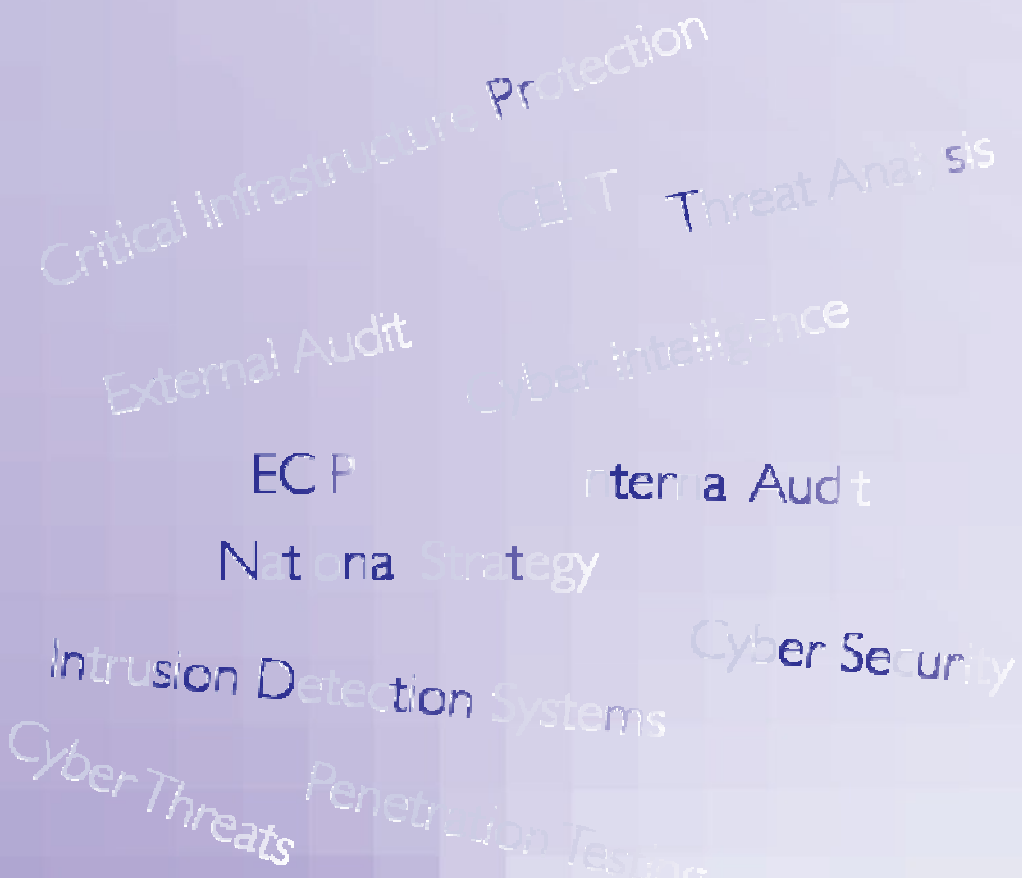
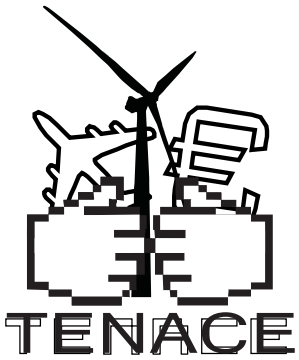
ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ:

Загрози, атаки та контрзаходи



Березень
2014



ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ:

Загрози, атаки та контрзаходи

Березень 2014

Редактори

Люка Монтанарі
Леонардо Куерзоні

Автори

Джузеппе Атенієзе
Роберто Бальдоні
Доменіко Даніеле Блуазі
Андреа Бондаваллі
Франческо Буккафуррі
Андреа Чеккареллі
Алессандро Сілардо
Марчелло Чинкве
Луїджі Копполіно
Доменіко Котронео
Сальваторе Д'Антоніо
Фелічіта Ді Джандоменіко
Чезаріо Ді Сарно
Джанлука Діні
Валеріо Формікола
Алесія Гарофало
Антонелла Гуццо
Лука Іоккі
Джанлука Лакс
Антоніо Ліой
Паоло Лолліні
Федеріко Маджі
Луїджі Вінченцо Манчіні
Іларія Маттеуччі
Лука Монтанарі
Леонардо Монтеккі
Лука Моретто
Даніель Нарді
Роберто Нателла
Антоніно Ночера
Нікола Ностро
Іда Клаудія Панетта
Антоніо Печчіа
Роберто П'єтрантуоно
Андреа Пульєзе
Леонардо Кверцоні
Луїджі Романо
Доменіко Розачі
Стефано Руссо
Марко Валліні
Ніно Вінченцо Верде
Стефано Занеро

За підтримкою:

Клаудіо Чиккотеллі
Elizabeth Lee Fabio Petroni

Зміст

Передмова **1**

Анотація **3**

1 Визначення та поняття **5**

1.1 Визначення критичної інфраструктури....5
1.2 Стратегія кібербезпеки ЄС....8
1.3 Національні стратегії захисту....9
1.4 Основні питання безпеки критичної інфраструктури....23

2 Загрози, вразливі місця та випадкові збої **27**

2.1 Загрози....27
2.2 Вразливості....29
2.3 Атаки....35
2.4 Підходи до відновлення та захисту....37
2.5 Випадкові несправності....39

3 Фінансові системи **49**

3.1 Опис критичної інфраструктури....49
3.2 Стандартні рішення для захисту КІ....56
3.3 Типи атак і використовувані вразливості....58
3.4 Стратегії захисту....60
3.5 Підходи до усунення несправностей....64
3.6 Відкриті проблеми....72

4 Електромережа **75**

4.1 Опис критичної інфраструктури....75

4.3 Типи атак і використовувані вразливості 88
4.4 Стратегії захисту 91
4.5 Підходи до усунення несправностей 93
4.6 Відкриті проблеми 95

5 Транспорт **101**
5.1 Управління повітряним рухом 101
5.2 Морська транспортна система 109
5.3 Залізнична система 117

6 Зрілість італійської критичної інфраструктури **131**
6.1 Актуальність КІ в суспільстві 131
6.2 Зрілість захисту від кібератак 141
6.3 Вартість кіберзлочинності в Італії 144
6.4 Готовність Італії до кібербезпеки 144

Бібліографія **149**

Передмова

Критична інфраструктура (КІ) є серцевиною будь-якої розвиненої цивілізованої країни. Вона включає, серед іншого, фінанси та страхування, транспорт (масовий транспорт, залізниці та літаки), державні послуги (правоохоронні органи, пожежні та екстрені служби), енергетику, охорону здоров'я. Нещодавні вірусні атаки на системи SCADA іранських ядерних установок, а також атаки, спрямовані на телекомунікаційну та енергетичну інфраструктуру Естонії та Грузії, показують, наскільки кібератаки на КІ стають все більш поширеними та руйнівними. Багато в чому це є результатом зростання впливу інформаційних технологій (ІТ), які використовуються в КІ, на Інтернет, що, у свою чергу, мотивується бажанням скоротити операційні витрати шляхом переходу на відкриті мережеві технології та готову обчислювальну техніку. Усі опитування провідних організацій сектору безпеки показують, що очікується, що атаки збільшаться в масштабах, стануть точнішими, а отже, стануть справжньою кіберзброєю.

Організації, які зазнають атак, несуть серйозні матеріальні та нематеріальні витрати, які, наприклад, у контексті фінансової установи, за деякими оцінками, можуть перевищувати 6 млн доларів США на день. Це на додаток до численних пов'язаних нематеріальних витрат, таких як шкода репутації та погіршення взаємодії з користувачем. У контексті енергетичного та транспортного секторів кібератаки на таку інфраструктуру також можуть бути людські жертви. Покращення знань, навичок і можливостей країни з кібербезпеки буде важливим для підтримки відкритого суспільства та захисту його життєво важливих інфраструктур (телекомунікаційні мережі, мережі електромереж, промисловість, фінансова інфраструктура тощо).

Цей примірник було розроблено та написано в контексті італійського проєкту TENACE, який фінансується в рамках програми PRIN 2010 Міністерством університетів та досліджень Італії (MIUR). Проект TENACE досліджує захист національної КІ від кіберзагроз, дотримуючись підходу співпраці. TENACE розглядає 3 сценарії: фінансову інфраструктуру, енергетичну мережу та транспортні системи. Вони представляють 3 дуже різні ситуації з різними взаємозалежностями, загрозами, вразливими місцями та можливими контрзаходами.

Метою TENACE є визначення спільних технічних та організаційних методологій, необхідних для підвищення захисту таких КІ. Крім того, існує конкретна мета — розглянути загальні кроки, необхідні для розробки єдиної методології та розуміння підпільної економіки, яка сприяє нападу. Результатом цього дослідження конкретних уразливостей КІ та пов'язаних з ними атак є розробка алгоритмів, моделей, архітектур та інструментів як засобів забезпечення ефективного захисту КІ, підвищення рівня безпеки та надійності, враховуючи супротивника, що постійно розвивається. Примірник надає читачеві в доступній формі сучасний аналіз захисту фінансової, енергетичної та транспортної інфраструктур від кібератак. Він вказує на стандартні рішення для захисту конкретної КІ, типи атак і використовуваних вразливостей, стратегії захисту та підходи до пом'якшення несправностей. Примірник відредагували Лука Монтанарі та Леонардо Куерцоні. Вміст написаний декількома вченими, що належать до консорціуму TENACE.

TENACE складається з міждисциплінарної групи академічних вчених із 9 найпрестижніших італійських університетів (Римський університет La Sapienza, Неаполітанський університет Федеріко II, Політехнічний інститут Мілана, Університет Тренто, Університет Флоренції, Політехнічний університет Турину, Університет Неаполя Партенопе, Університет Пізи, Університет Реджо-Калабрія, Університет Калабрії) та Національної дослідницької ради (CNR).

Рим, 3 Лютий 2014

Роберто Бальдоні
Координатор проєкту TENACE
Центр кіберрозвідки та інформаційної безпеки Università degli Studi di Roma "La Sapienza"

Анотація

Сьогодні більшість сучасних країн базують своє економічне багатство та суспільний добробут на кількох інфраструктурах. Ці інфраструктури є наріжним каменем розвитку країни, і завдяки цій ролі вони вважаються критично важливими активами, які необхідно захищати від можливих атак і збоїв у роботі. Оскільки ця тема незалежно розглядається різними країнами світу, немає однорідної концепції того, що означає захист критичної інфраструктури. Цей документ намагається надати аналіз поточної світової ситуації щодо цієї теми, зберігаючи при цьому особливу увагу до європейського сценарію.

Структура документа розділена на 3 частини. У І-ій частині (Розділ 1) документ містить огляд різних визначень того, що таке КІ та що означає її захист. У цій частині розповідається як про загальні відомості, так і про те, як різні країни адаптували свої законодавчі рамки для охоплення питань захисту КІ. У ІІ-ій частині (розділи 2, 3, 4 і 5) документ стосується більш технічних аспектів. Спочатку в ньому представлено передумови про загрози, уразливості та випадкові збої, які загрожують інфраструктурі в цілому, а потім аналізуються особливості 3 конкретних сценаріїв: фінансові системи, електромережі та транспортний сектор. ІІІ-я частина документа (розділ 6) завершується аналізом зрілості захисту КІ в Італії, надаючи кілька цифр і статистичних даних.

TENACE - Захист національної критичної інфраструктури від кіберзагроз – це дослідницький проєкт, який фінансується італійським Ministero dell'Istruzione, dell'Università e della Ricerca в рамках програми Progetti di Ricerca di Interesse Nazionale (номер проекту 20103P34XC). Додаткова інформація про TENACE доступна на офіційному веб-сайті за адресою http://www.dis.uniroma1.it/~tenace/.

Глава

1 Критичная інфраструктура: Визначення та поняття

Захист національної КІ сьогодні вважається першочерговою метою всіх сучасних країн світу. Оцінка складності проблем, пов'язаних із досягненням цієї мети, обов'язково повинна починатися з узгодженого бачення того, що таке КІ та що насправді означає захист критичної інфраструктури. На сьогодні не існує загальновизнаного визначення КІ. У цьому розділі наведено огляд найпоширеніших визначень, приділяючи особливу увагу європейському випадку, який охоплює всі країни-члени Європейського Союзу (Розділ 1.1). Повідомляються деякі інші визначення щодо інших реалій. Крім того, у цьому розділі аналізуються аспекти управління та законодавчі аспекти захисту КІ Італії та надається огляд деяких інших розвинених країн (Розділ 1.3). Нарешті, у цій главі обговорюються відкриті проблеми (розділ 1.4) і представлена важлива проблема у сфері захисту критичної інфраструктури: управління взаємозалежностями між інфраструктурами.

1.1 Визначення критичної інфраструктури

Що стосується критичної інфраструктури, то, незважаючи на численні спроби, досі не існує загальновизнаного визначення, яке забезпечує класифікацію, яка б відповідала характеристикам кожної нації. Критичною інфраструктурою часто називають таку інфраструктуру, неправильне функціонування якої, навіть протягом обмеженого періоду часу, може негативно вплинути на економіку окремих суб'єктів або груп, спричинивши економічні збитки та/або навіть поставити людей і речі під загрозу безпеці та безпеці [119].

У Європейському Союзі КІ визначається як «актив, система або її частина, розташована в державах-членах, яка має важливе значення для підтримки життєво важливих суспільних функцій, здоров'я, безпеки, економічного чи соціального добробуту людей, а також порушення або знищення яких мало б значний вплив на державу-члена в результаті нездатності підтримувати ці функції»[21]. Тоді як Європейська критична інфраструктура (ЕКІ) визначається як «КІ, розташована в державах-членах, порушення або знищення якої матиме значний вплив принаймні на 2 держави-члени. Значущість впливу повинна бути оцінена з точки зору наскрізних критеріїв. Це включає наслідки міжгалузевої залежності від інших типів інфраструктури»[21].

Позначення критичної інфраструктури як ЕКІ є результатом складного техніко-політичного процесу, який виникає внаслідок потенційного впливу, який може бути спричинений збоєм/руйнуванням інфраструктури з точки зору галузевої та міжгалузевої значимості. Критерії міжгалузевої оцінки стосуються:

- потенційних жертв за кількістю загиблих і поранених;
- економічного потенціалу;
- наслідків, з точки зору фінансових втрат, погіршення якості продукції або послуг, а також наслідків/збитків для навколишнього середовища;
- потенційних наслідків для населення з точки зору впливу на громадську довіру, фізичні страждання та порушення повсякденного життя, включаючи втрату основних послуг.

Що в основному випливає з європейської директиви [21], процитованої вище, це те, що зобов'язання власників/операторів щодо безпеки їхньої інфраструктури мають полягати у запобіганні або принаймні обмеженні наслідків для інших країн. Іншими словами, враховуючи загальноєвропейську роль, яку відіграє така велика інфраструктура, рівні безпеки повинні відповідати високому якісному стандарту, і, таким чином, правила, які мають бути прийняті, визначаються не лише державою-членом, у якій розташована така інфраструктура, а й на європейському рівні. Важливим компонентом Європейської програми захисту КІ (ЄПЗКІ) є інформаційна мережа попередження про критичну інфраструктуру (CIWIN), захищена загальнодоступна інформаційно-комунікаційна система в Інтернеті, яка дозволяє суб'єктам, залученим до захисту КІ (ЗКІ), обмінюватися інформацією. Інформація, пов'язана з ЗКІ, і передові практики.

Цікаве альтернативне визначення, незалежне від наданого в директиві ЄС, можна знайти в «Міжнародному довіднику СІІР 2008/2009» [119], де КІ визначаються як «інфраструктура, неправильне функціонування якої навіть протягом обмеженого періоду періоду часу, може негативно вплинути на економіку окремих суб'єктів або груп, спричинивши економічні збитки та/або навіть наразити їх на ризик безпеки».

Розглядаючи сценарій США, публічний закон 107–56 (26.10.2001) США визначає КІ як «системи та активи, фізичні чи віртуальні, які є настільки життєво важливими для Сполучених Штатів, що непрацездатність або знищення таких систем і активів матиме виснажливий вплив на безпеку, національну економічну безпеку, національне громадське здоров'я чи безпеку або будь-яку комбінацію цих питань». Незважаючи на наявність кількох відмінностей, по суті обидва наведені вище визначення спрямовані на виявлення потенційних загроз, таких, як людська помилка, випадкові аварії та атаки, які можуть призвести до несправності або початку кризи КІ, що знаходиться під спостереженням.

У 2006 році Європейська комісія визначила мережеву та інформаційну безпеку як «здатність мережі або інформаційної системи протистояти (...) випадковим подіям або зловмисним діям, які ставлять під загрозу доступність, автентичність, цілісність і конфіденційність збережених або передані дані та пов'язані з ними послуги, які пропонуються або доступні через ці мережі та системи»[19]. Таким чином, захист критичної інформаційної інфраструктури (ЗКІІ) має вирішальне значення як для автономної інфраструктури, так і для тих, які є функціональними для працездатності інших КІ. ЗКІІ включає «програми та діяльність власників інфраструктури, операторів, виробників, користувачів і регулюючих органів, які спрямовані на підтримку продуктивності КІІ у разі збоїв, атак або аварій вище визначеного мінімального рівня послуг і спрямовані на мінімізація часу відновлення та збитків»[17].

Енергетика	Атомна промисловість
Інформаційні комунікаційні технології	Водопостачання
Харчова промисловість	Охорона здоров'я
Фінансування	Транспорт
Хімічна промисловість	Космос
Дослідження	

Таблиця 1.1: Проект ЄС щодо сфер діяльності критичної інфраструктури [18].

Протягом багатьох років європейський уряд склав списки [18] з визначенням 11 територій, у яких працює КІ (див. таблицю 1.1).

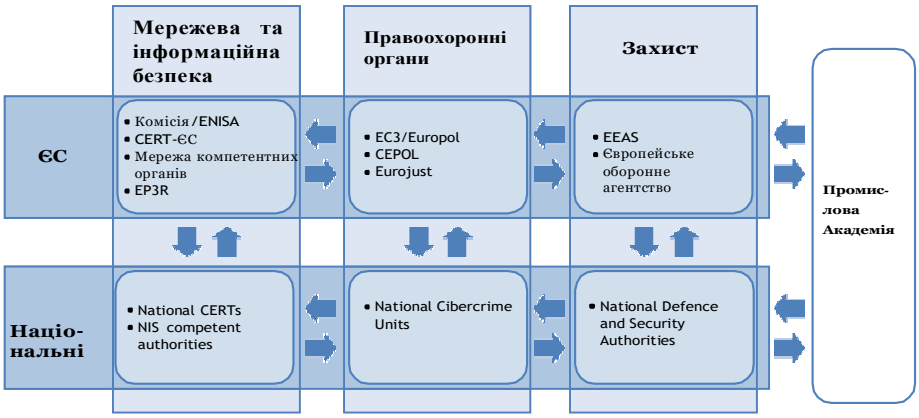
Мотиви, які спонукали ЄС до переліку цих КІ, часто прості: банківські та фінансові послуги відіграють життєво важливу роль в економіці кожної країни, тому порушення буде величезним ризиком для всієї системи. Крім того, енергетичний сектор є критичним. Електрична енергія має різні особливості, включаючи легкість перетворення в інші форми енергії (механічну, світлову, теплову тощо), легкість і гнучкість транспортування, можливість широкого розповсюдження і, в той же час, зберігається, тільки в обмежених кількостях. Це означає, що в будь-який час попит повинен бути збалансований виробництвом енергії. Необхідність використання ІКТ піддає зазначені сфери ризику комп'ютерних зломів. Слід зазначити, що з оприлюдненням директиви Ради 2008/114/ЕС [20] європейський уряд прийняв лише 2 з перерахованих вище сфер, а саме енергетику та транспорт, як ті, у яких діє ЕКІ. Більше того, кілька країн Європейського Союзу самостійно надають списки критичних секторів на національному рівні.

