2.1 ⊕ 1.1.2.2) ∨ (1.1.3.1 ⊕ 1.1.3.2) ∨ 1.1.6 ∨ (1.2.4.1 ⊕ 1.2.4.2)

Poufność

Wierzchołki = 2.1 = 2.1.1 = 2.1.1.1 = 2.1.2 = 2.1.2.1 = 2.1.3 = 2.1.3.1 =2.1.6= 2.2 =2.2.4 = 2.2.4.1 =1

$F_{BOOL}$= (2.1.1.1 ⊕ 2.1.1.2) ∨ (2.1.2.1 ⊕ 2.1.2.2) ∨ (2.1.3.1 ⊕ 2.1.3.2) ∨ 2.1.6 ∨ (2.2.4.1 ⊕ 2.2.4.2)

Niezaprzeczalność nadawcy

Wierzchołki = 3.1 = 3.1.1 = 3.1.1.1 = 3.1.2 = 3.1.2.1 = 3.1.3 = 3.1.3.1 = 3.1.6= 3.1.9 = 3.2 = 3.2.7 = 3.2.7.1 = 3.2.5 =1

$F_{BOOL}$= (3.1.1.1 ⊕ 3.1.1.2) ∨ (3.1.2.1 ⊕ 3.1.2.2) ∨ (3.1.3.1 ⊕ 3.1.3.2) ∨ 3.1.6 ∨ 3.1.9 ∨ (3.2.7.1 ⊕ 3.2.7.2) ∨ 3.2.5

**Krok2**

Integralność

Wierzchołki = 1.1 = 1.1.4 = 1.1.4.2 = 1.2 = 1.2.3 = 1.2.4 = 1.2.4.2 =1

$F_{BOOL}$= (1.1.4.1 ⊕ 1.1.4.2) ∨ (1.2.4.1 ⊕ 1.2.4.2) ∨ 1.2.3

Poufność

Wierzchołki = 2.1 = 2.1.4 = 2.1.4.2 = 2.1.8 = 2.2 =2.2.4 = 2.2.4.2 = 2.2.3 =1

$F_{BOOL}$= (2.1.4.1 ⊕ 2.1.4.2) ∨ 2.1.8 ∨ (2.2.4.1 ⊕ 2.2.4.2) ∨ 2.2.3

`

Bezpieczne przechowywanie danych

Wierzchołki = 4.2 = 4.2.7 = 4.2.7.1 = 4.2.6 =1

$F_{BOOL}$= (4.2.7.1⊕4.2.7.2) ∨ 4.2.6

Autoryzacja stron

Wierzchołki = 5.1 = 5.1.1 = 5.1.1.1 = 5.1.2 = 5.1.2.1 = 5.1.3 = 5.1.3.1 = 5.2 = 5.2.1 = 5.2.1.1 = 5.2.1.3 = 5.2.4 = 5.2.4.1= 1

$F_{BOOL}$= (5.1.1.1⊕5.1.1.2) ∨ (5.1.2.1⊕5.1.2.2) ∨ (5.1.3.1⊕5.1.3.2) ∨ (5.2.1.1 ⊕5.2.1.2) ∨ 5.2.1.3∨ (5.2.4.1⊕5.2.4.2)

Zarządzanie przywilejami

Wierzchołki = 6.2 = 1

$F_{BOOL}$= 6.2

**Krok3**

Integralność

Wierzchołki = 1.1 = 1.1.1 = 1.1.1.2 = 1.1.2 = 1.1.2.2 = 1.1.3 = 1.1.3.2 =1.1.6 = 1.2 = 1.2.4 = 1.2.4.2=1

$F_{BOOL}$= (1.1.1.1⊕1.1.1.2) ∨ (1.1.2.1⊕1.1.2.2) ∨ (1.1.3.1⊕1.1.3.2) ∨ 1.1.6 ∨ (1.2.4.1⊕1.2.4.2)

Poufność

Wierzchołki = 2.1 = 2.1.1 = 2.1.1.2 = 2.1.2 = 2.1.2.2 = 2.1.3 = 2.1.3.2 =2.1.6 = 2.2 =2.2.4 = 2.2.4.2 =1

$F_{BOOL}$= (2.1.1.1⊕2.1.1.2) ∨ (2.1.2.1⊕2.1.2.2) ∨ (2.1.3.1⊕2.1.3.2) ∨ 2.1.6 ∨ (2.2.4.1⊕2.2.4.2)

Niezaprzeczalność nadawcy

Wierzchołki = 3.1 = 3.1.1 = 3.1.1.2 = 3.1.2 = 3.1.2.2 = 3.1.3 = 3.1.3.2 = 3.1.6 = 3.2 = 3.2.7 = 3.2.7.1 =1

$F_{BOOL}$= (3.1.1.1⊕3.1.1.2) ∨ (3.1.2.1⊕3.1.2.2) ∨ (3.1.3.1⊕3.1.3.2) ∨ 3.1.6 ∨ (3.2.7.1⊕3.2.7.2)

**Krok4**

Integralność

Wierzchołki = 1.2 = 1.2.4 = 1.2.4.1=1

$F_{BOOL}$= (1.2.4.1⊕1.2.4.2)

Niezaprzeczalność nadawcy

Wierzchołki = 3.2 = 3.2.7 = 3.2.7.1 =1

$F_{BOOL}$= (3.2.7.1⊕3.2.7.2)

***WERSJA 2 (tab. 4.3)***

**Krok1**

Integralność

Wierzchołki = 1.1 = 1.1.1 = 1.1.1.2 = 1.1.2 = 1.1.2.2 = 1.1.3 = 1.1.3.2 = 1.1.6 =1.2 = 1.2.4 = 1.2.4.2=1

$F_{BOOL}$= (1.1.1.1⊕1.1.1.2) ∨ (1.1.2.1⊕1.1.2.2) ∨ (1.1.3.1⊕1.1.3.2) ∨ 1.1.6 ∨ (1.2.4.1⊕1.2.4.2)

Poufność

Wierzchołki = 2.1 = 2.1.1 = 2.1.1.2 = 2.1.2 = 2.1.2.2 = 2.1.3 = 2.1.3.2 =2.1.6= 2.2 =2.2.4 = 2.2.4.2 =1

$F_{BOOL}$= (2.1.1.1⊕2.1.1.2) ∨ (2.1.2.1⊕2.1.2.2) ∨ (2.1.3.1⊕2.1.3.2) ∨ 2.1.6 ∨ (2.2.4.1⊕2.2.4.2)

Niezaprzeczalność nadawcy

Wierzchołki = 3.1 = 3.1.1 = 3.1.1.2 = 3.1.2 = 3.1.2.2 = 3.1.3 = 3.1.3.2 = 3.1.6= 3.2 = 3.2.7 = 3.2.7.2 = 1

$F_{BOOL}$= (3.1.1.1⊕3.1.1.2) ∨ (3.1.2.1⊕3.1.2.2) ∨ (3.1.3.1⊕3.1.3.2) ∨ 3.1.6 ∨ (3.2.7.1⊕3.2.7.2)

**Krok2**

Integralność

Wierzchołki = 1.1 = 1.1.4 = 1.1.4.2 = 1.2 = 1.2.3 = 1.2.4 = 1.2.4.2 =1

$F_{BOOL}$= (1.1.4.1⊕1.1.4.2) ∨ (1.2.4.1⊕1.2.4.2) ∨ 1.2.3

Poufność

Wierzchołki = 2.1 = 2.1.4 = 2.1.4.2 = 2.1.8 = 2.2 =2.2.4 = 2.2.4.2 = 2.2.3 =1

$F_{BOOL}$= (2.1.4.1⊕2.1.4.2) ∨ 2.1.8 ∨ (2.2.4.1⊕2.2.4.2) ∨ 2.2.3

Bezpieczne przechowywanie danych

Wierzchołki = 4.2 = 4.2.7 = 4.2.7.1 = 4.2.6 = 4.2.4 = 1

$F_{BOOL}$= (4.2.7.1⊕4.2.7.2) ∨ 4.2.6∨ 4.2.4

Autoryzacja stron

Wierzchołki = 5.1 = 5.1.1 = 5.1.1.1 = 5.1.2 = 5.1.2.1 = 5.1.3 = 5.1.3.1 = 5.2 = 5.2.1 = 5.2.1.1 = 5.2.1.3 =5.2.4 = 5.2.4.1= 5.2.4.4 = 1