1.2 Стратегія кібербезпеки ЄС

Підтримка належного рівня кібербезпеки в контексті ЄС включає різні сектори з різними юрисдикціями та обов'язками як на національному рівні, так і на рівні ЄС. Управління кібербезпекою через централізований нагляд на європейському рівні неможливо. Національні уряди несуть основну відповідальність за підтримку належного рівня безпеки та повинні співпрацювати на рівні ЄС у разі ризиків і порушень безпеки, які виходять за межі національних кордонів.

Структури, задіяні в підтримці кібербезпеки, організовані в трьох основних областях: мережева та інформаційна безпека (NIS), правоохоронна діяльність і оборона. На національному рівні країни-члени вже повинні мати національні структури в кожній із вищезазначених сфер (або в результаті Європейської стратегії кібербезпеки) (див. рис. 1.1). Держави-члени несуть відповідальність за ретельне визначення ролей і відповідальності таких національних структур.

Європейська стратегія пропонує державам-членам заохочувати обмін інформацією між національними структурами, які займаються кібербезпекою, і приватним сектором, щоб вони могли мати комплексне бачення ризиків і загроз безпеці, а також краще розуміти методи кіберзлочинності, щоб швидше реагувати на них. і ефективно.



Малюнок 1.1: Стратегія кібербезпеки ЄС: взаємодіючі організації на національному рівні та рівні ЄС [34].

На рівні ЄС задіяно кілька організацій. У регіоні NIS Європейське агентство мережевої та інформаційної безпеки (ENISA), створене в 2004 році, відповідає за покращення мережевої та інформаційної безпеки. Наразі Рада Європи та Європейський парламент розглядають новий регламент [24] щодо зміцнення ENISA та модернізації її повноважень. ENISA також відповідатиме за формування експертних знань у сфері безпеки промислових систем контролю, транспортної та енергетичної інфраструктури. Команда реагування на комп'ютерні надзвичайні ситуації на рівні ЄС (CERT-EU), відповідальна за безпеку IT-систем агентств та установ ЄС, була створена в 2012 році.

Крім того, у березні 2009 року Європейська комісія заснувала Європейське державно-приватне партнерство для стійкості (EP3R) з метою заохочення обміну інформацією, пов'язаною з NIS, між зацікавленими сторонами в державному та приватному секторах на європейському рівні. У сфері правоохоронних органів у 2013 році в рамках Європолу було створено Європейський центр боротьби з кіберзлочинністю (EC3), який представлятиме європейський центр боротьби з кіберзлочинністю.

Зокрема, EC3 забезпечуватиме аналіз і розвідку, підтримуватиме розслідування, забезпечуватиме судово-медичну експертизу високого рівня та сприятиме співпраці та обміну інформацією між компетентними органами держав-членів, приватним сектором та іншими зацікавленими сторонами. Європол/EC3 та Євроюст тісно співпрацюватимуть, щоб покращити свій потенціал у боротьбі з кіберзлочинністю. У сфері оборони головну відповідальність за кіберзахист на рівні ЄС несе Європейське оборонне агентство (EDA). Європейська стратегія кібербезпеки підтримує співпрацю та обмін інформацією між цими організаціями, зокрема ENISA, Europol/EC3 та EDA, а також між ними та їхніми партнерами на національному рівні.

Нарешті, на міжнародному рівні Європейська Комісія та держави-члени ведуть діалог з міжнародними партнерами та організаціями, такими як Рада Європи, Організація економічного співробітництва та розвитку (ОЕСР), ОБСЄ, НАТО та ООН. На своєму веб-сайті ENISA надає список національних стратегій кібербезпеки [6].

1.3 Національні стратегії захисту

Правила, запроваджені на європейському рівні, запроваджені в попередніх розділах, були прийняті державами-членами по-різному. У цьому розділі описано кілька прикладів національних стратегій захисту на європейському рівні. Крім того, випадок із США описується як значущий порівняльний приклад нормативних актів, які не повинні відповідати директивам ЄС.

1.3.1 Огляд італійського управління та законодавства

Внутрішні характеристики кібербезпеки вимагають національного стратегічного плану ЗКІ та визначення практик для його реалізації, а також дій у відповідь на загрози за допомогою інструментів, в тому числі організаційних, здатних протистояти новому соціотехнологічному контексту та взаємозалежностям, створеним кіберпростором; іншими словами, управління кібербезпекою. Для досягнення цієї мети необхідне первинне та вторинне регулювання, яке визначає конкретні сфери компетенції, юрисдикційні сфери, залучених суб'єктів, типи та модальності апріорного та апостериорного втручання, таким чином застосовуючи позанаціональні правила. Зростаюча кількість загроз і порушень безпеки вже спричинила значні економічні збитки, тим самим зменшуючи довіру користувачів до використання нових послуг і технологій і перешкоджаючи розвитку електронної комерції та реалізації так званого «цифрового порядку денного» в Італії. У цій сфері Італія демонструє невелику затримку у визначенні управління кібербезпекою. Незважаючи на те, що питання кібербезпеки обговорюється в Італії з початку 2000-х років, значні покращення у визначенні дорожньої карти для впровадження національної стратегії спостерігаються лише нещодавно. Основні віхи, які привели до визначення ролей і відповідальності за захист кібербезпеки Італії, описані в наступному розділі.

Міжміністерським указом від 21.09.1999 було створено робочу групу, до складу якої увійшли представники Міністерства зв'язку (Ministero delle Comunicazioni), юстиції (Ministero della Giustizia) та внутрішніх справ (Ministero dell'Interno), із завданням діяльності в секторі мережевої безпеки та захисту комунікацій як підтримки адміністративного та регуляторного втручання.

Для досягнення поставлених цілей робоча група після аналізу вимог щодо технічної та нормативної підтримки, ресурсів для «безпечного» розвитку телекомунікаційних послуг, характеру відносин між державною адміністрацією та операторами телекомунікацій, в основному стосувалися міжнародно гармонізованих нормативних актів у секторі телекомунікацій, міжнародно гармонізованих.

У 2003 році робочу групу було перетворено на обсерваторію з питань захисту та безпеки мереж і комунікацій (Osservatorio permanente per la sicurezza e la tutela delle reti e delle comunicazioni) в рамках Міністерства економічного розвитку (Ministero dello Sviluppo Economico) з метою врахування технологічної та нормативної еволюції різних аспектів сектору телекомунікацій, приділяючи особливу увагу безпеці. Він постійно інтегрований з представниками Міністерства оборони (Ministero della difesa), Департаменту державної служби (dipartimento per la funzione pubblica), Департаменту інновацій та технологій (dipartimento per l'innovazione e le technologie) та Міністерства Продуктивної діяльності (Ministero delle attività produttive). Обсерваторія, серед іншого, зіграла допоміжну роль, спрямовану на реалізацію Директиви 2002/58/ЕС. Ця директива стосується обробки персональних даних і захисту конфіденційності в секторі електронних комунікацій, а також законодавчого декрету щодо Кодексу електронних комунікацій (Codice delle comunicazioni elettroniche), який був виданий 16.09.2003.

У жовтні 2001 року було створено Технічний міжвідомчий комітет цивільної оборони (Commissione Inter Ministeriale Tecnica della Difesa Civile - CITDC) як допоміжний орган політичного та військового

підрозділів для технічної координації діяльності цивільної оборони у разі криз. Він діє в рамках Департаменту пожежно-рятувальної служби та цивільної оборони (Dipartimento dei Vigili del Fuoco e del Soccorso Pubblico e della Difesa Civile). Він виконує роль оцінки надзвичайних ситуацій і планування заходів, яких необхідно вжити у випадку кризи. Комітет також розглядає інші гіпотези ризику, безпосередньо не пов'язані зі зловмисними діями, які можуть призвести до кризових ситуацій для безперервності влади, а також завдати шкоди населенню та, загалом, безпеці країни.

У березні 2003 року Міністерство інновацій та технологій заснувало Робочу групу з ЗКІІ (англ CIIP), до якої увійшли представники міністерств, що займаються управлінням КІ (внутрішніх справ, інфраструктури, зв'язку тощо), основних приватних провайдерів (ABI, ASI, CESI, GRTN, RFI, Snam Rete Gas, Telecom Italia, Wind), а також дослідницький і академічний світ. У березні 2004 року ця робоча група видала документ «ЗКІІ: ситуація в Італії» [16], в якому звітуються про результати роботи, проведеної протягом попереднього року.

Що стосується аспектів, суворо пов'язаних із ЗКІІ, законодавчий декрет (D.L.) n. 155 від 31/7/05 (Legge Pisanu) надав юрисдикцію МВС, визначивши Поліцію пошти та зв'язку як підрозділ, відповідальний за правоохоронні ініціативи проти кібератак на КІІ. У 2008 році МВС заснувало національний центр із запобігання кіберзлочинності для КІ під назвою Centro Nazionale Anticrimine Informationico per la Protezione delle Infrastrutture Critiche (CNAIPIC) як спеціальний підрозділ у складі Служби поліції пошти та зв'язку [22]. CNAIPIC діє як поліцейський орган для всіх заходів із запобігання, придушення та протидії злочинним діям, скоєним проти різної КІ через кіберпростір. З цією метою CNAIPIC та КІ підтримують виділені та захищені ексклюзивні телематичні канали для взаємного та постійного обміну даними та інформацією, що стосується практики оцінки, запобігання та придушення загроз та кіберзлочинності.

Крім того, «Відділ аналізу кіберзлочинності» (Unità d'analisi del crimine informatico -UACI) був створений для вивчення та аналізу явища кіберзлочинності у партнерстві з великими італійськими університетами. Територіальні підрозділи мають організацію, подібну до цієї служби, з більш оперативним профілем і більшою мірою прив'язаною до своєї юрисдикції. Ці відділи розглядають судові справи та надзвичайні ситуації, що виникають у зв'язку з повідомленнями громадян на гарячі лінії поліції.

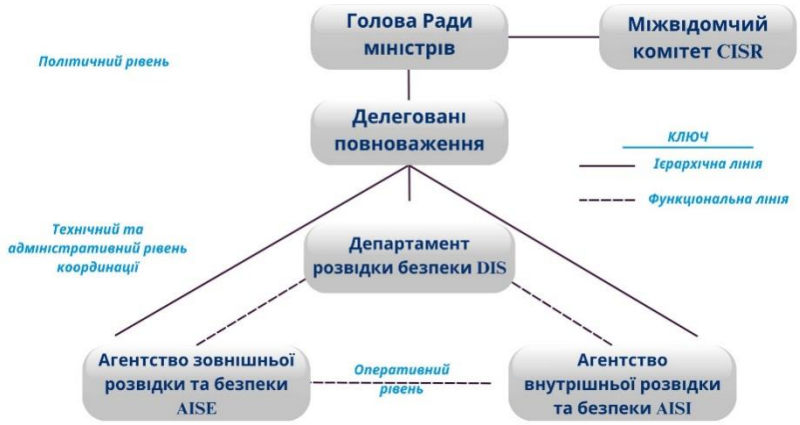
З метою підвищення ефективності стратегій боротьби з кіберзлочинністю поліція разом із деякими своїми представниками бере участь у постійних робочих групах, створених урядом або міжнародними організаціями, включаючи Міжміністерську групу з мережевої безпеки (Gruppo Interministeriale per la sicurezza delle reti), G8, Європейське співтовариство, Рада Європи, OCSE, Інтерпол, Європол. Крім того, він співпрацює з інституціями (включно з Міністерством зв'язку та Управлінням зв'язку) та приватними операторами, які займаються зв'язком загалом.

Парламентський комітет з безпеки Республіки (Comitato parlamentare per la sicurezza della Repubblica) (COPASIR), заснований законом № 124 від 3.08.2007, має на меті забезпечити систематичне та постійне забезпечення того, щоб діяльність системи інформаційної безпеки здійснюється відповідно до Конституції та законів, у виключних інтересах і для захисту Республіки та її установ. COPASIR має важливі консультативні повноваження; зокрема, парламентський орган зобов'язаний висловити свою необов'язкову думку щодо кожної нормативної схеми щодо організації та управління суб'єктами, пов'язаними з конфіденційною інформацією та справами безпеки. COPASIR та його президент є одержувачами інформаційного потоку від уряду та розвідувальних агенцій, і в такій сфері вони офіційно зобов'язані заздалегідь інформувати президента COPASIR про призначення директорів і віце-директорів. DIS, AISE та AISI. COPASIR повідомляє прем'єр-міністра та президентів верхньої та нижньої палати про

незаконну або нерегулярну поведінку, виявлену на основі проведеного контролю. Окрім річного звіту, COPASIR також може подавати до парламенту термінові звіти.

Той самий закон (124/2007) глибоко змінив Систему розвідки безпеки Республіки (Sistema di informazione per la sicurezza della Repubblica) (Мал. 1.2), яка наразі складається з комплексу органів, які мають завдання: забезпечення інформаційної діяльності для безпеки з метою захисту Республіки від кожного виду ризику та загрози як всередині країни, так і за її межами.

Мал. 1.2: Організація розвідувальної системи безпеки Республіки (www.sicurezzanazionale.gov.it).



Лінія дій щодо італійської кібербезпеки.

Відповідно до Італійського цифрового порядку денного (*Agenda Digitale Italiana*), національна стратегія кібербезпеки планує діяти в наступних сферах:

- ***Навчання громадян і підприємств***: підвищення обізнаності громадян, бізнесу та промисловості про серйозні ризики, пов'язані з використанням Інтернету (напр., британська ініціатива «Get Safe Online», державно-приватна онлайн-кампанія з підвищення обізнаності);

- ***Удосконалення інструментів виявлення та порівняння загроз***: розробити інструменти (організації, процеси, законодавство та програми), здатні виявляти та порівнювати потенційні загрози (напр., Національний центр кібербезпеки Нідерландів запровадить інструменти для підвищення обізнаності та класифікації загроз і вразливостей через публічно-приватний обмін інформацією);

- ***Сприяння освіті***: створення освітних шляхів, що здатні забезпечити необхідні компетенції з молодшого шкільного рівня (напр., США опублікували проєкт «Національної ініціативи щодо стратегічного плану освіти в галузі кібербезпеки», який окреслює освітні кроки, починаючи з початкової школи);

- ***Посилення державно-приватної співпраці***: створення механізмів обговорення, обміну та координації між державним і приватним секторами, особливо щодо ЗКІ (напр., Німеччина у своїй стратегії передбачила Національну раду з кібербезпеки, де представники приватного сектору запрошені до участі як асоційовані члени);

- ***Посилення механізмів міжнародної співпраці***: залучення до міжнародних форумів для обговорення стандартів, політики та міжнародних принципів кібербезпеки (напр., стратегія Чеської Республіки передбачає активну участь у форумах ЄС та НАТО);

- ***Створення та посилення механізмів реагування на інциденти***: необхідно посилити шляхом створення національних CERT (комп'ютерної групи реагування на надзвичайні ситуації) і створення спеціалізованих структур, здатних реагувати на кібератаки та інциденти в межах національних кордонів і здатних взаємодіяти з відповідними центрами на міжнародному рівні;

- ***Визначення стандарту*** для управління цифровими ідентифікаторами, а також керівних принципів для створення федеральної системи на національному та міжнародному рівнях, здатної задовольнити щоденні потреби цифрових громадян, включаючи покращену безпеку платіжних систем Інтернету;

- ***Стимулювання зростання італійської галузі кібербезпеки***, що стосується як технологій/послуг, так і навичок і талантів. Це дозволить не тільки розвивати та підтримувати спеціалізовані компетенції, але й залучатиме таланти та експертів з інших країн.

1.3.2 Ситуація в інших країнах

Німеччина. Федеральний уряд Німеччини робить значний внесок у кібербезпеку, підтримуючи та сприяючи економічному та соціальному процвітанню Німеччини. Остання німецька стратегія 2011 року в основному зосереджена на цивільних підходах і заходах. Вони доповнюються заходами, вжитими збройними силами (Бундесвером), спрямованими на захист своїх можливостей, і заходами, що базуються на мандатах щодо включення кібербезпеки як частини стратегії превентивної безпеки. Глобальний характер інформаційно-комунікаційних технологій підвищує необхідність міжнародного бачення та координації аспектів політики безпеки з метою посилення можливостей міжнародного співтовариства в галузі кібербезпеки. З цією метою Німеччина співпрацює з ООН, ЄС, Радою Європи, НАТО, G8, OCSE та іншими міжнародними організаціями.

Німецький стратегічний план складається з 10 конкретних стратегічних сфер:

1. *Захист КІІ* – є центральним компонентом майже всієї КІ. Таким чином, захист такої інфраструктури є основною метою кібербезпеки. З метою підтримки захисту КІІ планом враховано впровадження нових технологій. Співпраця та обмін інформацією між державним і приватним секторами також є пріоритетом.

2. *Безпека ІТ-систем* – Німеччина прагне підтримувати безпеку ІТ-систем за допомогою інформаційного втручання, надавати громадянам, малому та середньому бізнесу послідовну інформацію щодо ризиків, пов'язаних з використанням ІТ-систем, а також сприяти використанню основних функцій безпеки, таких як державне сертифіковане електронне підтвердження особи та надсилання електронної пошти[1]. Крім того, постачальники повинні будуть надати клієнтам базову колекцію продуктів і послуг безпеки, і на них може бути покладено більшу відповідальність.

3. *Посилення ІТ-безпеки в державному управлінні* – Німецький план посилення ІТ-безпеки в державному управлінні передбачає створення загальної, єдиної та безпечної мережевої інфраструктури у федеральній адміністрації, яка буде основою для електронного аудіо- та передачі даних.

4. *Створення Національного центру кіберреагування (НЦК)* – НЦК має на меті оптимізувати співпрацю між державними органами, таким чином покращуючи реагування на ІТ-інциденти. Обмін інформацією про вразливості, форми атак і профілі зловмисників дозволяє НЦК аналізувати ІТ-інциденти та надавати рекомендації щодо дій, яких необхідно вжити у відповідь на інциденти. Щоб сприяти готовності до ІТ-інцидентів, НЦК надаватиме рекомендації до Національної ради з кібербезпеки як регулярно, так і в разі виникнення конкретних інцидентів. У разі інцидентів кібербезпеки, які досягають рівня кризи, НЦК безпосередньо інформуватиме персонал управління кризою на чолі з державним секретарем Федерального МВС.

5. *Створення Національної ради з кібербезпеки* – Нац рада з кібербезпеки координуватиме превентивні інструменти та міждисциплінарні підходи до кібербезпеки державного та приватного секторів. Кілька міністерств землі та представники федеральних земель (Lãnder) братимуть участь у раді. Представників бізнесу та наукових кіл запрошуватимуть у певних випадках.

6. *Ефективна боротьба зі злочинністю в кіберпросторі* – Стратегічний план Німеччини передбачає зміцнення можливостей у боротьбі з кіберзлочинністю правоохоронних органів, Федерального відомства з інформаційної безпеки та приватного сектору. Щоб боротися з глобальною кіберзлочинністю, Німеччина докладе зусиль для досягнення глобальної гармонізації кримінального права на основі Конвенції Ради Європи про кіберзлочинність, а також перевірить, чи слід ухвалювати нові конвенції щодо кіберзлочинності на рівні ООН.

7. *Ефективні скоординовані дії для забезпечення кібербезпеки в Європі та світі* – Федеральний уряд Німеччини визнає важливість відповідності європейським і міжнародним стандартам у сфері кібербезпеки. На рівні ЄС Німеччина вживає заходів, заснованих на розширенні та помірному розширенні повноважень ENISA. Німеччина має намір сформувати свою зовнішню політику кібербезпеки таким чином, щоб інтереси та ідеї Німеччини щодо кібербезпеки відстоювали міжнародні організації, такі як ООН, ОБСЄ, Рада Європи, ОЕСР і НАТО.

8. *Використання надійних і надійних інформаційних технологій* – Враховуючи важливість доступності та надійності ІТ-систем, Німеччина має намір збільшити дослідження безпеки ІТ та ЗКІІ, зокрема, шляхом подальшого розвитку своїх технологій у цих сферах. Крім того, Німеччина схвалює різноманітність технологій, поєднуючи, коли це необхідно, власні ресурси разом із ресурсами своїх партнерів і союзників, віддаючи перевагу використанню технологій, сертифікованих за міжнародними стандартами.

9. *Розвиток персоналу в федеральних органах влади* – Одним із пріоритетів федерального уряду є перевірка того, чи потрібен органам влади додатковий персонал для посилення кібербезпеки. З метою покращення міжвідомчого співробітництва сприятиме обміну персоналом між федеральними органами влади, забезпечуючи відповідні заходи з навчання персоналу.

10. *Інструменти реагування на кібератаки* – Щоб досягти належної готовності до кібератак, уряд Німеччини визнає важливість створення у співпраці з окремими державними органами набору інструментів для ефективного реагування на кібератаки.

Метою уряду Німеччини є стале впровадження цих стратегічних цілей для забезпечення свободи та

процвітання в Німеччині. Технології, що використовуються у сфері IT-безпеки, мають короткі інноваційні цикли. Таким чином, Федеральний уряд Німеччини періодично перевірятиме, чи були досягнуті цілі стратегічного плану, під контролем Національної ради з кібербезпеки, і, якщо необхідно, узгодить їх з національними та міжнародними вимогами.

[1]*De-mail — це державна служба зв'язку Німеччини, подібна до італійської сертифікованої служби електронної пошти (Posta Elettronica CertiFIcata — PEC)*

Об'єднане Королівство. Стратегія Великобританії базується на більш ніж 10-річному розвитку. І-ий крок був зроблений у 2001 році групою безпеки комунікацій-електроніки (CESG). Ця група визнала, що зростання використання онлайн-сервісів потребує розробки заходів безпеки для захисту даних, і рекомендувала призначити центрального спонсора для інформаційного забезпечення державних даних. Таким чином, уряд опублікував свою І-шу національну стратегію в 2004 році, в якій була створена мережа старших власників інформаційних ризиків.

У 2009 році уряд визнав ризик кіберзагроз і опублікував свою І-шу стратегію кібербезпеки. У 2010 році уряд назвав кібератаки ключовим ризиком для національної безпеки та оголосив про виділення 650 млн фунтів для 4-річної Національної програми кібербезпеки. З 2011 року за кібербезпеку відповідає Офіс Кабміну. Остання стратегія була опублікована в 2011 році. У ній зазначено, як уряд планує реалізувати Національну програму кібербезпеки до 2015 року. 4 цілі, які характеризують стратегію:

- Боротьба з кіберзлочинністю та перетворення Великобританії на 1 з найбезпечніших місць у світі для ведення бізнесу;

- Зробити Великобританію більш стійкою до кібератак і краще захищати свої інтереси в кіберпросторі;

- Допомога у формуванні відкритого, стабільного та активного кіберпростору, яким громадськість Великобританії може безпечно користуватися та який підтримує відкрите суспільство;

- Розвиток наскрізних знань, навичок і можливостей Великобританії для підтримки всіх цілей кібербезпеки.

6 центральних департаментів і 9 державних організацій відповідають за надання послуг: МВС; Агентство з боротьби з серйозною організованою злочинністю; Вплив на дітей та захист в Інтернеті; Центральний відділ поліції з боротьби з електронною злочинністю; Поліція; Національне управління з боротьби з шахрайством; Департамент підприємницької діяльності, інновацій та навичок; Рада технологічної стратегії; Торгівля та інвестиції Великобританії; Кабмін; Агентства розвідки та безпеки; Міністерство оборони; Департамент культури, ЗМІ та спорту; МЗС і у справах Співдружності.

Щодо ЗКІ у Сполученому Королівстві все делеговано Центру ЗНКІ (CPNI). ЗНКІ (CPNI) захищає національну безпеку, надаючи поради щодо захисту персоналу, фізичної безпеки та кібербезпеки. ЗНКІ (CPNI) особливо враховує політичний контекст. Політичні міркування є одним із будівельних блоків механізму захисних порад щодо безпеки, які надає ЗНКІ (CPNI). Зокрема, кілька державних політик впливають на роботу ЗНКІ (CPNI):

- ***Стратегія нац безпеки***: встановлює стратегії, спрямовані на ефективне та швидке реагування на

загрози безпеці, такі як: терористичні акти, атаки на кіберпростір Сполученого Королівства, стихійні аварії та катастрофи та міжнародні військові кризи, які стосуються Сполученого Королівства та його союзників.

- ***Огляд стратегічної оборони та безпеки***: встановлює, як слід досягати цілей стратегії нац безпеки.
- ***Стратегія боротьби з тероризмом***: стратегія боротьби з тероризмом Сполученого Королівства розроблена в 4 основних напрямках: запобігання, переслідування, захист і підготовка. Робота ЗНКІ (CPNI) належить до категорії «захист», яка спрямована на зменшення вразливості Великобританії до терористичних атак.
- ***Стратегія кібербезпеки*** (як описано вище).
- ***Національний реєстр ризиків***: є загальнодоступною версією конфіденційної національної оцінки ризиків, яка реєструє події, які можуть завдати шкоди людям або майну або призвести до збою в роботі основних послуг. Події класифікуються за 3 категоріями: природні події, великі аварії, зловмисні атаки.
- ***Стійкість інфраструктури до природних небезпек***: щоб підвищити стійкість КІ та основних послуг до збоїв через стихійну небезпеку, Секретаріат цивільних непередбачених ситуацій при Кабміні розробив Програму стійкості КІ (CIRP).

ЗНКІ (CPNI) активно співпрацює з партнерами в державному та приватному секторах. У державному секторі ЗНКІ (CPNI) тісно співпрацює з Національним технічним органом із забезпечення інформації (CESG), а всередині поліції — з Національним офісом безпеки з питань боротьби з тероризмом (NaCTSO) і мережею радників з питань безпеки з питань боротьби з тероризмом (CTSA). Урядові департаменти несуть відповідальність за вжиття відповідних заходів для покращення безпеки у відповідних секторах. Ці відділи також відповідають за визначення КІ у своїх секторах у співпраці з ЗНКІ (CPNI) та галузевими організаціями. Залучені відділи є:

- Департамент бізнесу, інновацій та навичок;
- Департамент охорони здоров'я;
- Департамент у справах громад та місцевого самоврядування;
- Департамент транспорту;
- Домашній офіс;
- Департамент енергетики та зміни клімату;
- Казначейство Її Величини;
- Департамент з питань навколишнього середовища, продовольства та сільських справ та Агентства харчових стандартів;
- Кабінет міністрів.

1. DEFINITIONS AND CONCEPTS

Що стосується кібербезпеки, то в 2010 році уряд Великобританії створив Операційний центр кібербезпеки (CSOC) і Управління кібербезпеки та забезпечення інформації (OCSIA). ЗНКІ (CPNI) співпрацює з CSOC, OCSIA та CESG для реалізації програми кібербезпеки для уряду Великобританії. У приватному секторі ЗНКІ (CPNI) взаємодіє з організаціями, які працюють у національній інфраструктурі. Взаємовідносини, встановлені протягом багатьох років, між консультантами з питань безпеки ЗНКІ (CPNI) та менеджерами з безпеки в кількох секторах дозволяють обмінюватися інформацією між довіреними організаціями та, за необхідності, обмінюватися інформацією про вразливості та ефективними заходами реагування з метою покращення ЗНКІ та приватних організацій. Крім того, ЗНКІ (CPNI) створив партнерську програму Risk Management Delivery Group, яка спрямована на розвиток міцних зв'язків між основними консультаційними партнерами Великобританії.

Франція. Французький президент вперше представив французьку стратегію оборони та національної безпеки у червні 2008 року у французькій Білій книзі з оборони та національної безпеки. Зважаючи на несподівану появу кіберпростору у сфері національної безпеки, у 2009 році уряд створив Французьке агентство мережевої та інформаційної безпеки (Agence nationale de la sécurité des systèmes d'information – ANSSI)[2]. У 2010 році президент вирішив покласти на агентство, крім функції безпеки, відповідальність за захист інформаційних систем. 4 стратегічні цілі, що характеризують французьку стратегію:

- Становлення світової держави кіберзахисту;
- Захист спроможності Франції приймати рішення за допомогою захисту інформації, що стосується її суверенітету;
- Посилення кібербезпеки критичної національної інфраструктури;
- Забезпечення безпеки в кіберпросторі.

Для досягнення цих цілей французька стратегія визначила 7 напрямків діяльності:

- ***Ефективно передбачати та аналізувати середовище, щоб приймати відповідні рішення***. Необхідно слідкувати за останніми технологічними розробками, щоб зрозуміти та передбачити дії державних чи приватних суб'єктів.

- ***Виявляти та блокувати атаки, сповіщати й підтримувати потенційних жертв***. Франція розробляє можливості виявлення атак на інформаційні системи, розгорнуті в мережах міністерства. Це дозволить персоналу бути попередженим, оцінювати характер атак і створювати заходи протидії. ANSSI обладнано операційною кімнатою для вирішення цих завдань.

- ***Збільшувати та увічнювати науково-технічний, промисловий і людський потенціал*** Франції з метою збереження незалежності. Просування досліджень у сфері криптології, формальних методів та інших пов'язаних із безпекою сфер і створення дослідницьких центрів кіберзахисту у співпраці з промисловими партнерами. Для сприяння зміцненню промисловості держава надаватиме стратегічні інвестиційні кошти.

- ***Захист інформаційних систем нації та КІ для забезпечення кращої національної стійкості***. Французьку стратегію щодо продуктів і компонентів безпеки було переосмислено, щоб врахувати приєднання Франції до інтегрованого командування НАТО. Надійні системи аутентифікації будуть

інтегровані в міністерські мережі, що значно вплине на рівень безпеки. Для підвищення безпеки інформаційних систем операторів КІ буде створено державно-приватне партнерство. Оператори отримають користь від інформації, зібраної державою щодо аналізу загроз, і держава зможе забезпечити відповідний рівень захисту інфраструктури, що є вкрай важливим для належної роботи країни.

- ***Адаптувати французьке законодавство з урахуванням технологічних розробок і нових практик***: запровадити нові правила для захисту інформаційних систем і сповіщення державних органів у разі інцидентів щодо операторів електронних комунікацій. Забезпечення виконання Загальних рамок безпеки з метою підвищення рівня захисту інформаційних систем ОДВ.

- ***Розвивати ініціативи міжнародного співробітництва у сферах безпеки інформаційних систем, кіберзахисту та боротьби з кіберзлочинністю*** з метою кращого захисту національних інформаційних систем і сприяння обміну важливими даними (інформація про вразливості, послуги, загрози) шляхом створення широкої мережі іноземні партнери.

- ***Повідомляти, інформувати та підвищувати розуміння населенням Франції масштабів проблем***, пов'язаних із безпекою інформаційних систем, а також забезпечувати обізнаність та мотивацію окремих осіб та організацій. ANSSI проводитиме відповідні комунікаційні кампанії, орієнтовані на широку громадськість і компанії.

США. У травні 2009 року президент Обама оголосив про намір зробити кібербезпеку пріоритетом своєї адміністрації. Це призвело до публікації документа під назвою «Огляд політики кібербезпеки» (CPR). Зокрема, цей документ визначає 10 короткострокових заходів:

- Призначення посадової особи з політики кібербезпеки, відповідальної за координацію національної політики та заходів у сфері кібербезпеки.

- Підготовка до затвердження Президентом оновленої національної стратегії безпеки інформаційно-комунікаційної інфраструктури.

- Визначення кібербезпеки як одного з ключових пріоритетів управління президентом і встановлення показників ефективності.

- Призначення посадової особи з питань конфіденційності та громадянських свобод до Директорату з кібербезпеки NSC.

- Проведення міжвідомчого узгодженого правового аналізу пріоритетних питань кібербезпеки.

- Ініціювання національної просвітницької кампанії для просування кібербезпеки.

- Розробка міжнародної політики кібербезпеки та зміцнення міжнародного партнерства.

- Підготовка плану реагування на інциденти кібербезпеки та початок діалогу для посилення державно-приватного партнерства.

- Розробка основи для стратегій досліджень і розвитку, яка зосереджується на революційних

технологіях, які мають потенціал для підвищення безпеки, надійності, стійкості та надійності цифрової інфраструктури.

- Розробка бачення та стратегії управління ідентифікацією на основі кібербезпеки та використання технологій для покращення конфіденційності для країни.

Досягнення таких цілей має відповідати Комплексній національній ініціативі з кібербезпеки (CNCI) [13], започаткованій президентом Джорджем Бушем у січні 2008 року, яка складається з низки ініціатив, спрямованих на зміцнення кібербезпеки США. Президент Обама встановив, що CNCI має бути включено та розширено в оновлену стратегію національної кібербезпеки, і що вона відіграватиме ключову роль у реалізації 10 цілей. Протягом 14 місяців після випуску CPR було досягнуто багатьох цілей:

- Президент Обама призначив координатора з кібербезпеки на чолі Управління кібербезпеки, створеного в рамках Штабу національної безпеки (NSB). Цей координатор тісно співпрацює з Управлінням управління та бюджету та Управлінням науково-технічної політики.
- Директорат з кібербезпеки розпочав розробку оновленої стратегії кібербезпеки, яка розширює та реалізує стратегію, передбачену CPR та CNCI.
- Запроваджено постійний моніторинг федеральних мереж у реальному часі, що дозволяє швидше виявляти вразливості та ефективніше захищати інфраструктуру.
- Відповідно до CPR, у NSS було призначено посадову особу з питань конфіденційності та громадянських свобод.
- Національна ініціатива з освіти з кібербезпеки (NICE) була запущена для покращення набору, навчання та утримання фахівців з кібербезпеки, підвищення обізнаності громадськості щодо кібербезпеки та покращення освіти з кібербезпеки шляхом розширення освітньої програми CNCI.
- США працюють над посиленням співпраці та діалогу з міжнародними партнерами. У співпраці з країнами-союзниками США взяли на себе провідну роль у міжнародних організаціях, таких як ООН, щоб зробити кібербезпеку міжнародним пріоритетом.
- Національний план реагування на кіберінциденти (NCIRP) був розроблений, щоб забезпечити скоординовану національну реакцію на кіберінциденти.
- Адміністрація розробила стратегію досліджень і розробок, яка базується на 3 основних темах: рухомі цілі (системи, які постійно змінюються, щоб збільшити свою складність, таким чином обмежуючи зловмисників і вразливі місця), спеціально розроблені надійні простори (довірене середовище, яке дозволяє визначення індивідуальних вимог) та кібереконо мічні стимули (стимули до прийняття відповідних рішень кібербезпеки для окремих осіб та організацій).
- Оприлюднено проєкт «Національної стратегії надійних ідентифікаційних даних у кіберпросторі» (NSTIC), спрямованої на зменшення вразливості кібербезпеки за допомогою використання надійних цифрових ідентифікаційних даних.

[2]Decree No. 2009-834 of 7 July 2009 creating the French Network and Information Security Agency* (ANSSI).

Що стосується дорожньої карти США, у лютому 2013 року Президент Обама видав указ про подальше вдосконалення управління кібербезпекою КІ. Метою цього розпорядження є встановлення нового партнерства з власниками та операторами КІ, щоб збільшити обмін інформацією про кібербезпеку та спільно розробити стандарти, засновані на ризиках.

Обмін інформацією з питань кібербезпеки, таких як перенесені та попереджені атаки, загрози та вразливі місця, між державним і приватним секторами є ключовим фактором у процесі вдосконалення, передбаченого указом. Уряд США несе відповідальність за покращення такого обміну інформацією з точки зору обсягу, своєчасності та якості інформації, яка надається приватному сектору, таким чином дозволяючи суб'єктам приватного сектора краще захищатися від кіберзагроз. Згідно з указом, міністр внутрішньої безпеки, генеральний прокурор[3] і директорнаціональної розвідки відповідатимуть за забезпечення своєчасної підготовки конкретних несекретних звітів про кіберзагрози на території США. Крім того, секретні звіти будуть доставлені уповноваженим об'єктам КІ. Міністр внутрішньої безпеки та генеральний прокурор, у координації з директором національної розвідки, відповідатимуть за створення системи відстеження виробництва, розповсюдження та утилізації звітів. Мета полягає в тому, щоб максимально збільшити корисність обміну інформацією, пов'язаною з кіберзагрозами та атаками.

Виконавчий наказ також стосується захисту приватного життя та громадянських свобод. Важливі ролі в цьому контексті виконують Головний інспектор з питань конфіденційності та Офіцер з громадянських прав і громадянських свобод (Департаменту внутрішньої безпеки). Вони несуть відповідальність за оцінку ризиків для конфіденційності та громадянських свобод, пов'язаних із функціями, які виконує Міністерство внутрішньої безпеки, а також за визначення та звіт про способи мінімізації таких ризиків у загальнодоступному звіті, який буде опубліковано протягом 1 року з моменту виконання - тивний порядок. Під час підготовки звіту головний спеціаліст з питань конфіденційності та спеціаліст з питань громадянських прав і громадянських свобод консультуватимуться з Наглядовою радою з питань конфіденційності та громадянських свобод та Управлінням адміністративного управління.

Виконавчий указ, виданий президентом Обамою, також передбачає створення Рамкової програми кібербезпеки, спрямованої на зниження кіберризиків для КІ. Міністр торгівлі керуватиме директором Національного інституту стандартів і технологій у розробці рамок. Структура кібербезпеки включатиме набір стандартів і процедур для узгодження політики, бізнес- і технологічних підходів для кращого протидії кіберризикам. Структура також включатиме якомога більше найкращих галузевих практик і буде доступна в остаточній версії до лютого 2014 року. Міністр внутрішньої безпеки підтримуватиме прийняття структури власниками та операторами КІ та іншими зацікавленими особами.

1.4 Основні питання безпеки критичних інфраструктур

КІ кожної країни, починаючи від нафтопроводів і закінчуючи електричними мережами, від газових до водопровідних мереж, від транспорту до фінансових/банківських систем і закінчуючи державним управлінням, все частіше управляється електронним способом. Поступове запровадження систем керування мережею, моніторингу та контролю, а також взаємозалежність, що виникла, безсумнівно, підвищили рівень продуктивності такої інфраструктури, але це також дозволило отримати доступ кіберзлочинцям із подальшими кібератаками та збільшенням продуктивності ризик ефекту доміно. Таким чином, останніми роками сценарій стає дедалі складнішим, оскільки впровадження передових технологій поряд із традиційними загрозами додає нові джерела потенційного ризику. Ефективний

захист інфраструктури включає ідентифікацію загроз, зменшення вразливості та ідентифікацію джерела атаки або джерела пошкодження. Ця діяльність спрямована на мінімізацію простою служби та обмеження збитків.

Зазвичай кібератака запускається, щоб паралізувати роботу КІ або викрасти її інформаційні активи. Важливо оцінити можливі цілі атаки, щоб оцінити наслідки, також з точки зору часу, необхідного для відновлення нормальної поведінки (стійкості). Кіберзагроза є важливим викликом для національної економічної системи як через те, що вона стосується цифрової сфери, так і через її транснаціональний характер і, отже, через потенційні наслідки, які вона може спричинити. Зрозуміло, що коли цілями атак є КІ та системи оповіщення, наслідки для всього суспільства можуть бути катастрофічними. У світлі цього міркування та усвідомлення того, що це середовище постійно змінюється, необхідно терміново втрутитися на національному рівні та за його межами проти всіх форм кіберзлочинності, яка становить зростаючу загрозу для критичної ін, суспільства, бізнесу та громадян.