$F_{BOOL}$= (5.1.1.1⊕5.1.1.2) ∨ (5.1.2.1⊕5.1.2.2) ∨ (5.1.3.1⊕5.1.3.2) ∨ (5.2.1.1 ⊕5.2.1.2) ∨ 5.2.1.3 ∨ (5.2.4.1⊕5.2.4.2) ∨ 5.2.4.4

Zarządzanie przywilejami

Wierzchołki = 6.2 = 1

$F_{BOOL}$= 6.2

`

**Krok3**

Integralność

Wierzchołki = 1.1 = 1.1.1 = 1.1.1.2 = 1.1.2 = 1.1.2.2 = 1.1.3 = 1.1.6 =1.1.3.2 = 1.2 = 1.2.4 = 1.2.4.2=1.2.4.3=1

$F_{BOOL}$= (1.1.1.1⊕1.1.1.2) ∨ (1.1.2.1⊕1.1.2.2) ∨ (1.1.3.1⊕1.1.3.2) ∨ 1.1.6 ∨ (1.2.4.1⊕1.2.4.2) ∨ 1.2.4.3

Poufność

Wierzchołki = 2.1 = 2.1.1 = 2.1.1.2 = 2.1.2 = 2.1.2.2 = 2.1.3 = 2.1.6 = 2.1.3.2 = 2.2 =2.2.4 = 2.2.4.2 =1

$F_{BOOL}$= (2.1.1.1⊕2.1.1.2) ∨ (2.1.2.1⊕2.1.2.2) ∨ (2.1.3.1⊕2.1.3.2) ∨ 2.1.6 ∨ (2.2.4.1⊕2.2.4.2)

Niezaprzeczalność nadawcy

Wierzchołki = 3.1 = 3.1.1 = 3.1.1.2 = 3.1.2 = 3.1.2.2 = 3.1.3 = 3.1.3.2 = 3.1.8 =3.2 = 3.2.7 = 3.2.7.2 = 3.2.4 =1

$F_{BOOL}$= (3.1.1.1⊕3.1.1.2) ∨ (3.1.2.1⊕3.1.2.2) ∨ (3.1.3.1⊕3.1.3.2) ∨ 3.1.8 ∨ (3.2.7.1⊕3.2.7.2) ∨ 3.2.4

**Krok4**

Integralność

Wierzchołki = 1.2 = 1.2.4 = 1.2.4.2=1.2.4.4=1

$F_{BOOL}$= (1.2.4.1⊕1.2.4.2) ∨ 1.2.4.4

Niezaprzeczalność nadawcy

Wierzchołki = 3.2 = 3.2.7 = 3.2.7.2 = 3.2.4=1

$F_{BOOL}$= (3.2.7.1⊕3.2.7.2) ∨ 3.2.4

***WERSJA 3 (tab. 4.4)***

**Krok1**

Integralność

Wierzchołki = 1.1 = 1.1.1 = 1.1.1.2 = 1.1.2 = 1.1.2.2 = 1.1.3 = 1.1.3.2 = 1.1.6 = 1.2 = 1.2.4 = 1.2.4.2=1.2.4.3 = 1

$F_{BOOL}$= (1.1.1.1⊕1.1.1.2) ∨ (1.1.2.1⊕1.1.2.2) ∨ (1.1.3.1⊕1.1.3.2) ∨ 1.1.6 ∨ (1.2.4.1⊕1.2.4.2) ∨ 1.2.4.3

Poufność

Wierzchołki = 2.1 = 2.1.1 = 2.1.1.2 = 2.1.2 = 2.1.2.2 = 2.1.3 = 2.1.3.2 =2.1.6 = 2.2 =2.2.4 = 2.2.4.2 =2.2.4.3= 1

$F_{BOOL}$= (2.1.1.1⊕2.1.1.2) ∨ (2.1.2.1⊕2.1.2.2) ∨ (2.1.3.1⊕2.1.3.2) ∨ 2.1.6 ∨ (2.2.4.1⊕2.2.4.2) ∨ 2.2.4.3

Niezaprzeczalność nadawcy

Wierzchołki = 3.1 = 3.1.1 = 3.1.1.2 = 3.1.2 = 3.1.2.2 = 3.1.3 = 3.1.3.2 = 3.1.8 = 3.1.9= 3.2 = 3.2.7 = 3.2.7.2 =3.2.4=3.2.5 =1

$F_{BOOL}$= (3.1.1.1⊕3.1.1.2) ∨ (3.1.2.1⊕3.1.2.2) ∨ (3.1.3.1⊕3.1.3.2) ∨ 3.1.8 ∨ 3.1.9∨ (3.2.7.1⊕3.2.7.2) ∨ 3.2.4 ∨ 3.2.5

**Krok2**

Integralność

Wierzchołki = 1.1 = 1.1.4 = 1.1.4.2 = 1.1.4.3= 1.2 = 1.2.3 = 1.2.4 = 1.2.4.2 =1.2.4.3 = 1.2.4.4 =1

$F_{BOOL}$= [(1.1.4.1⊕1.1.4.2) ∨ 1.1.4.3]∨ [(1.2.4.1⊕1.2.4.2) ∨ 1.2.4.3∨ 1.2.4.4] ∨ 1.2.3

Poufność

Wierzchołki = 2.1 = 2.1.4 = 2.1.4.2 =2.1.4.3= 2.1.8 = 2.2 =2.2.4 = 2.2.4.2 = 2.2.4.3= 2.2.3 =1

$F_{BOOL}$= [(2.1.4.1⊕2.1.4.2) ∨ 2.1.4.3]∨ 2.1.8 ∨[ (2.2.4.1⊕2.2.4.2) ∨ 2.2.4.3] ∨ 2.2.3

Bezpieczne przechowywanie danych

Wierzchołki = 4.1 =4.1.1=4.1.1.2 = 4.1.2 = 4.1.2.2 = 4.1.3 = 4.1.3.2 = 4.2 = 4.2.7 = 4.2.7.2 = 4.2.6 = 4.2.4 = 1

$F_{BOOL}$= (4.1.1.1⊕4.1.1.2) ∨ (4.1.2.1⊕4.1.2.2) ∨ (4.1.3.1⊕4.1.3.2) ∨ (4.2.7.1 ⊕4.2.7.2) ∨ 4.2.6∨ 4.2.4

Autoryzacja stron

Wierzchołki = 5.1 = 5.1.1 = 5.1.1.2 = 5.1.2 = 5.1.2.2 = 5.1.3 = 5.1.3.2 = 5.2 = 5.2.1 = 5.2.1.1 = 5.2.1.3 =5.2.4 = 5.2.4.1= 5.2.4.4 = 1

$F_{BOOL}$= (5.1.1.1⊕5.1.1.2) ∨ (5.1.2.1⊕5.1.2.2) ∨ (5.1.3.1⊕5.1.3.2) ∨ (5.2.1.1 ⊕5.2.1.2) ∨ 5.2.1.3 ∨ (5.2.4.1⊕5.2.4.2) ∨ 5.2.4.4

Zarządzanie przywilejami

Wierzchołki = 6.1 = 6.2 =1

$F_{BOOL}$= 6.1∨ 6.2

`

**Krok3**

Integralność

Wierzchołki = 1.1 = 1.1.1 = 1.1.1.2 = 1.1.2 = 1.1.2.2 = 1.1.3 = 1.1.3.2 = 1.1.6 = 1.2 = 1.2.4 = 1.2.4.2=1.2.4.3=1.2.4.4=1

$F_{BOOL}$= (1.1.1.1 ⊕ 1.1.1.2) ∨ (1.1.2.1 ⊕ 1.1.2.2) ∨ (1.1.3.1 ⊕ 1.1.3.2) ∨ 1.1.6 ∨ (1.2.4.1 ⊕ 1.2.4.2) ∨ 1.2.4.3 ∨ 1.2.4.4

Poufność

Wierzchołki = 2.1 = 2.1.1 = 2.1.1.2 = 2.1.2 = 2.1.2.2 = 2.1.3 = 2.1.3.2 = 2.1.6 = 2.2 =2.2.4 = 2.2.4.2 =1

$F_{BOOL}$= (2.1.1.1 ⊕ 2.1.1.2) ∨ (2.1.2.1 ⊕ 2.1.2.2) ∨ (2.1.3.1 ⊕ 2.1.3.2) ∨ 2.1.6 ∨ (2.2.4.1 ⊕ 2.2.4.2)

Niezaprzeczalność nadawcy

Wierzchołki = 3.1 = 3.1.1 = 3.1.1.2 = 3.1.2 = 3.1.2.2 = 3.1.3 = 3.1.3.2 = 3.1.8 = 3.1.9= 3.1.10 =3.2 = 3.2.7 = 3.2.7.2 = 3.2.4 = 3.2.5=3.2.6=1

$F_{BOOL}$= (3.1.1.1 ⊕ 3.1.1.2) ∨ (3.1.2.1 ⊕ 3.1.2.2) ∨ (3.1.3.1 ⊕ 3.1.3.2) ∨ 3.1.8 ∨ 3.1.9 ∨ 3.1.10 ∨ (3.2.7.1 ⊕ 3.2.7.2) ∨ 3.2.4 ∨ 3.2.5 ∨ 3.2.6

**Krok4**

Integralność

Wierzchołki = 1.2 = 1.2.4 = 1.2.4.2=1.2.4.3 =1.2.4.4=1

$F_{BOOL}$= (1.2.4.1 ⊕ 1.2.4.2) ∨ 1.2.4.3 ∨ 1.2.4.4

Niezaprzeczalność nadawcy

Wierzchołki = 3.2 = 3.2.7 = 3.2.7.2 = 3.2.7.3 = 3.2.4= 3.2.5= 3.2.6 =1

$F_{BOOL}$= [(3.2.7.1 ⊕ 3.2.7.2) ∨ 3.2.7.3] ∨ 3.2.4 ∨ 3.2.5 ∨ 3.2.6

W następnym piątym kroku, ustalane są dalsze parametry potrzebne do obliczenia prawdopodobieństwa zajścia incydentu (rozdział 3.3.1). W przypadku podprotokołu zgłoszenia przetargu ustalono, że można w nim zdobyć średnie zasoby, czyli parametr *PP*=0,05, rodzaj instytucji realizujący proces elektroniczny, będzie o małym zagrożeniu (np. uczelnia), czyli *I*=0,03, a hipotetyczne ryzyko poniesione przez atakującego w wyniku wykrycia włamania niech będzie niskie, czyli *H*=0,01 (przetarg odbywa się w kraju o mało rygorystycznym prawodawstwie w stosunku do przestępczości elektronicznej). Innymi parametrami, które należy w tym kroku określić jest potencjalne przygotowanie atakujących pod względem wiedzy ($\omega_{LK}$) oraz poniesionych kosztów ($\omega_{LP}$). W rozpatrywanym przypadku ustalono, że napastnicy mają dużą wiedzę, czyli $\omega_{LK}$ = 0,8 ale mogą ponieść bardzo małe koszty finansowe, czyli $\omega_{LP}$ = 0,2. W kroku piątym należy również, określić

ewentualną uwzględnianą poprawkę do całkowitej wartości prawdopodobieństwa zajścia incydentu. Jej wartość jest zależna między innymi od ilości cząstkowych prawdopodobieństw, które zostaną uwzględnione w poprawce. W tym kroku należy tę liczbę określić, czyli wskazać parametr *N* (formuła (3.6)). W rozpatrywanym przypadku ustalono, że wartość parametru *N=2*. To zagadnienie jest szczegółowo opisane w rozdziale 3.3.3.
Ostatni, szósty krok trzeciej fazy schematu postępowania polega na zdefiniowaniu parametrów określających wpływ udanego ataku na system. W tym celu określane są parametry opisujące maksymalne zasoby zdobyte podczas udanego ataku (*LZ*), finansowe straty podczas udanego ataku (*F*), straty finansowe konieczne do usunięcia awarii, które zostały spowodowane udanym atakiem ($\alpha$) oraz straty poniesione w wyniku spadku reputacji firmy ($\beta$).

Tak jak podano w rozdziale 3.6 w tym miejscu można wprowadzić kolejne rozróżnienie wersji protokołu. W przypadku podprotokołu zgłoszenia przetargu, który jest częścią elektronicznej wersji przetargu (rozdział 4.4), rozpatrzono dwie jego wersje. Pierwsza zakłada, że realizowany będzie przetarg, którego wartość finansowa będzie wysoka, czyli potencjalne bezpośrednie straty będą wysokie (*F*). Natomiast straty pośrednie związane z usunięciem potencjalnych awarii wynikłych z udanego ataku będą przyjmowały średnią wartość ($\alpha$). Istotnym elementem w pierwszej rozpatrywanej wersji jest fakt, że przetarg jest realizowany dla bardzo istotnego kontrahenta i ewentualne jego niepowodzenie, bardzo mocno wpłynie na reputacje firmy ($\beta$). W drugim rozpatrywanym przypadku zarówno wartość finansowa przetargu (*F*) jak i pośrednie starty wynikłe z usunięcia awarii po udanym ataku ($\alpha$) nie ulegają zmianie. Istotna zmiana dotyczy rodzaju kontrahenta, dla którego realizowany jest przetarg, Firma ta nie posiada dużego prestiżu w wyniku czego ewentualne niepowodzenie nie będzie związane z dużą startą reputacji strony organizującej elektroniczny przetarg ($\beta$). W pierwszym przypadku aplikacja będzie procesem o dużym wpływie udanego ataku na system. Natomiast wersja druga będzie miała dużo mniejszy wpływ udanego ataku na system. Pierwsza wersja, będzie nazywana wersją A, a druga wersją B. W tab. 4.5, przedstawiono ustalone wartości wspomnianych parametrów. Definiowanie parametrów określających wpływ udanego ataku na system jest ostatnim krokiem trzeciej fazy schematu postępowania dla prezentowanej metodologii skalowanego bezpieczeństwa.

Tab. 4.5 Tabela prezentująca wybrane parametry charakteryzujące wpływu

`

udanego ataku na system dla poszczególne usługi bezpieczeństwa oraz konkretnych kroków podprotokołu zgłoszenia przetargu w wersjach A i B.