У цьому контексті ще один помітний аспект представлений взаємодією та взаємозалежністю між КІ. Розуміння та аналіз взаємозалежностей є надзвичайно важливими, оскільки вони можуть бути джерелом загрози для систем і сприяти невизначеності ризику з подальшим збільшенням швидкості та розміру втрат після виникнення збоїв.

Взаємозалежність — це двонаправлений зв’язок між 2 інфраструктурами, за допомогою якого стан кожної інфраструктури впливає або корелюється зі станом іншої [155]. Взаємозалежності інфраструктури можуть бути охарактеризовані відповідно до різних вимірів, щоб полегшити їх ідентифікацію, розуміння та аналіз. У [155] було визначено шість вимірів, які включають: a) зв’язки між інфраструктурою та їхній вплив на поведінку реагування (слабка чи жорстка, негнучка чи адаптивна), б) стан роботи (нормальний, напружений, аварійний, ремонт), c) тип відмови, що впливає на інфраструктуру (загальна причина, каскадна, ескалація), і d) типи взаємозалежностей. Зосереджуючись на типі взаємозалежностей, у [155] виділено 4 класи:

- ***Фізичні***: виникають через фізичні зв'язки або зв'язки між елементами інфраструктури. У цьому контексті збої та збурення в 1 інфраструктурі можуть поширюватися на іншу.
- ***Кібернетичні***: виникають, коли стан інфраструктури залежить від інформації, що передається через інформаційну інфраструктуру. Такі взаємозалежності є результатом збільшення використання комп’ютерних інформаційних систем, таких як системи SCADA, для підтримки діяльності з контролю, моніторингу та управління.
- ***Географічні:*** існують між 2 інфраструктурами, коли локальна екологічна подія може спричинити зміни стану в обох. Як правило, це відбувається, коли елементи інфраструктури знаходяться в безпосередній просторовій близькості.
- ***Логічні***: об’єднують усі взаємозалежності, які не є фізичними, кібернетичними чи географічними, спричинені, наприклад, нормативними, правовими чи політичними обмеженнями.

4 типи взаємозалежностей не виключають один одного, хоча кожен з них має свої особливості. У літературі також були запропоновані інші класифікації [124, 114, 150]. Наприклад, класифікація, запропонована в [124], розглядає як залучені системи, так і їхні потенційні взаємозв’язки, які характеризуються 2 ключовими факторами: i) характерний тип зв’язку, який визначає, на які елементи систем впливає: фізичний, логічний, людський/організаційний; ii) рівень взаємодії: структурний, функціональний, поведінковий.

[3]У федеральному уряді Сполучених Штатів Генеральний прокурор є членом Кабінету міністрів і як голова Міністерства юстиції є вищим співробітником правоохоронних органів і юристом уряду (Вікіпедія).

1.4. Basic Security Issues of Critical Infrastructures

Як обговорювалося в [59], основна частина дискусій і досліджень КІ зосереджена навколо більш класичної енергетичної інфраструктури. Однак КІІ може бути важливим джерелом взаємозалежностей через їхню роль у центрі іншої інфраструктури та властиву внутрішню складність через багато залучених підсекторів (включаючи інформаційні системи та мережевий захист, контрольно-вимірювальні прилади та контроль), систем (SCADA), фіксованого та мобільного зв'язку). Насправді, згідно з визначенням OECP, КІІ складається з тих інформаційно-комунікаційних технологій, мереж, послуг і активів, які, у разі порушення або знищення, або (1) мають серйозний вплив на здоров'я, безпеку або економічного добробуту громадян чи ефективного функціонування уряду, або (2) призводить до серйозних порушень функціонування КІ, яку він підтримує. Додаткова складність з точки зору взаємозалежностей виникає при класифікації інформаційної інфраструктури у 2 вимірах: 1) сервіс-орієнтоване уявлення та 2) інформація та дані. Перше стосується надання послуг кінцевим користувачам, а друге – надання інформації та даних для забезпечення правильного та регулярного функціонування послуг.

Хоча інтеграція КІ та її синергетичне використання, безсумнівно, забезпечує цінні переваги з точки зору ефективності, якості обслуговування та зниження витрат, взаємозалежності збільшують вразливість відповідної інфраструктури, оскільки вони породжують численні канали поширення помилок від однієї інфраструктури до іншої, що збільшує їх уразливість як випадковими, так і зловмисними загрозами. Отже, вплив збоїв компонентів інфраструктури та їх серйозність можуть бути посилені та, як правило, набагато вищі та важче передбачити, порівняно з збоями, обмеженими окремою інфраструктурою. Як повідомляється в [151], типові відключення електроенергії можуть бути викликані виходом з ладу одного елемента передачі (або генерації), яким не керують належним чином дії автоматичного керування або втручання оператора, що поступово призводить до каскадних відключень і, врешті-решт, до збою мережі. всю систему. Приклади каскадних ефектів від взаємозалежностей інфраструктури, що призводять до катастрофічних подій, на численні інфраструктури, які, можливо, охоплюють широкі географічні території, описані в [151, 46].

Глава 2

Довідкова інформація про загрози, уразливості та випадкові збої

Розвиток ІКТ зробив можливим і зручним дистанційне керування КІ (Інтернет). Тому індустрії та уряди поступово впроваджують ІТ-системи для консолідації роботи КІ. У результаті КІ та ІТ-системи об’єдналися. Це викликає занепокоєння щодо безпеки (і загрози), оскільки два раніше ізольовані світи, Інтернет і системи СІ, тепер взаємопов’язані. Цікаво, що Інтернет сам по собі є базовим, критичним активом сучасних КІ, оскільки їхні системи управління часто розподілені у віддалених місцях, підключених до Інтернету. Ця сильна кореляція між КІ та їхньою ІТ відбувається за рахунок збільшення складності та, як наслідок, збільшення ризиків випадкових збоїв. Тут важливо зазначити, що правильне керування незловмисними помилками є таким же важливим, як і керування ризиками безпеки. Насправді ці два аспекти тісно пов’язані між собою і завжди повинні розглядатися разом під час планування захисту КІ. У цьому розділі ми повідомляємо про декілька випадків випадкових збоїв та їхніх наслідків, які спостерігалися в реальній КІ протягом останніх десятиліть, приділяючи особливу увагу кібераспектам. Решта цієї глави організована таким чином: спочатку основні загрози (розділ 2.1) і мотиви, що стоять за ними, уразливості (розділ 2.2), які роблять деякі атаки можливими (розділ 2.3), і поточні підходи до виправлення (розділ 2.4).) досліджуються. Потім у розділі описуються поточні випадкові загрози, яким можуть наражатися КІ.

2.1 Загрози

Добре відомі загрози, такі як зловмисне програмне забезпечення або атаки на відмову в обслуговуванні, які впливають на безпеку підключених до Інтернету пристроїв, також стали загрозами для КІ. На відміну від інших пристроїв, підключених до Інтернету (ПК, мобільних пристроїв, серверів), КІ можуть виконувати реальні дії, які в кінцевому підсумку можуть вплинути на фізичне середовище. Це створює серйозні ризики для безпеки, з можливістю втрати виробництва, пошкодження обладнання, крадіжки інформації та навіть втрати людського життя. Однак, здається, що, всупереч жахливим прогнозам, суб’єкти, які стоять за подіями, представленими в новинах як «кібератаки», досліджують, не завдаючи навмисної шкоди, як описано в розділі 2.3.1. Однак у цьому пункті щось може змінитися, як описано в Розділі 2.3.2.

Решта цього розділу досліджує суб'єкти та їхні мотиви для нападу на КІ.

2.1.1 Суб'єкти

Одна з причин, чому безпека КІ є складною та актуальною проблемою, полягає в тому, що існує кілька суб'єктів, які становлять загрозу для КІ, можливо, більшу, ніж у традиційних ІТ-системах.

Нижче наведено неповний широкий перелік класів суб'єктів у порядку важливості:

Національні держави - важлива нова група суб'єктів у ландшафті кібератак проти КІ. Їх важливість випливає з того факту, що КІ є відповідними цілями в сучасній кібервійні. Як описано в розділах 2.3.1 і 2.3.2, атаки на КІ або цільові цілі можуть бути політично або економічно мотивованими. Важливу роль у цьому відіграють національні держави. Розширення цієї категорії суб'єктів включає зловмисників, яких спонсорують національні держави, тобто зовнішній суб'єкт, якому платять або підтримують офіси національних держав, щоб скомпрометувати КІ іншої країни.

Недержавні організовані групи загроз - «кібертерористи», також є тривожною загрозою. Потенціал для асиметричної війни випливає з легкості атаки на КІ за допомогою засобів кібервійни. Атака, описана в Розділі 2.3.2, хоча й не може бути пов'язана з терористичною групою з певністю, є прикладом того, як може виглядати організована терористична атака на інфраструктуру.

Хактивісти останнім часом привертають увагу. Термін «хактивіст» стосується зловмисника, у багатьох випадках з обмеженими технічними навичками, який покладається на готові до використання набори та служби атаки, або навіть сторонні бот-мережі, щоб завдати шкоди системі, наприклад, відмова в обслуговуванні, порча як засіб протесту. Протести часто мають політичну мотивацію. Незважаючи на те, що вони мають інші мотиви, ніж національні держави, хактивісти також бачать КІ як привабливу мішень у своїх кампаніях.

Зловмисники, орієнтовані на бізнес відносяться до більш традиційної категорії зловмисників (тобто тих, хто запускає атаку типу «відмова в обслуговуванні» на веб-сайт конкурента). У ландшафті кіберфізичних систем зловмисники, вмотивовані бізнесом, зацікавлені у зловживанні проти контрольованих конкурентами КІ, щоб завдати конкретної шкоди та отримати бізнес-переваги.

Звичайні зловмисники, такі як script kiddies, які в минулому запускали загальнодоступний експлойт проти випадкового веб-сайту без реальної мотивації, набувають набагато більшого значення, якщо розглядати їх у контексті КІ. Незважаючи на те, що звичайні зловмисники зазвичай не мають технічних навичок або не мають таких навичок, атаки на КІ, що виходять в Інтернет (SHODAN [11]), можуть завдати серйозної шкоди, набагато більшої, ніж у випадку простої ІТ-системи. (веб-сайт).

Важливо зазначити, що хактивісти, бізнес-орієнтовані нападники та випадкові нападники також можуть бути терпимими до національних держав як союзників у війні низької інтенсивності проти супротивної нації.

2.1.1 Мотивація та цілі

Вищезазначені суб'єкти керуються 2 широкими категоріями мотивацій.

Політична, стратегічна війна. З (дефіцитної) кількості достовірної інформації, яка поширюється щодо атак на КІ, можна зробити висновок, що більшість атак мають за собою військові або стратегічні мотиви. Найбільш відомі та нещодавні випадки – це Stuxnet (описано в розділі 2.3.1), Aramco (описано в розділі 2.3.2) і Duqu. Інший вид атак мав на меті вилучення розвідувальних даних або секретної інформації. Наразі неможливо з упевненістю сказати, якою буде кінцева використання такої інформації; однак можна стверджувати, що основні мотиви мають політичний характер. Такі суб'єкти, як національні держави та хактивісти, потрапляють до цієї категорії.

Фінансова. Ділові особи, орієнтовані на бізнес і національні держави, також керуються економічними причинами. Ця категорія мотивації також існувала до того, як КІ стали привабливою та чутливою ціллю. Однак використання цінних КІ може призвести до значно більшого фінансового впливу, ніж використання традиційних ІТ-систем.

2.2 Вразливості

КІ складаються з критичних компонентів. Кожен компонент необхідно проаналізувати з точки зору можливих ризиків і аспектів безпеки. Компоненти, призначені для роботи в критично важливих для безпеки середовищах, як правило, розроблені як безвідмовні, але зловмисники можуть використати вразливі місця в безпеці, щоб перешкодити механізмам безпеки.

Сучасні КІ мають різні класи вразливостей. Як пояснюється в Розділі 2.2.1, окрім логічної та конструктивної вразливості через збільшення зв’язку та відкритого дизайну цієї мережевої інфраструктури, використання комерційних готових компонентів (COTS), які не були створені за допомогою з урахуванням безпеки, збільшує поверхню атаки. Крім того, як описано в Розділі 2.2.2, прикладний рівень також виявляє вразливості і, що більш важливо, не має функцій безпеки.

2.2.1 Рівень мережі та інфраструктури

Оскільки КІ контролюються декількома інсталяціями взаємопов’язаних мережевих систем, рівень інфраструктури є важливою проблемою для забезпечення їхньої кібербезпеки. Через кілька факторів, які пояснюються нижче, такі шари зазвичай особливо вразливі.

Збільшення можливостей підключення. До недавнього часу системи керування були електронно ізольованими («повітряними проміжками») від усіх інших мереж. Тому промислова безпека забезпечувалася здебільшого за допомогою фізичної безпеки, щоб зловмисники не мали доступу до них [129, 160]. У наш час зростаючі вимоги промисловості до посиленого зв’язку між виробничими цехами та корпоративними мережами перетворили просту ізольовану мережу керування на члена складної міжмережі, такої як Інтернет.

Відкритий дизайн і використання компонентів COTS. Раніше системи керування базувалися на власних рішеннях, які забезпечували слабку форму безпеки через невідомість. Протягом багатьох років оператори КІ, а також індустрія автоматизації в цілому, відійшли від власних стандартів для протоколів зв’язку SCADA до відкритих міжнародних стандартів, таких як Ethernet або TCP/IP, а також апаратних і програмних компонентів COTS.

Першим результатом цього є те, що раніше поширене переконання про те, що

зловмисникам буде важко отримати доступ до інформації про мережі систем контролю - загальний захист, "хакери не знають наших систем" - більше не відповідає дійсності [168]. Слід зауважити, однак, що покладатися на власні протоколи та системи для забезпечення певної форми захисту було досить неправильним уявленням із самого початку, оскільки такі незрозумілі протоколи та пристрої зазвичай забезпечували дуже мало вбудованої безпеки.

Перехід систем, таких як SCADA, на TCP/IP полегшує взаємозв'язки між мережами SCADA та корпоративною інфраструктурою ІКТ [139]. Перетворення на стандартні протоколи часто відбувається шляхом інкапсуляції встановлених протоколів на основі послідовної лінії в пакет TCP. Багато з цих протоколів відмовляються від будь-яких суворих зв'язків головний/підлеглий, які традиційно спостерігаються в мережах SCADA, і пристрої, розроблені для цих мереж, часто надають додаткові інтерфейси прикладного рівня, окрім протоколу обміну повідомленнями SCADA. Вони можуть включати можливості веб-інтерфейсу, які в поєднанні з інтеграцією в корпоративну мережу дозволяють зручно збирати виробничу інформацію для управління на вищому рівні. Звичайно, включення цих служб робить будь-які пристрої в мережі SCADA, які їх підтримують, вразливими до популярних атак на прикладному рівні та TCP/IP. Навіть якщо це може бути зручним і економічно ефективним з операційної точки зору, ця тенденція викликає серйозні проблеми безпеки. Фактично, раніше незахищені протоколи SCADA можуть бути серйозно піддані атакам на носій TCP/IP. Крім того, атаки на корпоративну мережу можуть потім проникнути в систему SCADA і серйозно загрожувати контрольованому процесу.

Компоненти COTS також дозволяють заощадити кошти та скоротити час розробки, але вони не розроблені з урахуванням безпеки чи безпеки, тому пропонують спокусливу мішень для атаки. Будучи широко встановленим, база знань про легкодоступні атаки для такої системи, безумовно, ширша.

Бездротові сенсорні мережі (Wireless sensor networks). Захист КІ потребує механізмів моніторингу для виявлення збоїв і атак якомога раніше. Оскільки багато КІ мають великий географічний діапазон, захист КІ потребує механізмів моніторингу, які добре масштабуються. У цьому контексті бездротові сенсорні мережі (WSN) природно виникають як потенційне рішення. Наприклад, застосування датчиків для моніторингу структурного стану ліній електропередач є важливим способом зниження вразливості енергосистеми [116]. WSN можна відносно легко розгорнути у великому масштабі, і оскільки вони зазвичай створюються з недорогих пристроїв, вони можуть надавати послуги моніторингу економічно ефективним способом, оскільки не потребують додаткової інфраструктури. Крім того, розподілена природа WSN підвищує живучість мережі в критичних ситуаціях, тому що великомасштабна WSN з набагато меншою ймовірністю постраждає від збоїв або атак. У дуже критичних ситуаціях WSN можуть надати достатньо інформації про КІ, щоб допомогти оператору запобігти подальшому пошкодженню та почати процес відновлення. Однак має бути зрозуміло, що корисність WSN для захисту КІ в першу чергу визначається надійністю самого WSN [62]. WSN, який не повідомляє про несправний стан, не дозволяє оператору КІ виконувати відповідне технічне обслуговування, яке може вирішити проблему до того, як її наслідки вплинуть на КІ. З іншого боку, WSN, який повідомляє про забагато хибних спрацьовувань, призведе до марної витрати часу та ресурсів і поставить під загрозу користь від використання WSN.

Безпека в WSN є більш складною довгостроковою проблемою, ніж у традиційних розподілених системах [64], з різних причин. По-перше, WSN зазвичай встановлюються в неконтрольованих,

можливо ворожих, середовищах, які може бути важко захистити фізично, особливо в географічно великих розгортаннях або в несприятливих умовах для людей. Крім того, може бути економічно недоцільним зробити всі вузли стійкими до втручання. Таким чином, не можна виключити, що зловмисник може захопити та скомпрометувати вузли, таким чином змінюючи їх поведінку та потенційно впроваджуючи підроблені повідомлення в мережу.

2.2.2 SCADA/ICS та вбудовані пристрої

Однією з головних вразливостей SCADA та промислових систем управління є відсутність функцій безпеки в протоколах, які вони використовують. Як уже згадувалося, система SCADA еволюціонувала від фізичної та логічної відокремленості від інших мереж до взаємозв'язку та переходу на стандартні та відкриті протоколи [73]. Звичайно, це змінило ландшафт загроз і виявило такі вразливості, як описані нижче.

Відсутність засобів автентифікації та авторизації. Відсутність належних схем автентифікації та авторизації може дозволити несанкціонованому зловмиснику створювати помилкові повідомлення керування, таким чином викликаючи серйозні занепокоєння щодо правильної роботи системи та, можливо, призводячи до драматичних наслідків для громадської безпеки та здоров'я [105]. Ця ситуація демонструє, що системи SCADA повинні підтримувати ключові властивості безпеки, такі як автентифікація, авторизація, конфіденційність, цілісність, доступність і неспростовність.

У 2010 році команда реагування на надзвичайні ситуації в області промислових систем управління США (ICS-CERT) опублікувала попередження про те, що кілька дослідників безпеки успішно використали пошукову систему SHODAN [11] для виявлення систем SCADA, що виходять в Інтернет, які використовували незахищену автентифікацію та авторизацію. механізми [23]. Попередження не тільки продемонструвало, що потенційно незахищені системи управління легко доступні в Інтернеті, але також і те, що завдяки використанню таких інструментів, як SHODAN, зусилля та ресурси, необхідні для їх ідентифікації, були значно скорочені.

Відсутність механізмів захисту протоколу. Іншим джерелом уразливості систем управління є програмні помилки в пристроях SCADA. Навіть помилка підтвердження введення може зробити КІ вразливим до атак. Різні експерименти з тестуванням нечіткості продемонстрували, як навмисно неправильно сформовані вхідні дані можуть бути використані для успішного збою обладнання SCADA [83, 162]. З цієї причини захист систем SCADA вимагає ретельного тестування на вразливості програмного забезпечення. Однак такий тип тестування може бути проблемним: розробники SCADA зазвичай погано розуміють уразливості, тоді як зовнішні експерти з безпеки не мають необхідних знань і ресурсів SCADA для проведення ретельних тестів.