| | **Wersja A** | | | | **Wersja B** | | | |
|---|---|---|---|---|---|---|---|---|
| | ***LZ*** | ***F*** | $\alpha$ | $\beta$ | ***LZ*** | ***F*** | $\alpha$ | $\beta$ |
| *Krok 1* | | | | | | | | |
| **I** | 0,8 | 0,8 | 0,4 | 0,8 | 0,8 | 0,8 | 0,4 | 0,15 |
| **C** | 0,8 | 0,8 | 0,5 | 0,9 | 0,8 | 0,8 | 0,5 | 0,2 |
| **NRS** | 0,8 | 0,5 | 0,3 | 0,7 | 0,8 | 0,5 | 0,3 | 0,1 |
| *Krok 2* | | | | | | | | |
| **I** | 0,8 | 0,7 | 0,4 | 0,7 | 0,8 | 0,7 | 0,4 | 0,1 |
| **C** | 0,8 | 0,9 | 0,6 | 0,9 | 0,8 | 0,9 | 0,6 | 0,2 |
| **SS** | 0,7 | 0,6 | 0,4 | 0,6 | 0,7 | 0,6 | 0,4 | 0,1 |
| **Au** | 0,8 | 0,7 | 0,5 | 0,7 | 0,8 | 0,7 | 0,5 | 0,1 |
| **MP** | 0,3 | 0,3 | 0,2 | 0,4 | 0,3 | 0,3 | 0,2 | 0,05 |
| *Krok 3* | | | | | | | | |
| **I** | 0,8 | 0,6 | 0,4 | 0,7 | 0,8 | 0,6 | 0,4 | 0,1 |
| **C** | 0,8 | 0,7 | 0,6 | 0,9 | 0,8 | 0,7 | 0,6 | 0,2 |
| **NRS** | 0,8 | 0,4 | 0,3 | 0,5 | 0,8 | 0,4 | 0,3 | 0,05 |
| *Krok 4* | | | | | | | | |
| **I** | 0,3 | 0,3 | 0,3 | 0,6 | 0,3 | 0,3 | 0,3 | 0,05 |
| **NRS** | 0,3 | 0,4 | 0,3 | 0,5 | 0,3 | 0,4 | 0,3 | 0,05 |

### 4.7.4. Obliczanie poziomu bezpieczeństwa dla rozpatrywanej wersji podprotokołu zgłoszenia przetargu

Kiedy wszystkie parametry opisujące model skalowanego bezpieczeństwa dla danej wersji protokołu kryptograficznego zostały zdefiniowane, wówczas można przejść do ostatniej, czwartej fazy schematu postępowania, czyli obliczenie poziomu bezpieczeństwa dla wszystkich wersji rozpatrywanego protokołu. Poziom bezpieczeństwa jest obliczany według formuły (3.10) (rozdział 3.5). Formuła ta jest funkcją trzech czynników (parametrów): poziomu zabezpieczeń ($L^Z$) (rozdział 3.2), prawdopodobieństwa zajścia incydentu ($P$) (rozdział 3.3) oraz wpływu udanego ataku na system ($\omega$) (rozdział 3.4). W celu obliczenia poziomu bezpieczeństwa dla danej wersji protokołu, należy obliczyć czynniki wchodzące w skład formuły (3.10), które następnie posłużą do obliczenia końcowej wartości poziomu bezpieczeństwa.

W bieżącym rozdziale przedstawiono obliczone poziomy bezpieczeństwa dla wszystkich wyodrębnionych wersji rozpatrywanego podprotokołu zgłoszenia przetargu. Jak wspomniano wyżej przed obliczeniem poziomu bezpieczeństwa należy obliczyć czynniki wchodzące w skład formuły (3.10). Obliczenia wykonywane są indywidualnie dla wszystkich kroków wchodzących w skład podprotokołu zgłoszenia przetargu oraz dla wszystkich usług bezpieczeństwa wymaganych w poszczególnych krokach.

W rozpatrywanym przypadku zdefiniowano dwa rozróżnienia podprotokołu

zgłoszenia przetargu. Pierwsze dotyczy użytych mechanizmów bezpieczeństwa. Zdefiniowano wersje pierwszą (tab. 4.2), która zakłada użycie podstawowych mechanizmów bezpieczeństwa, wersję drugą (tab. 4.3), która zakłada użycie bardziej zaawansowanych mechanizmów bezpieczeństwa oraz wersję trzecią (tab. 4.4), która zakłada użycie najmocniejszych zabezpieczeń. Druga modyfikacja polega na wprowadzeniu różnego wpływu udanego ataku na system dla rozpatrywanego podprotokołu zgłoszenia przetargu. W tym celu utworzono wersję A, która zakłada, że wpływ udanego ataku na system jest wysoki oraz wersje B, która zakłada, że wpływ udanego ataku na system jest znacznie mniejszy niż w wersji A (tab. 4.5).

W tab. 4.6, 4.7 i 4.8 przedstawiono otrzymane wartości wspomnianych czynników wchodzących w skład formuły (3.10) oraz końcową wartość obliczonego poziomu bezpieczeństwa ($F_S$). Obliczenia zostały wykonane dla wszystkich zdefiniowanych wersji podprotokołu zgłoszenia przetargu.

***Wersja 1 (tab. 4.2)***

Tab. 4.6 Obliczone wartości poziomu bezpieczeństwa dla wersji 1 podprotokołu zgłoszenia przetargu wraz z trzema czynnikami wchodzącymi w skład formuły (3.10), czyli poziomu zabezpieczeń ($L^Z$), prawdopodobieństwa zajścia incydentu ($P$) oraz wpływu udanego ataku na system ($\omega$).

| | **wersja A** | | | **wersja B** | | |
|---|---|---|---|---|---|---|
| | ***P*** | $\omega$ | $L^Z$ | ***P*** | $\omega$ | $L^Z$ |
| *Krok 1* | | | | | | |
| **I** | 0,5752 | 0,533333 | 0,25 | 0,5752 | 0,36 | 0,25 |
| **C** | 0,56045 | 0,586667 | 0,25 | 0,56045 | 0,4 | 0,25 |
| **NRS** | 0,55324 | 0,4 | 0,16 | 0,55324 | 0,24 | 0,16 |
| *Krok 2* | | | | | | |
| **I** | 0,4233 | 0,48 | 0,04 | 0,4233 | 0,32 | 0,04 |
| **C** | 0,4014 | 0,64 | 0,7225 | 0,4014 | 0,453333 | 0,7225 |
| **SS** | 0,38242 | 0,373333 | 0,0225 | 0,38242 | 0,245 | 0,0225 |
| **Au** | 0,473692 | 0,506667 | 0,25 | 0,473692 | 0,333333 | 0,25 |
| **MP** | 0,206 | 0,09 | 0,25 | 0,206 | 0,055 | 0,25 |
| *Krok 3* | | | | | | |
| **I** | 0,5693 | 0,48 | 0,49 | 0,5693 | 0,32 | 0,49 |
| **C** | 0,5693 | 0,586667 | 0,49 | 0,5693 | 0,4 | 0,49 |
| **NRS** | 0,5752 | 0,32 | 0,16 | 0,5752 | 0,213333 | 0,16 |
| *Krok 4* | | | | | | |
| **I** | 0,28 | 0,12 | 0,01 | 0,28 | 0,065 | 0,01 |
| **NRS** | 0,28 | 0,12 | 0,01 | 0,28 | 0,075 | 0,01 |
| **$F_S$** | 0,062744 | | | 0,081779 | | |

***Wersja 2 (tab. 4.3)***

Tab. 4.7 Obliczone wartości poziomu bezpieczeństwa dla wersji 2

`

podprotokołu zgłoszenia przetargu wraz z trzema czynnikami wchodzącymi w skład formuły (3.10), czyli poziomu zabezpieczeń ($L^Z$), prawdopodobieństwa zajścia incydentu ($P$) oraz wpływu udanego ataku na system ($\omega$).