Безпека базових вбудованих пристроїв. Необхідно також враховувати безпеку різних вбудованих пристроїв, які складають систему керування. Захист окремих пристроїв може додатково підвищити загальну безпеку системи. Фактично, це може допомогти підтримати певні вимоги безпеки, які одні програми реального часу ніколи не зможуть вирішити [105].

Крім того, вбудовані пристрої можуть виявляти певні вразливості, які, якщо їх не усунути, можуть бути використані для компрометації всієї системи. Це особливо важливий аспект, оскільки безпека вбудованих пристроїв зазвичай ігнорується, оскільки такими пристроями не керують, як звичайними комп'ютерами. Наприклад, як показано в [149], незахищена утиліта оновлення мікропрограми в польових пристроях SCADA може бути використана зловмисником для віддаленої інсталяції шкідливої мікропрограми. Таким чином, зловмисник матиме повний контроль над функціональними можливостями пристрою та його взаємодією з рештою системи,

таким чином серйозно загрожуючи всій КІ.

2.1.1 Додатки

На прикладному рівні кілька вразливостей можуть вражати КІ, зокрема через їх розподілену природу.

Розглянемо, наприклад, де розгортається програма і де вона виконується. У розподіленій системі додаток може бути розгорнуто як унікальний фрагмент програмного забезпечення, що виконується унікальною довіреною платформою, або його можна розгорнути на різних платформах як окремі фрагменти коду, які можуть спілкуватися один з одним. Це призводить до можливих порушень безпеки. Обмін повідомленнями між частинами коду, розгорнутими на різних компонентах системи, має регулюватися таким чином, щоб жодна інформація не була втрачена чи виточена. Таким чином, канали мають бути захищені від усіх можливих атак (напр., людина посередині, скомпрометований датчик), щоб уникнути використання скомпрометованої інформації. Крім того, кожен компонент не може контролювати кожну частину коду, що виконується іншим компонентом системи. Ці 2 аспекти призводять до необхідності мати модель довіри для управління довірчими відносинами між компонентами КІ. Розподілені середовища не гарантують, що надана інформація є справжньою. Для забезпечення певних гарантій безпеки потрібна інфраструктура довірчого управління.

Інші загрози безпеці пов'язані з взаємозалежністю між компонентами КІ. Дійсно, взаємозалежність може бути використана для скоординованої атаки на систему кількома зловмисниками, розташованими в різних стратегічних точках інфраструктури. Насправді можна розрізнити та класифікувати атаки на 2 основні класи: атаки, які здійснюються окремо одним компонентом, і атаки, які здійснюються декількома компонентами, які співпрацюють, щоб порушити систему.

2.1.1 Бізнес-рівень

КІ та основні бізнес-додатки можна атакувати за допомогою багатьох різних векторів. Розширюючи попередній аналіз, слід пам'ятати, що КІ – це, на оперативному рівні, звичайний бізнес з усіма типовими недоліками, які це передбачає. Зрештою, Stuxnet, зловмисне програмне забезпечення, яке поставило під загрозу сотні комп'ютерів на іранських ядерних заводах у 2009-2010 роках, поширювалося через USB-ключ, який працівник підключив до своєї робочої станції. Співробітники справді є добре відомою точкою відмови для безпеки інфраструктури, незалежно від її природи.

Соціальна інженерія та подібні атаки. Поширеною технікою, яка використовується зловмисниками для проникнення в мережі та робочі середовища, є соціальна інженерія. Соціальна інженерія стосується будь-якої техніки, яка використовується для того, щоб обманом змусити користувача надати інформацію або виконати якісь, на перший погляд, нешкідливі та законні дії, які натомість компрометують систему чи мережу. Ця категорія атак дуже широка, і оперативно її можна реалізувати багатьма різними способами: від електронного листа із запитом облікових даних або вкладення підозрілого файлу до телефонної розмови, під час якої зловмисник вдає, що, наприклад, телефонує - надання певної форми технічної підтримки. Ці атаки переміщують фокус із

вразливостей системи та інфраструктури на людину, яка ними керує. Дещо дивно, але хоча ці атаки часто не дуже технічні, існує інфраструктура технічної атаки, щоб ними управляти. На чорному ринку кіберзлочинності кібершахраї розробляють і продають платформи та фреймворки для розробки та розгортання атак соціальної інженерії, наприклад, через електронну пошту. Citadel, наприклад, є дуже популярною соціальною платформою, яка дозволяє зловмисникам створювати власні атаки, обговорювати їх і давати відгуки своїм колегам і розробникам платформи. Таким чином можна без особливих зусиль підробити та розгорнути різноманітні соціально спроектовані атаки, поширюючи зловмисне програмне забезпечення та викрадаючи облікові дані (які також можуть належати обліковому запису користувача в КІ).

Фішинг і цілеспрямовані атаки. Ці типи атак можуть бути спрямовані як проти населення в цілому, коли зловмисник зацікавлений в накопиченні, наприклад, PIN-кодів кредитної картки, так і проти конкретного користувача; у цьому випадку атака спрямована на конкретну особу чи організацію, для якої жертва виступає в якості довіреної особи для атаки. Ці атаки зазвичай більш складні та продумані, ніж нецільові. Вони часто вимагають, щоб зловмисник мав певні попередні знання про жертву чи інфраструктуру, в якій вона працює. Зокрема, термін «фішинг» стосується атак, під час яких зловмисник видає себе за електронну адресу або контактну інформацію КІ або підроблює. співробітника, часто десь високо в ієрархії, і використовує його, щоб обманом змусити одержувачів електронної пошти виконати компрометуючу дію. Уявіть собі ситуацію, коли керівник відділу або генеральний директор компанії надсилає електронного листа співробітникам і просить візуалізувати вкладений файл: хто його не відкриє?

Цей тип соціальної інженерії явно більш цілеспрямований, ніж більш поширені методи фішингу. Однак інші типи цілеспрямованих атак можуть бути набагато більш технічними. Наприклад, використання вразливостей 0-day, які, як відомо, впливають на деякі системи КІ, часто вказує на те, що атака була явно спрямована проти цієї інфраструктури. Ці атаки дуже важко виявити та пом’якшити через саму їхню природу. Їхній вплив також важко оцінити. Які дані вкрав зловмисник? Що ще він скомпрометував після першої успішної атаки? Чи встановив зловмисник тихе шкідливе програмне забезпечення, яке організація повинна виявити та нейтралізувати? Останній випадок особливо складний.

Після того, як зловмисник отримав доступ до скомпрометованої системи, він може встановити тихе програмне забезпечення, яке важко виявити, яке відстежує, перевіряє або просто очікує команд зловмисника, перш ніж виконувати потенційно катастрофічні дії. Ці загрози називаються Advanced Persistent Threats (APT). APT є особливо шкідливими, тому що, навіть якщо їх виявлено, дуже важко оцінити початковий момент, коли загроза була введена, і який її фактичний вплив на організаційному рівні.

Каскадні збої у взаємозв'язаних системах. Каскадний збій — це послідовність залежних збоїв, які послідовно послаблюють систему. Завдяки своїй структурі та взаємозалежності між компонентами КІ (енергетичні системи) особливо схильні до таких відмов. Зазвичай під час каскадного збою можна спостерігати рухливий збій, коли секції опускаються, що призводить до виходу з ладу наступної секції, після чого перша секція повертається. Ця хвиля може кілька разів проходити через ті самі секції або сполучні вузли, перш ніж стабільність буде відновлена. Загрозу каскадних збоїв у КІбуло визначено як ключову проблему для урядів. Каскадний збій розглядається як потенційно катастрофічний, надзвичайно важко передбачуваний і все більш імовірний. Приватизація деяких КІ та подальше управління, орієнтоване на прибуток, можуть лише збільшити ризик таких невдач.

2.2 Атаки

Починаючи з уразливостей, описаних у попередніх розділах, виходить список можливих порушень. Зокрема, цей документ зосереджується на властивостях безпеки, пов'язаних із збереженням конфіденційності, цілісності та доступності. Прикладами такого роду власності є:

- Властивості авторизації, що вказують, які дії дозволені.
- Властивості контролю доступу, які регулюють доступ до деяких ресурсів. Рішення може бути прийнято відповідно до ролі користувача, якому потрібен доступ, або використання необхідного ресурсу. Політики контролю доступу можуть також перераховувати набір заборонених виконання шляхом визначення неприйнятних операцій.
- Властивості обмеженої доступності можна охарактеризувати як властивості безпеки. Приклад: «одному принципалу не можна відмовити у використанні ресурсу для більш ніж D кроків у результаті використання цього ресурсу іншими принципалами». Тут визначальний набір часткових виконань містить інтервали, що перевищують D кроків і протягом яких принципалу відмовлено у використанні ресурсу.
- Політика Китайської стіни регулює доступ до ресурсів, які класифікуються у двох різних доменах. Зокрема, політика китайської стіни гарантує, що якщо користувач має доступ до інформації одного набору, цей користувач не може мати доступу до інформації, що належить до іншого набору. Політика «Китайської стіни» поєднує комерційний розсуд із законодавчо обов'язковим контролем. Він необхідний для роботи багатьох організацій, що надають фінансові послуги, і тому, можливо, такий же важливий для фінансового світу, як політика Белла-ЛаПадули [55] для військових.

Посилаючись на політику Bell-LaPadula, представлено набір властивостей потоку інформації. У друкованих роботах є багато визначень такого роду властивостей. Основна ідея полягає в тому, що потік інформації від користувачів високого рівня до користувачів низького рівня можна заборонити таким чином, щоб діяльність користувачів високого рівня була прозорою щодо користувачів низького рівня. З точки зору КІ, в якій кілька компонентів взаємодіють один з одним, політика потоку інформації може складатися з регулювання потоку інформації між різними компонентами таким чином, щоб конфіденційна інформація не розголошувалася або витікала можливим зловмисником.

2.2.1 Приклад із застосування: Stuxnet

W32.Stuxnet [92], також просто відомий як Stuxnet, — це зловмисне програмне забезпечення, яке використовувалося в 2009-2010 роках для здійснення цілеспрямованої атаки. Ця атака привернула велику увагу як у ЗМІ, так і в дослідницькому співтоваристві. Після трьох років залишається багато незрозумілих моментів, але, судячи з того, що відомо, Stuxnet був створений спеціально для поширення та скомпрометації мережі ICS під брендом Siemens. Завдяки 0-денній уразливості, руткіту Windows, руткіту PLC та багатьом іншим вдосконаленим методам уникнення та реплікації Stuxnet вдалося заразити багато об'єктів, якими керує ICS. Основним поясненням реакції ЗМІ, промисловості, урядів і дослідників є те, що атомні станції Ірану були найбільш зараженою ціллю.

Мета Stuxnet полягала в тому, щоб змінити функціонування PLC (завдяки першому знайденому руткіту PLC), щоб змінити роботу обладнання, можливо, саботуючи весь об'єкт, спричиняючи серйозну шкоду у фізичному світі (наприклад, вибухи). , радіація).

Недавній звіт Symantec [128] описує, що попередні версії цієї складної кіберзброї містили інші

відомі версії шкідливого коду, який, як повідомляється, було запущено США та Ізраїлем кілька років тому, намагаючись саботувати ядерну програму Ірану. Це вказує на те, що Stuxnet був активний приблизно за два роки до основного інциденту. Це також означає, що жодна з двох кампаній Stuxnet (у 2007 та 2009–2010 роках) не мала серйозного впливу на ядерні об'єкти Ірану, визнану головну ціль атаки. Незважаючи на те, що Stuxnet фактично зазнав невдачі, важливий факт залишається вірним: Stuxnet було створено (державними офісами, як стверджують деякі експерти) за допомогою ретельного планування та кількох ресурсів.

2.2.2 Приклад із застосування: Aramco

16.08.2012 Symantec і Kaspersky Lab [10], а за ними кілька інших постачальників і дослідників, описали нового модульного комп'ютерного хробака, який отримав назву Shamoon. Зловмисне програмне забезпечення було частиною низки кібершпигунських і диверсійних атак на Близькому Сході (разом із раніше описаним Stuxnet, див. Розділ 2.3.1). Він відомий не своїми механізмами розповсюдження, які використовують спільні диски та папки, а скоріше унікальним корисним навантаженням.

Після зараження системи Shamoon збирає файли з певних місць у системі, надсилає зібрану інформацію назад зловмисникові та замінює файли та головний завантажувальний запис системи зображенням, вирізаним із зображення американського прапора у вогні. .

Самозвана група Cutting Sword of Justice взяла на себе відповідальність за використання Shamoon проти 30 000 робочих станцій Saudi Aramco, через що компанія витратила тиждень на відновлення своїх послуг. Дивно, але атака не вразила жоден з комп'ютерів і мереж управління виробництвом і обмежилася офісними та адміністративними системами.

2.3 Підходи до відновлення та захисту

Складність, неоднорідність, адаптивність і мобільність КІ накладають нові виклики на розробку систем зменшення ризиків і механізмів безпеки. Дійсно, структури розвиваються для покращення якості послуг, що надаються, а також для управління можливими загрозами, викликаними новими методами атак.

Основним завданням, необхідним для захисту системи, є виконання оцінки вразливості. Цей процес може допомогти ідентифікувати, кількісно оцінити та ранжувати вразливі місця системи та запровадити засоби контролю безпеки, необхідні для пом'якшення таких вразливостей. Хоча ця операція добре підходить для традиційних інформаційних систем, вона може призвести до незадовільного та обмеженого обсягу для КІ. Насправді, хоча час простою, викликаний оцінкою вразливості, може бути прийнятним для традиційних систем, він стає неприйнятним для КІ, оскільки він ризикує порушити контрольовані процеси та пошкодити дороге обладнання [174]. Крім того, коли вразливості ідентифіковано та вирішено, виправлення компонентів КІ є проблематичним як для вимог доступності, так і для великомасштабного характеру систем [139]. Представлені проблеми підкреслюють надзвичайну потребу в проектуванні та розробці систем КІ з особливою увагою до властивостей безпеки. Дослідники розробляють тестові стенди, що складаються як з фізичних, так і з віртуальних пристроїв, які можуть допомогти виявити загальні вразливості та перевірити ефективність різних підходів до захисту, не впливаючи на роботу реальних КІ [174, 106].

Можливим рішенням для уникнення неавторизованого доступу є відокремлення мережі. У сценарії КІ ця методика полягає у відокремленні мереж систем управління від корпоративних

мереж, які зазвичай підключені до Інтернету. Таким чином можна запобігти несанкціонованому доступу співробітників і віддалених зловмисників. Хоча це може бути ефективним для підвищення безпеки системи, повне фізичне відокремлення не є життєздатним і перспективним рішенням для сучасних систем КІ. Великомасштабний і розподілений характер цих систем робить необхідним віддалений доступ до них для управління, моніторингу та контролю, навіть з мобільних пристроїв [139]. Тим не менш, механізми логічної сегрегації мережі повинні бути реалізовані, щоб захистити КІ від несанкціонованого доступу. Мережі керування мають бути ізольовані від корпоративних мереж за допомогою засобів фільтрації безпеки, таких як брандмауери. Трафік внутрішнього моніторингу та адміністрування можна додатково відокремити від звичайного трафіку локальної мережі за допомогою VLAN. Цей метод забезпечує віртуальну ізоляцію користувачів, які отримують доступ до критичних даних, від решти трафіку [106]. Нарешті, має бути дозволений лише авторизований і захищений віддалений доступ. Цього можна досягти шляхом впровадження віртуальних приватних мереж (VPN) з використанням, наприклад, тунелів IPsec [23]. Очевидно, що саме поділ мережі не забезпечує повного захисту КІ. Наприклад, фізичний доступ до мереж систем керування, який може бути досягнутий за допомогою атак соціальної інженерії, долає будь-який захист від сегрегації мережі та може серйозно загрожувати всій системі. З цієї причини інші механізми безпеки повинні бути реалізовані для подальшого захисту КІ.

Значне покращення може стати результатом переробки протоколів зв’язку, орієнтованої на безпеку. Розробка захищених протоколів є делікатним, трудомістким і дорогим завданням, але його потрібно серйозно взяти до уваги, оскільки незахищені протоколи становлять серйозну загрозу для КІ. Однак розробка нових протоколів з нуля може не бути задовільним рішенням у короткостроковій перспективі, оскільки прийняття цих протоколів може призвести до неприпустимих простоїв і несумісності із застарілими системами. З цієї причини дослідники зосередили свої зусилля на розробці рішень безпеки, які відповідають існуючим специфікаціям і стандартам протоколів. Зокрема, Chandia та ін. [73] пропонують прийняти невикористовувані функціональні поля в стандартних протоколах SCADA (Modbus і DNP3) для забезпечення конфіденційності та цілісності. Цей підхід покращує безпеку КІ без втрати сумісності із застарілими системами. Іншим рішенням є методи прозорого тунелювання. Використовуючи ці методи, існуючі протоколи можна загорнути в захищені комунікаційні тунелі, які забезпечують такі фундаментальні властивості безпеки, як автентифікація, цілісність і конфіденційність. Тунелі можуть бути реалізовані як незалежний рівень програмного забезпечення в існуючих польових пристроях або всередині вбудованих компонентів спеціального призначення, які діють як шлюзи.

Для подальшого захисту систем КІ слід запровадити моніторинг трафіку та механізми виявлення аномалій. Як і в традиційних інформаційних системах, ці методи можуть допомогти ідентифікувати дані, що транспортуються в мережі, контролювати транзакції між різними компонентами та запобігати або виявляти спроби атак. Ці методи можуть також покращити КІ з функціональної точки зору, наприклад, для оптимізації продуктивності установки шляхом моніторингу поведінки процесу [73]. Механізми моніторингу трафіку та виявлення аномалій можуть бути реалізовані системами запобігання вторгненням (IPS), які дозволяють зменшити шкідливу активність. Основним завданням розгортання IPS є етап навчання, який використовується для аналізу та збору даних про звичайну мережеву активність. Після цього етапу IPS здатна розпізнавати зловмисну активність і відповідним чином реагувати.

У традиційних IT-мережах, де трафік створюється користувачами за допомогою складних шаблонів зв’язку, це завдання може бути надзвичайно складним. Однак однорідність і низькі

обсяги трафіку в типових системах КІ спрощують завдання навчання настільки, що воно стає здійсненним [73]. Однак для належної роботи IPS необхідні глибокі знання вразливостей систем і протоколів. Як зазначалося раніше, аналіз уразливостей для систем КІ є складною та постійною операцією, яка вимагає від експертів із безпеки набуття спеціальних знань і ресурсів. Доступні результати вже були використані для розробки сигнатур атаки для стандартних протоколів SCADA (Modbus, DNP3 та ICCP). Ці сигнатури атак інтегровані в більшість комерційних систем запобігання вторгненням [149].

2.5. Випадкові несправності

Хоча все більше уваги приділяється зловмисним діям, націленим на КІ, випадкові збої залишаються важливим джерелом збоїв, які можуть вплинути як на фізичні, так і на кібернетичні аспекти КІ.

Особливий інтерес при аналізі взаємозалежної критичної інфраструктури становлять три типи відмов:

- Каскадні збої, які виникають, коли збій в одній інфраструктурі викликає збій одного або кількох компонентів у другій інфраструктурі;

- Ескалація збоїв, яка виникає, коли існуючий збій в одній інфраструктурі посилює незалежний збій в іншій інфраструктурі, збільшуючи його серйозність або час для відновлення та відновлення після цього збою;

- Збої із загальної причини, які виникають, коли дві або більше інфраструктури зазнають одночасного впливу через спільну причину.