| | **wersja A** | | | **wersja B** | | |
|---|---|---|---|---|---|---|
| | ***P*** | $\omega$ | $L^Z$ | ***P*** | $\omega$ | $L^Z$ |
| *Krok 1* | | | | | | |
| **I** | 0,5693 | 0,533333 | 0,49 | 0,5693 | 0,36 | 0,49 |
| **C** | 0,5457 | 0,586667 | 0,49 | 0,5457 | 0,4 | 0,49 |
| **NRS** | 0,5693 | 0,4 | 0,25 | 0,5693 | 0,24 | 0,25 |
| *Krok 2* | | | | | | |
| **I** | 0,4233 | 0,48 | 0,04 | 0,4233 | 0,32 | 0,04 |
| **C** | 0,4014 | 0,64 | 0,7225 | 0,4014 | 0,453333 | 0,7225 |
| **SS** | 0,375137 | 0,373333 | 0,04 | 0,375137 | 0,245 | 0,04 |
| **Au** | 0,462712 | 0,506667 | 0,3025 | 0,462712 | 0,333333 | 0,3025 |
| **MP** | 0,206 | 0,09 | 0,25 | 0,206 | 0,055 | 0,25 |
| *Krok 3* | | | | | | |
| **I** | 0,5575 | 0,48 | 0,7225 | 0,5575 | 0,32 | 0,7225 |
| **C** | 0,5693 | 0,586667 | 0,49 | 0,5693 | 0,4 | 0,49 |
| **NRS** | 0,5575 | 0,32 | 0,3025 | 0,5575 | 0,213333 | 0,3025 |
| *Krok 4* | | | | | | |
| **I** | 0,385 | 0,12 | 0,09 | 0,385 | 0,065 | 0,09 |
| **NRS** | 0,39448 | 0,12 | 0,0625 | 0,39448 | 0,075 | 0,0625 |
| **$F_S$** | 0,086599 | | | 0,111805 | | |

***Wersja 3 (tab. 4.4)***

Tab. 4.8 Obliczone wartości poziomu bezpieczeństwa dla wersji 3

podprotokołu zgłoszenia przetargu wraz z trzema czynnikami wchodzącymi w skład formuły (3.10), czyli poziomu zabezpieczeń ($L^Z$), prawdopodobieństwa zajścia incydentu ($P$) oraz wpływu udanego ataku na system ($\omega$).

| | **wersja A** | | | **wersja B** | | |
|---|---|---|---|---|---|---|
| | ***P*** | $\omega$ | $L^Z$ | ***P*** | $\omega$ | $L^Z$ |
| *Krok 1* | | | | | | |
| **I** | 0,5575 | 0,533333 | 0,7225 | 0,5575 | 0,36 | 0,7225 |
| **C** | 0,5457 | 0,586667 | 0,7225 | 0,5457 | 0,4 | 0,7225 |
| **NRS** | 0,55632 | 0,4 | 0,4225 | 0,55632 | 0,24 | 0,4225 |
| *Krok 2* | | | | | | |
| **I** | 0,3996 | 0,48 | 0,25 | 0,3996 | 0,32 | 0,25 |
| **C** | 0,41303 | 0,64 | 1 | 0,41303 | 0,453333 | 1 |
| **SS** | 0,375137 | 0,373333 | 0,49 | 0,375137 | 0,245 | 0,49 |
| **Au** | 0,462712 | 0,506667 | 0,4225 | 0,462712 | 0,333333 | 0,4225 |
| **MP** | 0,4144 | 0,09 | 1 | 0,4144 | 0,055 | 1 |
| *Krok 3* | | | | | | |
| **I** | 0,5516 | 0,48 | 0,81 | 0,5516 | 0,32 | 0,81 |
| **C** | 0,5693 | 0,586667 | 0,49 | 0,5693 | 0,4 | 0,49 |
| **NRS** | 0,55278 | 0,32 | 0,5625 | 0,55278 | 0,213333 | 0,5625 |
| *Krok 4* | | | | | | |
| **I** | 0,3768 | 0,12 | 0,16 | 0,3768 | 0,065 | 0,16 |
| **NRS** | 0,3994 | 0,12 | 0,2025 | 0,3994 | 0,075 | 0,2025 |
| $\mathbf{F_S}$ | 0,163866 | | | 0,204509 | | |

Analizę otrzymanych wyników dla rozpatrywanego podprotokołu zgłoszenia przetargu rozpoczniemy od uzyskanych wartości prawdopodobieństwa zajścia incydentu ($P$). Rozważania zostaną wykonane w porównaniu z analizą analogicznych wyników otrzymanych dla protokołu SSL Handshake Protocol (rozdział 3.7.5). Tak samo jak w przypadku protokołu SSL Handshake Protocol, w obrębie poszczególnej rozpatrywanej wersji podprotokołu np. wersji 3 (tab. 4.8) wartości parametru $P$ dla wersji A i B oraz dla odpowiednich kroków, a w ich obrębie konkretnych usług bezpieczeństwa, są identyczne. Jest to spowodowane tym, że według naszego założenia wersje A i B różnią się jedynie wpływem udanego ataku na system ($\omega$).

Podczas analizy otrzymanych wyników dla protokołu SSL Handshake Protocol (rozdział 3.7.5) stwierdzono, że dla poszczególnych wersji rozpatrywanego protokołu otrzymane wartości prawdopodobieństwa zajścia incydentu ($P$), dla wszystkich kroków oraz założonych w nich usług bezpieczeństwa, przyjmują przybliżoną wartość. Stwierdzono również, że ten

`

fakt jest spowodowany tym, że w każdym kroku rozpatrywanego protokołu, używane są podobne, podstawowe mechanizmy bezpieczeństwa (tabela 3.8), które to wykorzystują podobne moduły kryptograficzne (rozdział 3.7.2). Otrzymane wyniki dla wszystkich wersji podprotokołu zgłoszenia przetargu, posiadają tak samą charakterystykę. Wartości prawdopodobieństwa zajścia incydentu (*P*) w obrębie każdego kroku są zbliżone. Wyjątkiem jest przypadek, gdy w danym kroku nieużywane są podstawowe mechanizmy bezpieczeństwa, takie jak w przypadku większości kroków, tylko inne, dodatkowe mechanizmy bezpieczeństwa. Taka sytuacja ma miejsce w kroku 4 dla wszystkich wersji podprotokołu zgłoszenia przetargu (tab. 4.6, 4.7, 4.8). Wartości prawdopodobieństw zajścia incydentu (*P*) przyjmują wówczas dużo niższe wartości niż w przypadku pozostałych kroków. Ten fakt jest dodatkowym potwierdzeniem przedstawionych rozważań.

Podczas analizy otrzymanych wyników dla przypadku protokołu SSL Handshake Protocol (rozdział 3.7.5) stwierdzono, że w obydwu wersjach (wersja 1 i 2) rozpatrywanego protokołu prawdopodobieństwo zajścia incydentu (P) dla poszczególnych kroków protokołu przyjmuje średnie wartości. Stwierdzono dalej, że jest to w dużym stopniu spowodowane faktem, że w rozpatrywanym przypadku zdolność atakującego pod względem wiedzy, jak i poniesionych kosztów jest również na średnim poziomie i wynosi odpowiednio $\omega_{LK}$ = 0,6 i $\omega_{LP}$ = 0,5. W rozważanym podprotokole zgłoszenia przetargu zauważono taką samą tendencję. W tym przypadku zdolność atakującego pod względem poniesionych kosztów jest niższa niż w protokole SSL Handshake Protocol i wynosi $\omega_{LP}$ = 0,2 ale jest to rekompensowane przez zdolność atakującego pod względem wiedzy, która jest wyższa i wynosi $\omega_{LK}$ = 0,8.

Analiza protokołu SSL Handshake Protocol wykazała, że wraz ze zwiększeniem zastosowanych mechanizmów bezpieczeństwa w poszczególnych wersjach (wersja 1 i 2) wartość prawdopodobieństwa zajścia incydentu zmienia się nieznacznie. Stwierdzono, że jest to spowodowane tym, że dodatkowe mechanizmy bezpieczeństwa oprócz wprowadzenia nowych zabezpieczeń stanowią nowe zagrożenie dla systemu. W przypadku rozpatrywanego podprotokołu zgłoszenia przetargu dla poszczególnych wersji (wersja 1,2,3) można zauważyć taką samą tendencję (tab. 4.6, 4.7, 4.8).