Звичайно, окрім аналізу типів несправностей, важливо розуміти різні причини, які можуть призвести до виникнення таких несправностей. Після того, як стане відомо про причину збою, можна вжити належних заходів на рівні системного керування інфраструктурою, щоб запобігти виникненню такої ж несправності в майбутньому або принаймні пом'якшити її вплив на систему.

Зі звітів про інциденти в ряді критичних секторів, таких як глобальне фінансування, розподіл енергії, транспортування, є емпіричні докази того, що ризики від взаємозалежностей, здається, не були достатньо розглянуті або оцінені. Хоча цілком очевидно, що існують взаємозалежності між інфраструктурою, наприклад, телекомунікації потребують електроенергії, вода потребує електроенергії для перекачування, а електростанція потребує води для запуску, необхідно визначити, до якого рівня залежності є значним внеском у ризик піддати інфраструктуру катастрофічним наслідкам. Оцінка важливості взаємозалежностей і, загалом, невизначеності у взаємодії інфраструктури є проблемою, головним чином через складність, неоднорідність і масштаб залучених систем. Було вжито багато ініціатив для вирішення цієї проблеми та розроблено початкові підходи, включаючи якісний і кількісний аналіз даних про інциденти, а також рішення для моделювання та симуляції.

Важливо відзначити, що традиційні дослідження безпеки або надійності майже завжди розроблялися на основі припущення номінальної поведінки в одному з двох вимірів: жодних атак не передбачається, якщо допускаються випадкові помилки, і жодних помилок не відбувається, коли стикаються з нападами.

Є деякі часткові винятки з цього ставлення. Найбільш чудовим є візантійська відмовостійкість, де не передбачається обмежень на поведінку несправних одиниць (тобто включно з навмисними зловмисними), завдяки чому деякі пропозиції включають неоднорідні несправності, поєднуючи навмисні зловмисні

несправності та просто випадкові. Як було описано раніше, коли йдеться про взаємозалежності, критична інфраструктура демонструє ескалацію та каскад збоїв через комбінації атак і незловмисних помилок, таким чином роблячи зв'язки та взаємодію між такими атаками та незловмисними помилками дуже важливими для розуміння та абсолютно критичними контролювати. Таким чином, окрім того, щоб йти в ногу з новими загрозами та атаками, які постійно з'являються, виникає новий фундаментальний виклик, спрямований на захист критичної інфраструктури, що вимагає розвитку сукупності знань із інтегрованим баченням усіх загроз, навмисних і випадкових , що може вразити критичну інфраструктуру.

2.5.1 Огляд випадкових несправностей і контрзаходів

Відповідно до Технічного комітету з відмовостійких обчислень IEEE Computer Society та IFIP Working Group 10.4, Dependable Computing and Fault Tolerance, які нещодавно систематизували основні концепції надійних обчислень у [49], причиною є збій (визначено або гіпотетично) неправильного стану системи. Некоректний стан, званий помилкою, перетворюється на збій, коли послуга, що надається комп'ютерною системою, відхиляється від правильної служби та негативно впливає на користувачів та інші зовнішні системи.

Несправності можна класифікувати за кількома параметрами. Наприклад, ми можемо розрізняти апаратні та програмні збої, або постійні та тимчасові збої. Крім того, несправності можуть бути внутрішніми або зовнішніми в системі. Якщо дивитися на феноменологічну причину, несправності можна класифікувати як природні (спричинені природними явищами, такими як погіршення стану, несподіване випромінювання або шум, погані умови навколишнього середовища тощо) або спричинені людиною (в результаті дій людини). Несправності, створені людиною, можна далі класифікувати на зловмисні та незловмисні. Зловмисні помилки навмисно вводяться під час розробки або використання з явним наміром завдати шкоди системі. Незловмисні помилки можуть бути натомість результатом людської помилки або неправильного рішення, і можуть бути класифіковані як випадкові помилки, якщо вони внесені ненавмисно, або помилки некомпетентності, якщо вони спричинені відсутністю професійної компетентності. Зрозуміло, що всі природні дефекти є випадковими, ненавмисними та спричиненими не людьми.

Незважаючи на зусилля інженерів для уникнення випадкових несправностей, запобігти їх виникненню, на жаль, неможливо. По суті, жодна ретельна розробка не може гарантувати, що великі та складні комп'ютерні системи, які включають кілька мережевих апаратних і програмних компонентів, як у випадку КІ, не вийдуть з ладу через випадкові несправності, такі як старіння обладнання, наслідок захисний пристрій, екологічні чи техногенні несправності. З цієї причини досягнення надійного КІ вимагає поєднання як ретельного проектування, щоб запобігти випадковим збоям і підтримувати їх виникнення в розумних межах, так і додаткових засобів для пом'якшення впливу випадкових збоїв, з метою усунення випадкових збоїв із системи та уникаючи того, що вони призводять до більш серйозних каскадних збоїв критичної інфраструктури в цілому. Стратегії, які можуть бути прийняті для пом'якшення випадкових несправностей, згруповані в:

Відмовостійкість, яка дозволяє уникнути збоїв в обслуговуванні шляхом автоматичного визначення несправностей і відновлення після них, наприклад, ізоляції несправного компонента або його заміни за допомогою резервних компонентів.

Усунення несправностей, що зменшує кількість і серйозність несправностей як під час розробки, шляхом суворого тестування, інспекцій або офіційної верифікації, так і під час використання системи, шляхом профілактичних і коригувальних технічних заходів.

Прогнозування несправностей, яке аналізує випадки та наслідки несправностей, щоб забезпечити якісну/кількісну оцінку поведінки системи за наявності несправностей. Ця оцінка забезпечує корисний зворотний зв'язок для покращення дизайну системи, наприклад, пропонуючи, де використовувати відмовостійкість для підвищення надійності.

2.5.2 Випадкові збої в критичній інфраструктурі

Нижче наведено кілька випадків випадкових несправностей КІ та пов'язаних з ними збоїв, де це доцільно, з посиланням на домени застосування, що мають відношення до проекту TENACE, а саме домен електромережі, транспортний домен (контроль повітряного руху та залізниці), і фінансова сфера. Підсумкове опитування є сумою безпосереднього досвіду партнерів TENACE у минулих або поточних дослідницьких проектах і промисловому співробітництві за участю КІ.

Фінансова сфера. Фінансова система включає складний ландшафт учасників, включаючи зацікавлені сторони, регуляторні органи, постачальників фінансових послуг і комунікаційні мережі, що їх зв'язують. Ці системи є квінтесенцією функціонування сучасних національних економік, і їх можна однозначно вважати КІ суспільства. Фінансова екосистема покладалася на ІТ-ресурси та цифрові комунікації з моменту народження комерційних комп'ютерних рішень (ще з шістдесятих років). Цей багаторічний досвід у використанні та управлінні складними ІТ-ресурсами, а також величезний обсяг ноу-хау, накопичений за цей час ІТ-відділами фінансових установ, роблять цих гравців більш готовими до зустрічі з викликами, які пропонує сучасний взаємопов'язаний світ. Тим не менш, широке використання додатків, які повсюдно з'єднують користувачів із їхніми банківськими рахунками, і порив до високошвидкісних фінансових транзакцій піддають фінансову інфраструктуру серйозному ризику. Ця інфраструктура, яка значною мірою базується на ІТ-системах, схильна до кількох різних ризиків, таких як збої обладнання, мережі та живлення; втрата даних через невідповідні засоби або правила резервного копіювання; погано навчений/кваліфікований ІТ-персонал, якому бракує достатніх знань; надмірна залежність від ІТ-аутсорсингу; погана практика управління ІТ; невідповідні приміщення або інвестиції в ІТ.

ІТ-інцидент 2012 року в Королівському банку Шотландії (RBS) [125] є яскравим прикладом неочікуваних проблем, які можуть виникнути, якщо такі ризики не враховуються належним чином. У червні 2012 року 16,7 млн клієнтів трьох банків (RBS, NatWest і Ulster Bank) протягом чотирьох днів не мали доступу до грошей на своїх рахунках. Інцидент стався через звичайну людську помилку під час керування завданням пакетного оновлення на критично важливому мейнфреймі IBM, який використовувався для керування понад 20 млн транзакцій на день. Завдання оброблялися планувальником CA-7, який не оновлювався три дні поспіль. Протягом цього періоду транзакції буферизувалися без можливості підтвердження. Більш ніж 100 мільйонів транзакцій не були виплачені на банківські рахунки. Це спричинило серйозні наслідки для клієнтів, які не мали доступу до своїх рахунків або користувалися дебетовими картками. Невдача навіть засудила чоловіка провести вихідні у в'язниці, оскільки він не зміг сплатити заставу [104]. Банківські експерти заявили, що витрати RBS на вирішення ІТ-проблем, включаючи витрати на додатковий персонал, а також гроші на відшкодування клієнтам, ймовірно, становитимуть від 50 до 100 млн фунтів стерлінгів. Внаслідок цієї аварії Управління фінансових послуг Великобританії почало чинити тиск на банки Великобританії, щоб вони оновили свої старі системи до більш сучасних та керованих технологій. Фактично крах RBS став серйозним тривожним дзвіночком для глобальних банків, багато з яких покладаються на ІТ-

системи, які працювали десятиліттями і стають дедалі складнішими, оскільки банки розширювалися шляхом придбання, часто без повної інтеграції систем, які вони успадкували [100].

Навіть якщо IT-інфраструктура підтримується належним чином, серйозні інциденти все одно можуть виникати через випадкову взаємодію незалежних систем, як показало нещодавнє дослідження поведінки торгових алгоритмів [109]. В алгоритмічній торгівлі високопродуктивні машини запускають автоматизовані алгоритми, метою яких є відстеження мікроколивань на фінансових ринках і використання їх для виконання швидких ринкових транзакцій (одну транзакцію можна підготувати менш ніж за 740 нс [78]). У 2012 році на алгоритмічну торгівлю припадало понад 50% торгівлі в США та понад 30% торгівлі в ЄС. При правильному та високошвидкісному виконанні ці транзакції можуть легко призвести до великих доходів для інвестора. Однак сьогодні такі системи працюють на такій високій швидкості, що контроль і втручання в них людини є вкрай непрактичним. Ця проблема в поєднанні з відсутністю математичних моделей, здатних передбачити колективну поведінку цих алгоритмів, породила групу конкурентоспроможних машин, що містять натовпи хижих алгоритмів, якими неможливо повністю керувати. Ціна за цю відсутність контролю вже сплачена: у 2010 році Уолл-стріт зазнала так званого «спалахового краху», коли індекси Dow Jones, S&P500 і Nasdaq зазнали втрати майже на 9% протягом дня. Після п'яти місяців розслідувань SEC і Комісія з торгівлі товарними ф'ючерсами представили звіт, у якому чітко описано, як високочастотні торгові переговори підштовхнули складну систему, якою є фінансовий ринок, у неочікуваному напрямку [176]. Незважаючи на нові правила, спрямовані на контроль над ринком, нові випадки виникають часто [120].

Домен електромережі. Електромережа – це система виробників і споживачів електроенергії [170]. Він включає в себе генератори електроенергії, споживачів електроенергії, вимикачі, які контролюють електроенергію, а також підстанції, лінії електропередач і трансформатори, які постачають електроенергію. Громада може мати генератор для забезпечення електроенергією. Генератор може змінювати свою продуктивність у міру використання споживачами. Коли попит на енергію занадто великий для генератора, громада купує електроенергію з іншого джерела. Коли генератор виробляє більше електроенергії, ніж використовує громада, її можна продати іншим громадам.

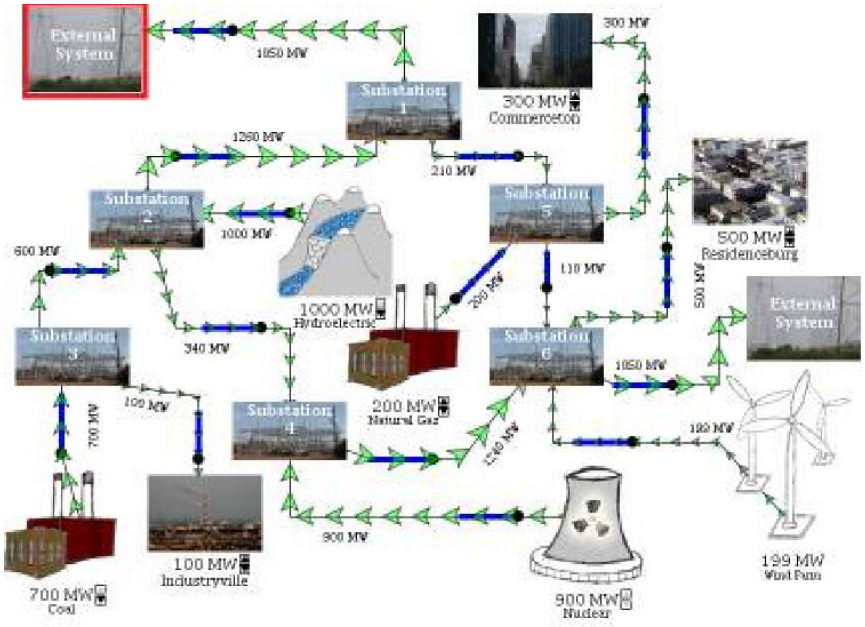
Електромережа – це система, що складається з взаємопов'язаних генераторів електроенергії, систем передачі та користувачів, які виробляють, передають і споживають електроенергію. На малюнку 2.1 показано сценарій, який використовує вугільну, гідроенергію, природний газ, вітрові та атомні генератори. Зелені стрілки (Малюнок 2.1a) показують напрямок, у якому рухається електроенергія, витікаючи з генераторів, через підстанції та в громади. Більші стрілки вказують на більшу потужність. Електроенергія від різних генераторів розподіляється між користувачами в Коммерстоні, Індустрівіллі та Резиденбурзі. Будь-яка потужність, яка не використовується спільнотами, надсилається користувачам в інших системах (зовнішні системи, червоний прямокутник на малюнку 2.1a). Зовнішньою системою може бути така країна, як Італія, яка купує електроенергію у Швейцарії. Сума потужності, що надходить на підстанцію, повинна дорівнювати сумі потужності, що виходить з цієї підстанції. Наприклад, вугільний генератор надсилає 700 МВт електроенергії на підстанцію 3: Industryville отримує 100 МВт цієї потужності, а 600 МВт надходить на підстанцію 2.

Основні відключення електроенергії, які зазнали за останнє десятиліття в кількох електромережах у всьому світі, були спричинені випадковими несправностями. Наприклад, американо-канадське відключення електроенергії 14.08.2003 , яке торкнулося приблизно 50 млн людей у восьми штатах США та двох канадських провінціях, почалося з проблем з реактивним електропостачанням у штатах Індіана та Огайо, які не були негайно вирішені через відсутність раннього попередження через проблеми з програмним забезпеченням. 28 вересня 2003 року в континентальній Європі сталося ще

одне відключення електроенергії, що призвело до повного знеструмлення по всій Італії. Це почалося з відключення великої лінії електропередач між Італією та Швейцарією, спричинене спалахом дерева (природна причина), але з'єднання не було відновлено, оскільки автоматичне керування вимикачем не замкнуло лінію (техногенна помилка розробки). Отриманий каскадний ефект відключення ліній спричинив крах усієї італійської системи.

На малюнку 2.1b показано приклад того, що сталося в той час. Лінія електропередачі між підстанцією 4 та підстанцією 2 була пошкоджена, тому зв'язок між підстанцією 2 та підстанцією 1 був перевантажений. Зокрема, ця ланка мала близько 1600 МВт потужності (червоні стрілки). Після того, як перевантаження тривало кілька хвилин, лінія передачі перестала працювати, і несправність поширювалася в електромережі, поки не відбулося знеструмлення.

Проект EU-FP6-027513 CRUTIAL (2006-2009), за участю дослідницького підрозділу CNR, стосувався нових мережевих ІКТ-систем для управління електричними мережами. Цей проект виявив як випадкові помилки, так і зловмисні атаки, що загрожують цим КІ. Перехідними та постійними відключеннями електричних компонентів вважаються такі, як відключення, перевантаження, зменшення виробництва, збільшення або зменшення попиту, падіння напруги. З точки зору інфраструктури управління, модель відмов включала пропуски, час і візантійні збої через випадкові джерела або атаки. Крім того, була врахована модель відмови взаємодії між електричною мережею та її системою керування. Проаналізовано вплив збоїв системи керування на стан мережі, а саме з точки зору топології та значень електричних параметрів, таких як напруга, активна та реактивна потужність, залежно від логічних компонентів, на які впливають збої, і від тип несправностей. Передбачається, що збої в електромережі впливають на систему керування, зменшуючи її функціональні можливості аж до повного збою, у крайньому випадку збій призводить до повного знеструмлення.



Малюнок 2.1: Приклад критичної інфраструктури електромережі.

Домен управління повітряним рухом. Цивільна система управління повітряним рухом (ATC) — це типова критично важлива система з інтенсивним використанням програмного забезпечення, яка відіграє ключову роль в управлінні повітряним рухом (ATM) [90]. Він надає засоби та послуги наземним диспетчерам і пілотам для безпечного керування наземними польотами та польотами на маршруті.

Ці системи повинні відповідати суворим вимогам якості обслуговування щодо доступності, щоб, у свою чергу, забезпечити високу доступність усієї інфраструктури. Для досягнення цієї мети програмні додатки повинні розповсюджувати та тиражувати дані, наприклад, маршрути польотів на кількох вузлах, підключених через глобальну або локальну мережу. З огляду на природу таких систем, копії програмного забезпечення повинні бути суворо узгодженими, щоб підтримувати однаковий стан у часі, таким чином забезпечуючи однакові результати для запитів на обслуговування. У таких складних розподілених системах часті збої окремих компонентів, і з ними потрібно безпечно поводитися, щоб забезпечити живучість системи. Широке тестування на етапі проектування програмного додатку не може уникнути виникнення несправностей під час роботи, які можуть призвести до катастрофічних наслідків для всієї системи.

Основним компонентом програмного забезпечення АТС є система обробки польотних даних (FDPS), яка надає таку інформацію, як маршрути польотів, їх поточна траєкторія, інформація про літак і метеорологічні дані. FDPS був однією з головних цілей експериментів, проведених під час останніх дослідницьких проектів, таких як італійський проект PRIN DOTS-LCCI1, який залучав підгрупу партнерів TENACE, і державно-приватну регіональну лабораторію COSMIC2 в регіоні Кампанія, яка залучала дослідницький підрозділ UNINA та компанія SELEX-ES Finmeccanica, яка разом з іншими європейськими партнерами розробляє FDPS.

Аналіз потенційних збоїв, що впливають на FDPS, про який повідомляється в [148], вказує на ризик відмови всієї системи через збої в окремих компонентах програмного забезпечення та заохочує до прийняття стратегій пом'якшення збоїв. Режими збоїв програмних об'єктів FDPS включають збої процесу, тобто об'єкт припиняє надавати послугу через неочікуваний збій, пасивні зависання. Об'єкт необмежений час чекає на ресурс, який ніколи не буде звільнено, наприклад, взаємоблокування та активні зависання, тобто об'єкт зупиняється на невизначений час, але він тримає системні ресурси зайнятими (напр., він застряг у нескінченному циклі). У свою чергу, відсутність програмного забезпечення управління повітряним рухом може спричинити помітні затримки та збої в обслуговуванні, а також наражати літаки на серйозні аварії. Це був випадок збою голосової комутації та системи управління в Центрі управління рухом на маршрутах Лос-Анджелеса, що спричинило втрату голосового контакту з літаками, унеможливлюючи попередження про небезпеку, що наближається [99, 185]. Цей збій програмного забезпечення вплинув на 800 польотів у США, і принаймні в 5 випадках літаки знаходилися в межах обов'язкових мінімальних відстаней поділу, встановлених Федеральним управлінням цивільної авіації США, таким чином значно підвищуючи ризик зіткнень.

Область залізниць. Залізничний транспорт є важливим прикладом сфери, де відмовостійкість і функції безпеки відіграють життєво важливу роль. Через несправності в інфраструктурі, швидкість або помилкову сигналізацію в залізничних системах з плином часу траплялися незліченні катастрофічні збої. Підходи до проектування, орієнтовані на відмовостійкість і безпеку в галузі залізниці, звичайно, охоплюють багато різних галузей техніки. Для цілей проекту основна увага приділяється комп'ютерним системам управління залізницею. По суті існує три класи систем управління залізницею, що мають важливе значення для безпеки:

- Системи блокування для керування маршрутами поїздів і сигналами на станціях;
- Системи управління рухом для керування рухом поїздів на рівні колії;
- Системи керування поїздом для керування рухом поїзда на борту.

Еволюція комп'ютерних систем призвела до більш складних режимів відмови, оскільки кожна з вищезазначених систем реалізована як дедалі складніша комп'ютерна платформа, часто у формі неоднорідних вбудованих систем реального часу, розподілених по масштабній інфраструктурі. Через це дуже складно забезпечити вимоги до надійності, доступності, ремонтопридатності, безпеки та захисту (RAMSS).

Малюнок 2.2: Загрози надійності системи керування залізницею.

[1]http://dots-lcci.prin.dis.unina.it/
[2]http://www.cosmiclab.it

Загрози для надійності систем керування залізницею можна підсумувати, як показано на рисунку 2.2. Несправності можуть бути виявлені на етапі проектування та розробки, що вимагає застосування цілого ряду підходів до проектування та найкращих практик, перш ніж система буде запущена в експлуатацію. Під час нормальної роботи системи несправності можуть виникати з різних джерел. Люди-користувачі, наприклад, керівництво, оператори, супроводжувачі, можуть викликати системні збої як ненавмисно, так і навмисно. Несправності інфраструктури, включаючи, наприклад, електропостачання та мережі передачі даних, також становлять загрозу для системи управління залізницею. Нарешті, природні дефекти, спричинені умовами навколишнього середовища, наприклад, температурою, вологістю, космічною радіацією тощо, представляють різноманітні загрози, які слід враховувати для забезпечення вимог RAMSS.

Глава

3 Фінансові системи

Фінансова система визначається набором установ (ринків і посередників), через які домогосподарства інвестують свої заощадження, а корпорації та уряди отримують фінансування для своєї діяльності. Фінансові системи також існують для забезпечення потоку коштів від заощаджувачів (кредиторів) до позичальників (інвесторів або споживачів) як частина кредитної системи, навіть для полегшення платежів у рамках платіжної системи. Надаючи широкий спектр послуг, які є основою світової економіки, фінансову систему можна вважати квінтесенцією функціонування економіки сучасної нації. Тому цю систему можна однозначно вважати КІ нашого суспільства, і через постійне зростання проникнення Інтернету в цю інфраструктуру її потрібно захищати від кібератак.

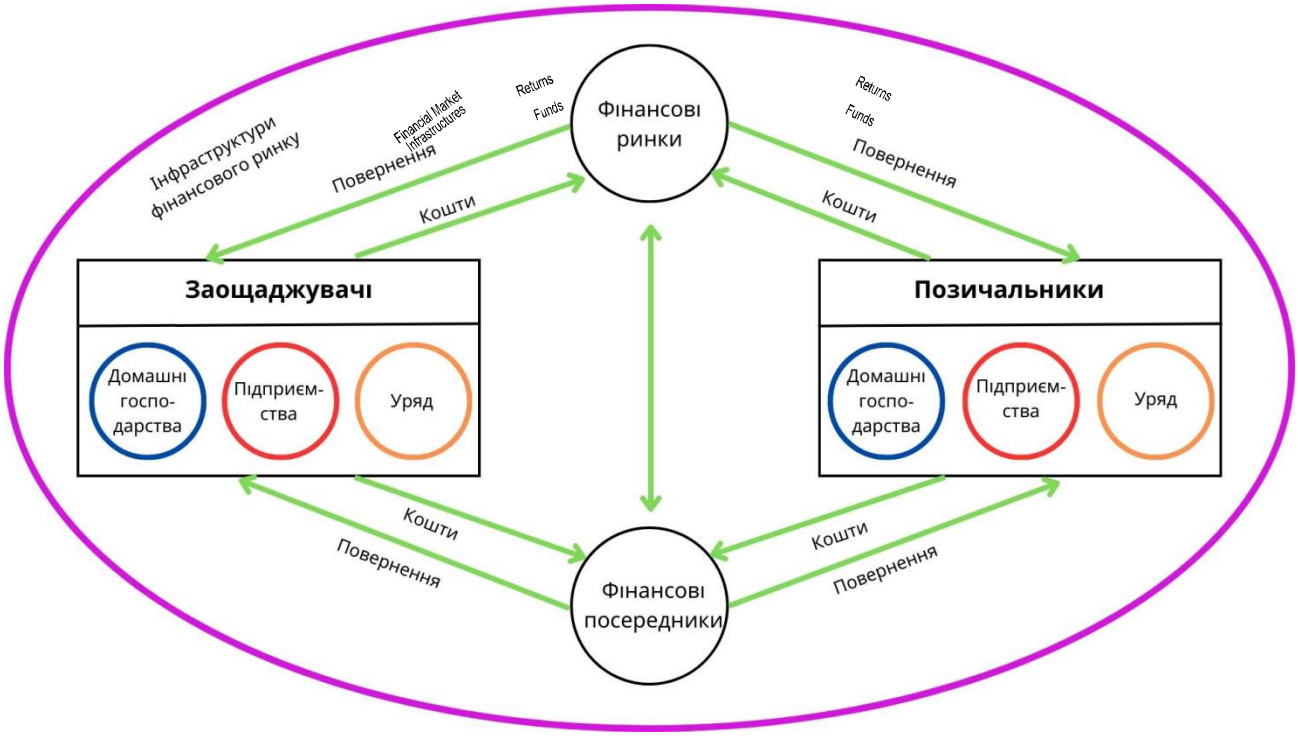
У цьому розділі представлено фінансову систему (ФС) з її основними зацікавленими сторонами та гравцями та її вимоги як інфраструктури для економіки. Далі в ньому описуються деякі стратегії захисту, спрямовані на запобігання будь-якому ефекту від атак, а потім завершується оглядом відкритих проблем у цій галузі.

3.1 Опис критичної інфраструктури

Фінансова система в основному є нематеріальним активом, який сприяє економічному зростанню шляхом полегшення переказу коштів від вкладників до позичальників і полегшення платежів. Навіть якщо форма фінансової системи в кожній країні може постійно відрізнятися, фінансова система з більшою чи меншою ефективністю приносить користь економіці, зокрема:

- ***Фізичні особи***. Вони забезпечують можливість диверсифікації ризиків їхніх інвестицій, ліквідність фінансових активів (здатність обміняти фінансовий актив на готівку в короткий термін і за низьку вартість), а також інформацію для оцінки відповідних даних щодо ризику та прибутку різні фінансові операції (дозволяють збирати та передавати інформацію про вкладників і позичальників).

- ***Суспільство***. Воно сприяє ефективному розподілу дефіцитних економічних ресурсів, забезпечуючи ефективну кредитну систему для переказу коштів між заощаджувачами та позичальниками, що сприяє економічному зростанню, а також забезпечує ефективну платіжну систему для стимулювання транзакцій.



Малюнок 3.1: Схематичне зображення фінансової системи.

Термін «система» у фінансовій системі вказує на групу складних і тісно пов'язаних установ, агентів, процедур, ринків, операцій, претензій і зобов'язань в економіці. Для спрощення ми можемо розглянути п'ять основних компонентів, які ідентифікують фінансову систему: i) фінансові інструменти, ii) фінансові ринки, iii) фінансові посередники, iv) законодавча та регулятивна база, v) інфраструктури фінансового ринку (докладніше в наступному розділі).

Традиційно схематичне зображення фінансових систем, наприклад те, що зображено на малюнку 3.1, призначене для опису фінансової системи певної країни. Це спрощений і обмежений погляд, оскільки завдяки технологічному розвитку більше немає фізичних чи технологічних перешкод для своєчасного та відносно дешевого потоку коштів у будь-якій точці світу. Крім того, якщо ми розглядаємо таку територію, як ЄС, ми можемо говорити про фінансову систему, яка виходить за національні кордони кожної європейської країни. За визначенням і беручи до уваги роль зростання економіки, фінансову систему можна вважати критичною інфраструктурою; крім того, як детально описано в наступних розділах, правильне функціонування FS залежить від правильного функціонування всіх залучених елементів і фінансової інфраструктури, яку система використовує для свого функціонування (наприклад, платіжна система тощо), сьогодні все більше і більше на основі технологій та IT-систем. Це робить надзвичайно важливим, щоб фінансова система була захищена від кібератак.

3.1.1 Основні зацікавлені сторони та гравці

Як зазначалося вище, фінансову систему можна аналізувати через її головну складову:

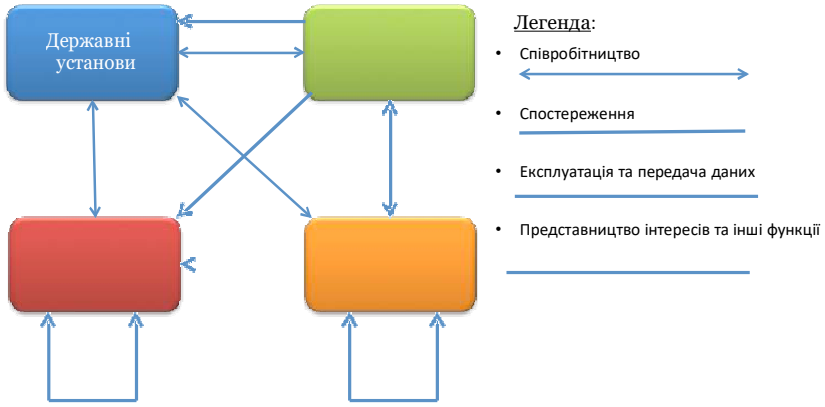
Фінансові інструменти – це всі продукти, якими торгують на фінансовому ринку/системі; це відноситься до всіх фінансових активів, цінних паперів або інших видів фінансових інструментів відповідно до потреб інвесторів і шукачів кредиту. Сучасні фінансові ринки характеризуються наявністю різноманітних фінансових інструментів, у тому числі цінних паперів (боргові інструменти та акції) та похідних інструментів (ф'ючерси, опціони та свопи). Вони вказують на вимогу щодо погашення основної суми в майбутньому або сплата регулярної суми у вигляді відсотків або дивідендів. Акції, боргові зобов'язання, облігації, деривативи тощо – це деякі приклади.

Фінансові ринки – це місце, де створюються та/або передаються фінансові активи/інструменти. Метою ринку цінних паперів є об'єднання двох груп учасників: тих, хто має капітал для інвестування (інвесторів), і тих, хто хоче позичити цей капітал (напр., фірми та державні органи). Таким чином, як альтернативу позичанню грошей у посередника (напр., банку), фірми та державні органи можуть залучати кошти безпосередньо від інвесторів шляхом випуску цінних паперів. Без фінансових ринків або недостатньо розвинутих, позичальникам важко знайти кредиторів. У цьому випадку посередники допомагають або замінюють ринки в цьому процесі (напр., банки беруть депозити від інвесторів і позичають гроші з цього пулу вкладених грошей людям, які потребують позик). Щоб ринок цінних паперів працював, він має бути підкріплений механізмами та інфраструктурою для роботи з цінними паперами. Це включає посередників, правила, процедури та процеси, а також організації, які надають послуги з торгівлі, клірингу та розрахунків. Він покладається на установи, які надають рахунки в цінних паперах і пов'язані з ними послуги. Ландшафт торгівлі цінними паперами змінюється з появою нових ринків та інфраструктури. На додаток до традиційних бірж, були запроваджені нові визнані ринки (такі як багатосторонні торгові об'єкти) та інші нові торгові місця, такі як електронні комунікаційні мережі (ECN). ECN – це керовані замовленнями електронні ринки на основі екрана для торгівлі цінними паперами, які обходять традиційних маркет-мейкерів. Крім того, деякі інвестиційні компанії пропонують своїм клієнтам платформи субторгівлі для цінних паперів, якими торгують на кількох біржах. Фінансові ринки, як правило, поділяються на грошові ринки, які обслуговують короткострокові фінансові активи строком менше року, і ринки капіталу, на яких фінансові активи мають термін погашення більше року.

Малюнок 3.2: Правова та нормативна база. Джерело: IOSCO 2013.

Фінансові посередники – це установи, які мобілізують заощадження інвесторів прямо чи опосередковано через фінансові ринки (рис. 3.1), використовуючи різні фінансові інструменти та користуючись послугами багатьох постачальників фінансових послуг; вони, як правило, глибоко регулюються та контролюються. Як правило, розрізняють банки, небанківські фінансові компанії (NBFC), взаємні фонди та страхові організації. Фінансові посередники або установи надають широкий спектр фінансових послуг безпосередньо або через компанії, що працюють у ФС. Сектор фінансових послуг пропонує низку професійних послуг, таких як кредитний рейтинг, фінансування венчурного капіталу, взаємні фонди, комерційні банківські послуги, депозитарні послуги, формування книг тощо.

Правова та регуляторна база відіграє ключову роль у функціонуванні фінансових ринків. Законодавча та нормативна база забезпечує, серед іншого, відповідну структуру регуляторного органу, відповідні повноваження щодо регулювання та нагляду за ринками та продуктами, надійний режим захисту споживачів, дієві правила для прозорих процесів та надійного управління та ефективного система примусового виконання. Крім того, правова система визначає форму кожного типу фінансового посередника в кожній країні. Відтоді як у 2007 році почалася світова фінансова криза, пом'якшення її причин стало головним завданням для глобальних установників стандартів і національних і регіональних державних регуляторів. На глобальному рівні уряди заснували Групу двадцяти (G20) і закликали до регулятивної реформи всього фінансового сектора, щоб запобігти загостренню та можливому повторенню кризи. Координацію цієї великої програми реформ було доручено новоствореній Раді з питань фінансової стабільності (FSB). Інші організації, що встановлюють стандарти, такі як IOSCO та BIS, надають нові глобальні стандарти та принципи. На регіональному та національному рівнях уряди працюють над директивами, законами та постановами для впровадження конкретних реформ (див. рис. 3.2).



Малюнок 3.3: Спрощено логічні зв'язки між гравцями фінансової системи.

Інфраструктури фінансового ринку (FMIs) визначаються як «багатостороння система між фінансовими установами-учасниками, включаючи оператора системи, яка використовується для цілей реєстрації, клірингу або розрахунків за платежами, цінними паперами, деривативами або іншими фінансовими операціями»1. Основна мета механізмів оплати, клірингу та розрахунків полягає в тому, щоб полегшити транзакції між економічними агентами та підтримати ефективний розподіл ресурсів в економіці. Ринкова інфраструктура для платежів та фінансових інструментів є одним із наскрізних основних компонентів фінансової системи, який поєднує всі суб'єкти фінансової системи. Складність і важливість ринкової інфраструктури для обробки платежів і фінансових інструментів значно зросла в останні десятиліття не тільки внаслідок величезного зростання обсягів і вартості фінансових операцій, але також через багатство фінансових операцій. інновації та досягнення в інформаційних і комунікаційних технологіях. Платіжна система складається з трьох основних елементів або процесів:

- платіжні інструменти, які є засобом авторизації та здійснення платежу (засіб, за допомогою якого платник дає своєму банку авторизацію на переказ коштів або засіб, за допомогою якого одержувач платежу дає своєму банку інструкції щодо стягнення коштів із платник);
- обробка (включаючи кліринг), яка передбачає обмін платіжними інструкціями між відповідними банками (та рахунками);
- засіб розрахунку для відповідних банків (тобто банк платника має компенсувати банку одержувача або двосторонньо, або через рахунки, які два банки мають у сторонньому агенті з розрахунків).

[1]IOSCO, 2011

Основні групи зацікавлених сторін	**Учасники**	
Регулюючі органи	Органи фінансового нагляду Управління податкового та фінансового контролю	
Державні установи	Національні центральні банки Державні казначейства	
Зацікавлені сторони фінансової індустрії	**Грошові ринки**	Банки
		Спеціалізовані кредитні установи
		Кооперативні кредитні установи
		Ощадні кооперативи
		Кредитні кооперативи
		Фінансові підприємства
	Ринки капіталу	Інвестиційні фірми
		Менеджери інвестиційних фондів
		Інші установи
	Кошти	Недержавні пенсійні фонди
		Добровільні пенсійні фонди
		Фонди охорони здоров'я та заміщення доходу
	Страхові компанії	Власні страхові компанії
		Компанії взаємного страхування
		Страхові брокери
		Страхові консультанти

Таблиця 3.1: Основні стейкхолдери фінансової галузі.

Платіжна система також покладається на установи, які надають платіжні рахунки, інструменти та послуги клієнтам (включно зі споживачами, підприємствами та державними установами), а також на організації, які надають платіжні, клірингові та розрахункові послуги (такі як міжбанківські системи переказу коштів). Банки та інші фінансові установи є основними учасниками ринкової інфраструктури. Банки є основними постачальниками платіжних рахунків, інструментів і фінансових послуг для кінцевих користувачів. Відносно недавно на ринок вийшли небанківські установи, які надають послуги на різних етапах ініціювання та обробки транзакцій. ІФР, які сприяють кліринґу, розрахункам і реєстрації грошових та інших фінансових операцій, можуть зміцнити ринки, які вони обслуговують, і відіграють вирішальну роль у зміцненні фінансової стабільності. Однак, якщо не керувати належним чином, вони можуть становити значні ризики для фінансової системи та бути потенційним джерелом зараження, особливо в періоди ринкового стресу. Взаємодію між основними компонентами фінансової системи важко представити, оскільки кожен гравець може взяти на себе різну роль у системі та працювати з кількома контрагентами. Синтетичне зображення цієї взаємодії наведено на рисунку 3.3 з урахуванням основного типу логічної взаємодії.

Нарешті, у таблиці 3.1 узагальнено основні зацікавлені сторони фінансової системи, виходячи з цієї загальної моделі.

3.1.2 Вимоги

Фінансова IT-інфраструктура використовується для обробки, зберігання та обміну важливою та конфіденційною інформацією, тому вона характеризується суворими вимогами безпеки. Системи, мережі, дані та інформація, якою обмінюються, повинні бути захищені від будь-якого типу зловмисної діяльності (напр., перехоплення, вставлення підробленої інформації, оновлення, видалення). Фінансова IT-інфраструктура є ключовою КІ для фінансових операторів і, отже, має бути надійною та надійною. Атрибути надійності [165] відносяться до ступеня (піддається кількісній оцінці) впевненості користувача в тому, що система працюватиме, як очікувалося, і що система не дасть збою при нормальному використанні. По суті, IT-фінансова інфраструктура повинна задовольняти наступним вимогам і властивостям надійності та безпеки:

- ***Доступність*** - можливість доступу до систем, мереж і критичних даних для виживання інфраструктури в будь-який час, навіть якщо інфраструктура працює в екстремальних умовах.

- ***Надійність*** - здатність гарантувати, що система або мережа виконуватиме заплановані функції без збоїв при експлуатації в певних умовах протягом визначеного інтервалу часу.

- ***Автентифікація*** - здатність ідентифікувати користувача відповідно до конкретної інформації та типу послуги.

- ***Контроль доступу*** - можливість забезпечити доступ до системних і мережевих ресурсів лише авторизованим користувачам.

- ***Конфіденційність даних і повідомлень*** - можливість гарантувати, що лише авторизовані користувачі можуть отримати доступ до захищених даних і повідомлень.

- ***Цілісність даних і повідомлень*** - здатність гарантувати, що дані, якими керують системи, і повідомлення, що передаються через мережу, не змінюються неавторизованими користувачами або негарантованим програмним або апаратним забезпеченням.