Kolejnym parametrem, który zostanie rozważony, jest parametr charakteryzujący wpływ udanego ataku na system ($\omega$ ). Uzyskane wyniki przedstawiają również taką samą tendencję jak w przypadku rozpatrywanego w rozdziale 3.7.4 protokołu SSL Handshake Protocol. Zauważono tam, że w obydwu wersjach (wersja 1 i 2) wraz ze zmniejszeniem parametrów określających wpływ udanego ataku na system, czyli parametrów *F* i $\alpha$ (wersja B) ostateczna wartość parametru określającego wpływ udanego ataku na system ($\omega$ ) przyjmuje mniejsze wartości. W rozważanym podprotokole

zgłoszenia przetargu, dla wszystkich rozpatrywanych wersji (wersja 1,2,3) w stosunku do wersji początkowej (wersja A) został zmniejszony jeden parametr określających wpływ udanego ataku na system, czyli parametr $\beta$ (wersja B). Taka modyfikacja powoduje, że ostateczna wartość parametru określającego wpływ udanego ataku na system ($\omega$ ) przyjmuje mniejsze wartości.

Ostatnim obliczanym parametrem jest poziom zabezpieczeń ($L^Z$). Wartość tego parametru jest uzależniona od wybrany mechanizmów bezpieczeństwa (tab. 4.2, 4.3, 4.4). Podobnie jak w przypadku parametru określającego prawdopodobieństwo zajścia incydentu ($P$) jest sprawą oczywistą, że w obrębie poszczególnej rozpatrywanej wersji podprotokołu np. wersji 3 (tab. 4.8) jego wartość dla wersji A i B oraz dla odpowiednich kroków a w ich obrębie konkretnych usług bezpieczeństwa jest identyczna. Jest to spowodowane tym, że zgodnie z naszymi założeniami wersje A i B różnią się jedynie wpływem udanego ataku na system ($\omega$ ).

Prezentowana w książce optymalizacja podprotokołu zgłoszenia przetargu polega na wyznaczeniu poziomów bezpieczeństwa, które są zróżnicowane w zależności od potencjalnego zagrożenia. W zależności od potencjalnych zagrożeń stosowane są różne mechanizmy ochrony informacji, a zmniejszenie ich nadmiarowości prowadzi do zwiększenia wydajności, dostępności a w rezultacie bezpieczeństwa podprotokołu. Istotą prezentowanego modelu skalowalności jest określenie poziomu bezpieczeństwa ($F_S$) dla poszczególnych wersji podprotokołu. Analizując wersję 1 rozpatrywanego podprotokołu zgłoszenia przetargu (tab. 4.6) widać, że wraz ze zmniejszeniem wpływu udanego ataku na system uzyskiwany poziom bezpieczeństwa realizowanego procesu elektronicznego rośnie. Dla wersji A przyjmuje on wartość $F_S$=0,062744, a dla wersji B przyjmuje wartość $F_S$=0,081779.

Podobne wyniki zostały uzyskane w przypadku, gdy w wersji 2 podprotokołu zgłoszenia przetargu (tab. 4.7) zostały użyte dodatkowe mechanizmy bezpieczeństwa. W tym przypadku również wraz ze zmniejszeniem wpływu udanego ataku na system uzyskiwany poziom bezpieczeństwa realizowanego procesu elektronicznego rośnie. Dla wersji A przyjmuje on wartość $F_S$=0,086599 a dla wersji B przyjmuje wartość $F_S$=0,111805.

W wersji 3 podprotokołu zgłoszenia przetargu (tab. 4.8) zostały użyte bardzo wysokie mechanizmy bezpieczeństwa. W tym przypadku tendencja jest nadal zachowana i wraz ze zmniejszeniem wpływu udanego ataku na system, uzyskiwany poziom bezpieczeństwa realizowanego procesu elektronicznego rośnie. Dla wersji A przyjmuje on wartość $F_S$=0,163866, a dla wersji B przyjmuje wartość $F_S$=0,204509.

Istotą prezentowanej optymalizacji jest to, że zmieniając charakter realizowanego procesu elektronicznego w rozpatrywanym przypadku podprotokołu zgłoszenia przetargu było to związane z rodzajem kontrahenta, dla którego realizowany jest elektroniczny przetarg, można zrezygnować z niektórych użytych mechanizmy bezpieczeństwa, zachowując jednocześnie

`

określony poziom bezpieczeństwa. W celu potwierdzenia tej optymalizacji przedstawiono następujące rozumowanie. Analiza będzie dotyczyła tab. 4.7. Jeżeli w rozpatrywanej wersji 2 podprotokołu zgłoszenia przetargu zastosowano zwiększone mechanizmy bezpieczeństwa i gdy wpływ udanego ataku na system jest duży (wersja A), wówczas uzyskany poziom bezpieczeństwa, który gwarantuje bezpieczne przeprowadzenie procesu, jest równy $F_S$=0,086599. Warunkiem koniecznym, żeby inne wersje rozpatrywanego podprotokołu spełniały założone wymogi bezpieczeństwa jest uzyskanie poziomu bezpieczeństwa, który jest większy lub równy od obliczonego, czyli $F_S \geq$ 0,086599. Warto zwrócić uwagę na otrzymane poziomy bezpieczeństwa dla wersji 1 rozpatrywanego podprotokołu (tab. 4.6). Jeżeli dla danego podprotokołu zmniejszymy wpływ udanego ataku na system, czyli w rozpatrywanym przypadku wersja B, wówczas otrzymany poziom bezpieczeństwa będzie równy $F_S$=0,081779, czyli mniejszy od obliczonego w wersji 2. Niestety uzyskany poziom bezpieczeństwa jest mniejszy, czyli ta wersja podprotokołu nie spełnia założonych wymogów bezpieczeństwa. Warto jednak zauważyć, że uzyskane poziomy bezpieczeństwa są bardzo zbliżone a ich różnica jest niewielka. W celu spełnienia wymogów bezpieczeństwa określonych w wersji 2 ($F_S \geq 0{,}086599$) należy rozpatrzyć kolejną wersję podprotokołu zgłoszenia przetargu, pośrednią między 1 i 2, w której zostaną zwiększone w stosunku do wersji 1 mechanizmy bezpieczeństwa na tyle, żeby osiągnięty poziom bezpieczeństwa spełniał wspomniany warunek. Biorąc pod uwagę różnicę w uzyskanym poziomie bezpieczeństwa dla wersji 1 i 2 można stwierdzić, że ich wersja pośrednia będzie stosowała mniej mechanizmów bezpieczeństwa niż w wersji 2. Dzięki temu będzie można zmniejszyć nadmiarowe środki ochrony informacji co wprowadzi dodatkową optymalizacje procesu elektronicznego, która poprawi jego wydajność, dostępność a w rezultacie bezpieczeństwo.

BIBLIOGRAFIA

**[1]** **Aldrich D., Bertot J. C., McClure Ch. R.:** *E-Government: initiatives, developments, and issues,* **Government Information Quarterly, 19, s.349-355, (2002).**

**[2]** **ANSI X3.106:** *American National Standard for Information Systems-Data Link Encryption,* **American National Standards Institute, (1983).**

**[3]** **Aoki K., Ichikawa T., Kanda M., Matusi M., Moriai S., Nakajima J., Tokita T.:** *Camellia: A 128-bit block cipher suitable for multiple platforms,* **Springer: Lecture Notes in Computer Science, 1528, (2000).**

**[4]** **Ball M. J., Lillis J.:** *E-health: transforming the physican/patient relationship,* **International Journal of Medical Informatics, 61, s. 1-10, (2001).**

**[5]** **Baudron O., Stern J.:** *Non-interactive Private Auctions,* **InProceedings of the 5th Annual Conference on Financial Cryptography, s.300-313, (2000).**

**[6]** **Blum L., Blum M., Shub M.:** *A simple unpredictable pseudo-random number generator,* **SIAM Journal of Computing, 15, pp. 364-383, (1986).**

**[7]** **Cantoni V., Cellarion M., Porta M.:** *Perspectives and challenges in e-learning: towards natural interaction paradigms*, **Journal of Visual Languages & Computing, 15, s. 333-345, (2004).**

**[8]** **CERT Polska:** *Zabezpieczenie prywatności w usługach internetowych,* (**2001).**

**[9]** **CERT Polska**: *Analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespołu CERT Polska w roku 2003,* **(2003).**

**[10]** **CERT Polska:** *Analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespołu CERT Polska w roku 2004,* **(2004).**

**[11]** **Comer D.E**.: *Sieci komputerowe i intersieci,* **Wydawnictwo Naukowo Techniczne, Warszawa 2001.**

**[12]** **Dantu R., Kolan P.:** *Risk management using behavior based Bayesian Networks,* **Springer: LNCS, 3495, s. 115-126, (2005).**

**[13]** **Deliverable No: D.JRA.6.3.4.**: *Secure protocol architectures through the concept of pseudonymization,* **EuroNGI NoE, (2003).** http://eurongi.enst.fr/archive/127/JRA634.pdf .

**[14]** **Dz.U. z 2004 r. Nr 19, poz. 17:** *Prawo zamówień publicznych* : http://ks.sejm.gov.pl/proc4/ustawy/2218_u.htm

**[15]** **ElGamal T.:** *A public key cryptosystem and signature scheme based on discrete logarithms.* **IEEE Trans. Inform. Theory, 31, s.469-472, (1985).**

**[16]** **ETSI TS 102 042**: *Policy requirements for certification authorities issuing public key certificates***, (2002).**

**[17]** **ETSI TS 102 023:** *Policy requirements for time-stamping authorities,* **(2003)**.

**[18]** **Farn K., Lin S., Fung A.:** *A study on information security management system evaluation- assets, threat and vulnerability,* **Elsevier: Computer Standards & Interfaces, 26, s. 501-513, (2004).**

**[19]** **FIPS PUB 46,** *Data Encryption Standard,* **National Bureau of Standards, U.S. Department of Commerce, (1977).**

**[20]** **FIPS PUB 140-2:** *Security Requirements for Cryptographic Modules,* **Federal Information Processing Standards Publication, (2001).**

**[21]** **FIPS PUB 197,** *Advanced Encryption Standards,* **Federal Information Processing Standards Publication 197, (2001).**

**[22]** **Francik J., Trybicka-Francik K.**: *Gospodarka elektroniczna – perspektywy i bariery,* **Studia Informatica, 22, (2001)**.

**[23]** **Gerber M., Solms R**.: *Management of risk in the information age,* **Elsevier: Computer & Security, 24, s. 16-30, (2005).**

**[24]** **Gregor B., Stawiszyński M.**: *e-Commerce*", **Oficyna Wydawnicza Branta, Bydgoszcz-Łódź 2002**.

**[25]** **Gritzalis S., Katsikas S., Lekkas D., Monstantinos K., Polydorou E.:** *Securing The Electronic Market: The KEYSTONE Public Key Infrastructure Architecture,* **Elsevier: Computer & Security, 9, s. 731-746, (2000).**

**[26]** **Groves J**.: *Security for Application Service Providers,* **Network Security, 1, s.6-9, (2001).**

**[27]** **Hager C.T.R.:** *Context Aware and Adaptive Security for Wireless Networks*. **PhD dissertation, Department of Electrical and Engineering, Virginia Polytechnical Institute and State University, Blacksburg, Virginia, November 2004.**

**[28]** **Ham W., Kim K., Imai H.:** *Yet Another Strong Sealed-Bid Auction,* **In Proceedings of the Symposium on Cryptography and Information Security, (2003).**

**[29]** **Harkavy M., Tygar J.D., Kikuchi H.:** *Electronic auctions with private bids,* **in Proceedings of the 3rd USENIX Workshop on Electronic Commerce, s.61-74, (1998).**

**[30]** **ISI for DARPA, RFC 793:** *Transport Control Protocol,* **September 1981.**

**[31]** **ISO/IEC FDIS 13335-1:** *Information technology – Security techniques – Concepts and models for managing and planning ICT security.*

**[32]** **ISO/IEC 15408:** *Information technology – Security techniques – Evaluation criteria for IT security.*

**[33]** **ISO/IEC 19790:** *Security techniques – Security requirements for cryptographic modules.*

**[34]** **ISO/IEC 11770-3:** *Key management-Part 3: Mechanisms using asymmetric techniques,* (**1999).**

**[35]** **ISO/IEC 17799:** *Information technology – Code of practice for information security management,* **(2002).**

**[36]** **ISO/IEC 18033-2:** *Security techniques – Encryption algorithms – Part 2: Asymmetric cipher,* **(2003).**

`

**[37]** **ISO/IEC 18033-3:** Security *techniques – Encryption algorithms – Part 3: Block cipher*, (**2003).**

**[38]** **ISO/IEC 14888-3:** *Security techniques – Digital signatures with appendix – Part 3: Certificate-based mechanism,* **(2004).**

**[39]** **ISO/IEC 18031:** *Security techniques – Random bit generation,* **(2004).**

**[40]** **Jaeger P.T., Thompson K.M**.: *E-government around the world: Lessons, challenges and future directions,* **Government Information Quarterly, 20, s. 389-394, (2003).**

**[41]** **Jakobsson M., Juels A.:** *Mix and match: secure function evaluation via ciphertexts,* **Springer: Lecture Notes in Computer Science, 1976, s.162-177, (2000).**

**[42]** **Jha, S., Linger, R., Longstaff, T., Wing, J.:** *Survivability Analysis of Network Specifications,* **International Conference on Dependable Systems and Networks, IEEE CS Press (2000).**

**[43]** **Juels A., Szydlo M.:** *A two-server, sealed-bid auction protocol,* **Springer: Lecture Notes in Computer Science, 2357, (2002).**

**[44]** **Karwowski W., Orłowski A.**: *Bezpieczeństwo usług WWW,* **Materiały VIII Krajowej Konferencji Zastosowań Kryptografii Enigma (2004).**

**[45]** **KEYSTONE project deliverable 9.1:** *Final project report,* **(1998).**

**[46]** **Księżopolski B., Kotulski Z.:** *Cryptographic protocol for electronic auctions with extended requirements,* **Annales UMCS: Informatica, 2, s. 391-400, (2004).**

**[47]** **Księżopolski B., Kotulski Z.:** *Bezpieczeństwo e-urzędu - Centrum Certyfikacji,* **Współczesne Problemy Systemów Czasu Rzeczywistego, Wydawnictwo Naukowo Techniczne, Rozdział 31, s. 349-359, Warszawa 2004.**

**[48]** **Księżopolski B., Kotulski Z.:** *Zagrożenia procesów komunikacyjnych w e-commerce oraz sposoby przeciwdziałania,* **Informatyka narzędziem współczesnego zarządzania, Wydawnictwo Polsko-Japońskiej Wyższej Szkoły Technik Komputerowych, 2004.**

**[49]** **Księżopolski B., Kotulski Z.:** *On a concept of scalable security: PKI-based model with supporting cryptographic modules,* **in: Electronic Commerce Theory and Applications, Wydawnictwo Wydziału Zarządzania i Ekonomii Politechniki Gdańskiej, s.73-83, (2005).**

**[50]** **Księżopolski B., Kotulski Z.:** *On a probability modeling of incidence occurrence in electronic processes,* 7**th NATO regional conference on military communications and information systems, Wydawnictwo Wojskowego Instytutu Łączności, Zegrze, s.297-305, (2005).**

**[51]** **Księżopolski B., Dziurda A.:** *Implementation of certification subprotocol for electronic auction,* **Annales UMCS: Informatica, 3, s.355-364, (2005).**

**[52]** **Księżopolski B., Kotulski Z.:** *On a concept of scalable security: PKI-based model with using additional cryptographic modules,* **9th East-European Conference on Advances in Databases and Information Systems, Tallinn University of Technology Press, Estonia, pp. 221-232,** ISBN 9985-59-545-9. Wersja elektroniczna: **CEUR –WS, vol. 152, pp. 221-232,** ISSN 1613-0073, **(2005).**

**[53]** **Kulesza K., Kotulski Z.:** *On Automatic Secret Generation and Sharing for Karin-Greene - Hellman Scheme,* **Kluwer: Artificial Intelligence and Security in Computing Systems, s. 281-292, (2003).**

**[54]** **Lai X.:** *On the Design and Security of Block Ciphers,* **Hartung-Gorre Verlag, ETH Series in Information Processing, 1, (1992).**

**[55]** **Lambrinoudakis C., Gritzalis S., Dridi F., Pernul G.:** *Security requirements for e-government services: a methodological approach for developing a common PKI-based security policy,* **Elsevier: Computer Communication, 26, s. 1873-1883, (2003).**

**[56]** **Lindskog S.:** *Modeling and Tuning Security from a Quality of Service Perspective,* **PhD dissertation, Department of Computer Science and Engineering, Chalmers University of Technology, Göteborg, Sweden,**
**(2005).**

**[57]** **Lindskog S., Jonsson E.:** *Adding Security to Quality of Service Architectures.* **In *Proceedings of the SS-GRR Conference*, L'Aquila, Italy, August (2002).**

`

**[58]** **Lye, K., Wing J.:** *Game Strategies in Network Security,* **International Journal of Information Security, February (2005).**

**[59]** **Madan B., Goseva-Popstojanova K., Vaidyanathan K., Trivedi K.**: *A method for modeling and quantifying the security attributes of intrusion tolerant systems,* **Elsevier: Performance Evaluation, 56, s. 167-186, (2004).**

**[60]** **Menezes A.J., Oorschot P., Vanstone S.C.:** *Handbook of Applied Cryptography***, CRC Press, Boca Raton 1997.**

**[61]** **Merabti M., Shi Q., Oppliger R.:** *Advanced security techniques for network protection,* **Elsevier: Computer Communications, 23, s.151-158, (2000).**

**[62]** **Ministerstwo Nauki i Informatyzacji:** *Strategia Informatyzacji Rzeczypospolitej Polskiej - ePolska,* **maj 2003.**

**[63]** **NIST:** *Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories,* **(2004)**.

**[64]** **NIST FIPS PUB 186:** *Digital Signature Standard,* **National Institute of Standards and Technology, U.S. Department of Commerce, (1994).**

**[65]** **NIST FIPS PUB 180-1:** *Secure Hash Standard,* **National Institute of Standards and Technology, U.S. Department of Commerce, DRAFT, (1994).**

**[66]** **Ong C.S., Nahrstedt K., Yuan W.:** *Quality of protection for mobile applications.* **In Proceedings of the 2003 IEEE International Conference on Multimedia & Expo (ICME'03), Baltimore, Maryland, USA, (2003).**

**[67]** **OpenSSL Project, official webpage:** http://www.openssl.org/.

**[68]** **OpenTSA Project, official webpage:** http://www.opentsa.org/.

**[69]** **Oram A.:** *Peer-to-Peer: Harnessing the power of Disruptive Technologies***, Wydawnictwo O'Reilly, 2001.**

**[70]** **Patel A., Gladychev P., Katsikas S., Gritzalis S., Lekkas D**.: *Support for Legal Framework and Anonymity in the KEYSTONE Public Key Infrastructure Architecture.*
http://www.syros.aegean.gr/users/lekkas/pubs/c/1999UIPPb.pdf

**[71]** **Pieprzyk J. Hardjono T. Seberry J. :** *Teoria bezpieczeństwa systemów komputerowych*, **Wydawnictwo Helion, Gliwice 2005.**

**[72]** **Reiter M., Rubin A.:** *Crowds: Anonymity for Web Transaction,* **ACM Transaction on Information and System Security**, **1, s.66-92, (1998).**

**[73]** **Rivest R.L., Shamir A., Adelman L.M.:** *A method for obtaining digital signatures and public-key cryptosystems,* **Communications of the ACM, 21, s.120-126, (1978).**

**[74]** **Rivest R. RFC 1321:** *The MD5 Message Digest Algorithm*, **April (1992)**.

**[75]** **Schneck P., Schwan K.:** *Authenticast: An Adaptive Protocol for High-Performance, Secure Network Applications,* **Technical Report GIT-CC-97-22, (1997).**

**[76]** **Schneier B.:** *Kryptografia dla praktyków,* **Wydawnictwo Naukowo Techniczne, Warszawa 2002.**

**[77]** **Schneier, B.:** *Attack Trees,* **Dr. Dobb's Journal, vol. 12 (1999)**

**[78]** **Security in a Web Services World**: *A Proposed Architecture and Roadmap*, http://www106.ibm.com/developerworks/webservices/library/ws-secmap.

**[79]** **Sewilla European Council:** *An information society for all – Commission of the European Communitie*," **eEurope 2005, (2002).**

**[80]** **Shamir. A.:** *How to share a secret,* **Communication of the ACM, 22, p.612-613, (1979).**

**[81]** **Shoup V.:** *IBM Research Report: On formal Models for Secure Key Exchange,* **(1999).** http://www.shoup.net/papers/skey.pdf.

**[82]** **Specyfikacja opisująca protokół kryptograficzny SSL v. 3.00:** http://wp.netscape.com/eng/ssl3/.

**[83]** **Stallings W.:** *Ochrona sieci i intrsieci,* **Wydawnictwo Naukowo Techniczne, Warszawa 1999.**

**[84]** **Stinson R.D.:** *Kryptografia. W teorii i w praktyce*, **Wydawnictwo Naukowo Techniczne , Warszawa 2005.**

`

**[85]** **Suzuki K., Kobayashi K., Morita H.:** *Efficient sealed-bid auction using hash chain,* **Springer: Lecture Notes in Computer Science, 2015, s.183-191, (2001).**

**[86]** **Swiler, L.: Phillips, C., Ellis, D., Chakerian, S.:** *Computer-attack graph generation tool.* **DISCEX '01 (2001)**

**[87]** **Szczypiorski K.:** *System steganograficzny dla sieci o współdzielonym medium,* **Krajowe Sympozjum Telekomunikacji KST, s.199-205, (2003).**

**[88]** **Teoh A., Ngo D., Goh A.:** *Personalised cryptographyic key generation based on Face Hashing,* **Elsevier: Computer & Security, 23, s.606-614, (2004).**

**[89]** **Tzong-Sun W., Chien-Lung H.:** *Efficient user identification scheme with key distribution preserving anonymity for distributed computer networks,* **Elsevier: Computer & Security, 23. s.120-125, (2004).**

**[90]** **Viswanathan K., Boyd C., Dawson E.:** *A three phased schema for sealed-bid auction system design,* **Springer: Lecture Notes in Computer Science 1841, s.412-426, (2000).**

**[91]** **W3C Recommendation:** *XML Encryption Syntax and Processing*, http://www.w3.org/TR/XMLENC-CORE.

**[92]** **W3C Recommendation:** *XML Signature Syntax and Processing,* http://www.w3.org/TR/XMLDSIG-CORE.

**[93]** **Zimmermann P.R.:** *The Official PGP User's Guide*, **MIT Press 1995**.

**[94]** **Zwierko A., Kotulski Z.:** *A new protocol for group authentication providing partial anonymity,* **Proceedings IEEE**: **Next Generation Internet Networks, pp. 356 – 363, (2005).**

**[95]** **Zwierko A., Kotulski Z.:** *Mobile agents: preserving privacy and anonymity,* **Springer: Lecture Notes in Computer Science, 3490, pp. 246-258, (2005).**

**[96]** **Zwierko A., Kotulski Z.:** *A new protocol for group authentication providing partial anonymity,* **1st EuroNGI Conference on Next Generation Internet Networks - Traffic Engineering /NGI 2005 / Rome in: Next Generation Internet Networks, s. 356 – 363, (2005).**

**[97]** **Księżopolski B., Lafourcade P.:** *Attack and revision of electronic auction protocol using OFMC,* **IBIZA 2007 - Annales UMCS Informatica 2007, pp. 171-183**.

`