- ***Надійна доставка повідомлень*** — можливість уникнути втрати та реплікації повідомлень і гарантувати впорядковану доставку, а також можливість надати підтверджені докази доставки до обох кінцевих точок зв'язку.

- ***Невідмовність*** — можливість надати перевірений доказ доставки повідомлення до обох кінцевих точок зв'язку, щоб переконатися, що відправник повідомлення не може заперечити, що надіслав повідомлення, і що одержувач не може заперечити отримання повідомлення.

Окрім вимог до надійності та безпеки, фінансова інфраструктура має відповідати вимогам до продуктивності та якості обслуговування (QoS), які характеризуються спеціальними технічними показниками низького рівня для мереж взаємозв'язку (скидання пакетів, час затримки мережі в обидві сторони, тремтіння, неправильна доставка та помилки передачі), а також показники вищого рівня бізнес-рівня (кількість переданих, відсоток відхилених, кількість неправильних транзакцій).

3.2 Стандартні рішення для захисту КІ

Найбільш складним аспектом у фінансових КІ є нова модель, яка встановлюється для фінансових операцій. Ще 20 років тому фінансова трансакція виникла з фінансовою зацікавленою стороною (напр., банком) і була отримана через складну комунікаційну мережу та кілька проміжних вузлів іншою фінансовою зацікавленою стороною (напр., іншим банком в іншому місці). Комунікаційні мережі на той час були досить контрольованими та безпечними. Сьогодні нова модель передбачає транзакції в режимі онлайн і реального часу, які генеруються нефінансовою зацікавленою стороною (бізнес-клієнтом), проходять через фінансових зацікавлених сторін і проміжні вузли, а іноді надходять до іншої нефінансової зацікавленої сторони (напр., підприємства або SME). У цій новій моделі комунікаційна мережа включає багато різних типів мереж і досить часто включає також Інтернет. У такому випадку комунікаційна мережа не може вважатися внутрішньо контрольованою та безпечною.

Комунікації між фінансовими суб'єктами здійснюються за допомогою досить різних технологічних рішень, що забезпечують різні рівні продуктивності, надійності та безпеки: комунікації між фінансовими установами зазвичай використовують виділені виділені лінії зв’язку, офіси центрального банку з’єднані з місцевими установами через інші виділені лінії або через безпечну віртуальну приватну мережу. Мережі (VPN) через Інтернет-посилання.

Сьогодні фінансові організації об’єднані між собою розгалуженими власними мережами, щоб надавати своїм фінансовим клієнтам розширені послуги та безпечно обмінюватися фінансовими повідомленнями для бізнес-цілей (напр., для управління готівкою, переказу коштів, кредитних консультацій, сповіщень). Ці мережі призначені лише для фінансових операцій, а складні вимоги щодо безпеки та конфіденційності призводять до закритих мереж. Зазвичай фінансові мережі ієрархічно пов’язані між собою відповідно до деревовидної структури. У цій моделі взаємозв’язку кожна мережа може розглядатися як вузол на чітко визначеному рівні. Таким чином, дві мережі, що існують на одному рівні, можуть спілкуватися одна з одною, надсилаючи свої повідомлення в мережу на верхньому рівні, що гарантує безпечний і надійний обмін інформацією.

Видані лінії, що з’єднують фінансові установи, спеціально розроблені для високої доступності. Відмовостійкість забезпечується за допомогою багаторазового резервування. Висока надійність також досягається за рахунок ізоляції цих виділених ліній зв'язку щодо Інтернет-трафіку. Цей вибір захищає фінансові комунікації від проблем із доступністю. Виділені лінії зв’язку, які використовуються для обміну інформацією між фінансовими гравцями, можуть забезпечити жорстко контрольоване середовище, у якому можна запровадити політику, орієнтовану на ефективність. У цьому контексті можливість гарантій продуктивності є прямим наслідком ізоляції виділених ліній зв’язку щодо загального Інтернету. В ізольованих мережах досить просто розробити та забезпечити комунікаційну інфраструктуру, продуктивність якої не може бути під загрозою через неконтрольовані Інтернет-явища та/або атаки, які можуть призвести до погіршення продуктивності каналу зв’язку. Крім того, повна ізоляція фінансових мереж від інших забезпечує високий рівень безпеки від вторгнень або збоїв у роботі ззовні. Однак часто буває важко відокремити фінансові мережі від зовнішніх, тому що їм потрібне зручне підключення до інших мереж для обміну важливими даними для фінансових цілей. Тому важливо забезпечити максимальну безпеку мережевого з’єднання за цих умов, використовуючи відповідні політики захисту та технічні рішення, які гарантують повний доступ і безпеку обміну даними. На межі фінансових КІ є зв’язки між фінансовими установами та їхніми клієнтами. У той час як високі гарантії безпеки можна досягти

через виділені канали, комунікація між фінансовим гравцем і його клієнтами здійснюється через Інтернет. Тим не менш, можна гарантувати автентифікацію, неспростовність, конфіденційність і цілісність шляхом використання найсучасніших алгоритмів шифрування та розподілу ключів. VPN можна встановити для забезпечення безпечного зв'язку між відомим і автентифікованим користувачем і (фактично) будь-яким хостом, що належить до внутрішньої мережі фінансової організації. Це рішення можна ефективно використовувати для забезпечення безпечних (але не надійних) каналів зв'язку для клієнтів або співробітників фінансової установи, підключених через Інтернет. Безпека транзакцій буде реалізована на рівні платформи та програми, і продуктивність часто не гарантується. Процеси встановлення та захисту каналу зв'язку та керування транзакціями будуть визначені фінансовими установами, а потім ретельно запроваджені клієнтом (наприклад, використання паролів OTP для підтвердження транзакції). Комунікації, які використовують Інтернет як магістраль, не можуть характеризуватися гарантіями продуктивності. Можна передбачити угоди про рівень обслуговування (SLA), якщо серед фінансових установ є один постачальник або коли трафік обмежується однією автономною системою. Однак у більш загальних випадках неможливо (або дуже важко) гарантувати контракти SLA, коли між кінцевими точками зв'язку задіяно декілька автономних систем. Насправді Інтернет-трафік може бути довільно затриманий або відкинутий проміжною автономною системою, яка базується на службі маршрутизації з найкращими зусиллями.

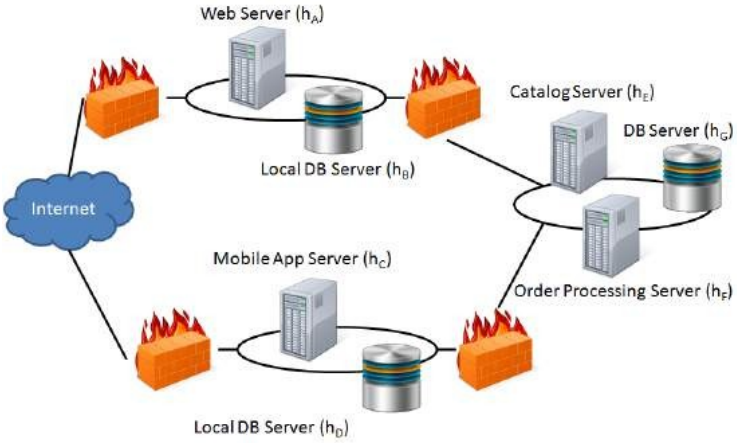
Товариство всесвітніх міжбанківських фінансових телекомунікацій (SWIFT) є найважливішою світовою фінансовою комунікаційною інфраструктурою, яка забезпечує обмін повідомленнями між банками та іншими фінансовими установами. Він був заснований у 1973 році як кооперативне товариство, що належить банкам-учасникам. SWIFT не генерує транзакції, але відповідає за надання швидких, безпечних, доступних і точних засобів передачі різноманітних фінансових інструкцій від імені своїх міжнародних членів. Це приватна мережа, яка надає платформу, продукти та послуги для підключення та обміну фінансовою інформацією між фінансовими організаціями по всьому світу. Тому SWIFT можна розглядати як один із вузлів у верхній частині моделі дерева, що представляє структуру взаємозв'язку європейських фінансових мереж.

3.3 Типи атак і використовувані вразливості

У міру того як сучасне суспільство все більше залежить від мережевих інформаційних систем, кібератаки на IT-інфраструктуру отримують можливість націлюватися на найважливіші служби, якими користується кожен громадянин у своїй повсякденній діяльності. Кібератаки на IT-інфраструктуру фінансових установ та їхніх клієнтів є типовими для цієї тенденції. Переважна більшість фінансової діяльності здійснюється за допомогою мережевих комп'ютерів, а взаємодія між фінансовими установами та їхніми клієнтами зазвичай здійснюється через відкритий Інтернет. Цей ландшафт відкриває нові можливості для зловмисників. Зокрема, можливість скомпрометувати безпеку онлайн-фінансових транзакцій є особливо привабливою, оскільки вони дають зловмиснику можливість легко монетизувати успішну атаку.

У цьому контексті кілька різних стратегій атак уже використовувалися в недавньому минулому для підготовки або здійснення шахрайства та вимагання від банків та їхніх клієнтів. Ці кібератаки надзвичайно різнорідні: від внутрішніх загроз до вторгнення в мережу зовнішнього зловмисника, від атак, націлених на певну фінансову установу, до широко поширених кампаній СПАМу та фішингу, від використання вразливостей у програмному забезпеченні, що використовується фінансовими установами, до вторгнення в персональні комп'ютери клієнтів.

Найпоширенішими стратегіями атак є: Man-in-the-Middle, сканування портів, розподілена відмова в обслуговуванні, захоплення сесії та атаки на клієнтів фінансових установ із застосуванням зловмисного програмного забезпечення. Усі ці атаки мають спільну рису, яка робить їх особливо актуальними: вони залучають кілька об'єктів. Атаки Man-in-the-Middle спрямовані на кількох клієнтів і, можливо, на кілька фінансових установ. Діяльність Portscan регулярно виявляють практично всі фінансові установи, і часто виконуються кількома скоординованими зловмисниками. Розподілена відмова в обслуговуванні є добре відомою загрозою, яка нещодавно була націлена на кілька фінансових установ, джерела яких є географічно розподіленими. Методи викрадення сесії можна використовувати для порушення цілісності фінансових операцій, які здійснюються декількома клієнтами. Нарешті, банківське зловмисне програмне забезпечення зазвичай представлене самовідтворюваним програмним забезпеченням, яке атакує сотні тисяч уразливих персональних комп'ютерів, таким чином націлюючись на велику кількість клієнтів фінансових установ.



Малюнок 3.4: Приклад архітектури мережі електронної комерції

Крім того, є багато випадків, коли стратегії атак мають більш складні структури, визначені різними шаблонами. Враховуючи послідовність зареєстрованих дій, тоді необхідно шукати підпослідовності журналу, які відповідають атаці. Моделі атак повинні бути здатними представляти моделі з багатьма альтернативами та відповідними обмеженнями. Розглянемо, напр., архітектуру мережі електронної комерції, показану на малюнку 3.4. Ця мережа складається з 3 підмереж, розділених міжмережевими екранами. 2 підмережі містять хост, доступний з Інтернету. III-я підмережа реалізує бізнес-логіку та включає центральний сервер бази даних. Зловмиснику, який хоче викрасти конфіденційні дані з центрального сервера бази даних, потрібно буде зламати брандмауери та отримати привілеї на кількох хостах, перш ніж досягти цілі.

Тепер припустимо, що існує дуже простий шаблон атаки, який включає наступні дії:

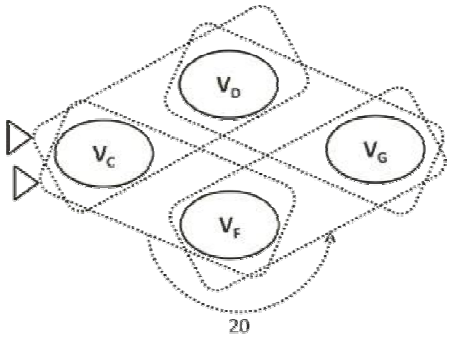
1. Використання вразливості VC на сервері мобільних додатків,

2. Використання уразливості VD на сервері DB hD або уразливості VF на сервері обробки замовлень,

3. Використання вразливості VG на центральному сервері БД.

Також припустимо, що переміщення через сервер обробки замовлень викликає базове попередження безпеки, яке запобігає зловмисникам отримати доступ до центрального сервера БД, якщо загальний час транзакції перевищує 20 одиниць часу. Цей шаблон можна представити простим графом на малюнку 3.5, де додано часове обмеження між ребрами (VC, VF) і (VF , VG).

Цей простий приклад показує, що (гіпер-)графи можуть виявитися дуже ефективними як основа для моделей атак. Наші знання про складну поведінку зловмисника можна формально закодувати за допомогою гіперграфа, де вершини представляють можливу групу подій (тобто дії зловмисника або вразливості, які можна використовувати), а гіперребра серед вершин визначають часову послідовність атаки (як асоціації між вершинами), з передбачуваним значенням того, що події, що належать одному гіперребру, повинні бути завершені в межах визначеного часового вікна в будь-якому можливому порядку. Крім того, моделі атак повинні дозволяти вказувати різного роду обмеження під час можливих атак, зокрема в термінах причинно-наслідкових зв'язків, які зберігаються над гіперребрами, і, отже, над подіями, які вони групують разом. Тоді важливо визначити та вивчити форми обмежень, які забезпечують високий ступінь гнучкості в представленні різних сценаріїв безпеки. Крім того, необхідно ефективно вирішувати проблеми перевірки узгодженості та/або надмірності моделей атак, а також ефективного виявлення випадків атак у послідовностях зареєстрованих дій.



Малюнок 3.5: Приклад графіка атак

3.4 Стратегії захисту

У цьому розділі розглядаються стратегії захисту, спрямовані на запобігання будь-якому ефекту від атак. Стратегії зазвичай подвійні. І-ша стратегія полягає в тому, щоб визнати, що певна служба справді вразлива, і протидіяти цій вразливості, зробивши потенційну винагороду від атаки якомога меншою. Інша стратегія полягає в зменшенні вразливості майже до нуля. Обидві стратегії зробили б неприваблівим атаку на службу, і можна було б очікувати, що атак не відбудеться.

Постійний порядок. Використання постійних доручень зростає. Постійне доручення – це угода між клієнтом банку та банком, яка автоматично здійснює платежі, тобто дебетує рахунок клієнта та надсилає відповідну кредитну інструкцію банку-кредитору. Існує одна угода для кожної пари боржник/кредитор. У договорі часто встановлюється обмеження щодо вартості кожного платежу. Договір є безперервним, тобто на повторні платежі діє один і той самий договір до моменту розірвання договору замовником. Кредитор також повинен укласти договір з банком. Зловмисника слід було б визнати законним кредитором для платежів за постійним дорученням як перший крок до обману клієнтів. Платежі здійснюються автоматично на основі інформації, яка централізовано зберігається в банках. Клієнту не потрібно входити в систему, щоб платіж відбувся. Тому існує обмежений простір для троянів, Man-in-the-Middle, Man-in-the-Browser, коли мова йде про зміну інформації про транзакції. Збільшення використання постійних доручень

обмежить поле для шахраїв.

Електронне виставлення рахунків. Використання електронних рахунків-фактур повільно зростає в Європі. Завдяки електронному виставленню рахунків уся інформація щодо платіжних інструкцій стає доступною для клієнта через Інтернет-банкінг. Іншими словами, клієнт не вводить платіжну інформацію, наприклад, суми, номер кредитного рахунку. Клієнт або приймає електронний рахунок-фактуру, або відхиляє його. Кредитор і боржник повинні укласти угоди зі своїми банками, щоб налаштувати електронне виставлення рахунків.

Як із постійними дорученнями, так і з електронним рахунком-фактурою платник не вводить платіжну інформацію, і для порушника дуже мало можливостей для зміни платіжної інформації.

Одноразовий пароль. Зараз кілька банків використовують одноразовий пароль для входу клієнта в Інтернет-банк. Основна ідея полягає в тому, що після того, як клієнт увійшов у систему, жоден самозванець, який отримав фішинг або іншим чином отримав доступ до коду, не може увійти, використовуючи той самий код. Проте, використовуючи більш-менш просунуті схеми фішингу, самозванці змогли отримати доступ до коду ще до того, як він потрапив до банку. Один із випадків схеми наблизився до повної автоматизації, оскільки зловмисники надавали клієнтам банківської системи автоматизований інтерфейс до банківської програми, через який відбувався вхід, надаючи зловмисникам повний доступ до облікового запису клієнта. Для боротьби з цим типом атак деякі банки запровадили автентифікацію транзакцій. Це означає, що клієнт повинен вводити окремий одноразовий пароль (OTP) під час надсилання кожної транзакції, тобто після та на додаток до OTP, поданого під час входу в систему. до інтернет-банкінгу. Однак багато OTP-токенів (пристроїв, які виробляють OTP) синхронізовано за часом із машинами, на яких розміщено Інтернет-банкінг. Оскільки годинники, як правило, дещо відрізняються, і для того, щоб вистачило часу на передачу та обробку коду, існує часове вікно, у межах якого OTP є дійсним. Це часове вікно дозволяє зловмисникам підманити два коди, які згодом виявляються дійсними; один для входу та один для автентифікації (шахрайської) транзакції.

Антивірус. Кілька банків зараз пропонують клієнтам безкоштовне антивірусне програмне забезпечення для завантаження та запуску на своїх комп'ютерах. Їй відведено чільне місце на домашній сторінці банків, і клієнтам настійно рекомендується завантажити її. Постачальники антивірусів беруть участь у гонці озброєнь проти виробників шкідливих програм, і вони протистоять добре організованому та винахідливому противнику. Останнім часом ми спостерігаємо злиття двох виробників шкідливих програм (Spyeye і Zeus). Вдосконалені шкідливі програми, наприклад, поліморфні варіанти, динамічно змінюють свій підпис і можуть уникнути антивірусного програмного забезпечення. Тому ефективність і ефективність антивірусного програмного забезпечення ставиться під сумнів. Після атаки на норвезьких клієнтів онлайн-банкінгу аналітики безпеки повідомили, що більше половини перевірених заражених систем працювали під керуванням повністю оновлених версій антивіруса та операційної системи.

Аналіз транзакцій. Щоб виявити та зупинити неавторизовані транзакції, банки виконують внутрішній аналіз транзакцій як негайно, так і ретроспективно. Відомо, що під час нещодавньої хвилі атак на банки в Норвегії бек-енд-аналіз запобіг збиткам. Транзакції порівнювалися з чорними списками рахунків. Слід трояна було ідентифіковано, і транзакції, які збігалися із слідом, були зупинені. Є компанії, які вправно збирають сліди та ознаки того, що облікові дані автентифікації було зламано. Компанії розміщують ці сліди на так званих сайтах, які містять профілі скомпрометованих користувачів.

Команда реагування на комп'ютерні надзвичайні ситуації. Кілька банків підписалися на CERT. У кількох країнах CERT є державними органами. CERT укомплектовано висококваліфікованими техніками, які аналізують трафік і моделі трафіку на предмет можливих атак. Під час нещодавньої атаки в Норвегії норвезький національний CERT зіграв визначну роль в аналізі трояна, а також використав свої повноваження, щоб переконати провайдерів закрити IP-адреси центру керування та управління трояном.

Захист від комплексних атак. Більшість компаній сьогодні використовують різноманітні технології для виявлення та запобігання підозрілій діяльності. Загальні технології включають використання брандмауерів для їх виявлення на периметрі мережі, антивірусних пакетів для виявлення шкідливого коду, що проникає в системи компанії з різних джерел, і програмного забезпечення виявлення вторгнень (IDS) для сканування пакетів у мережах і моніторингу різноманітних сумнівних дій. на серверах додатків і на рівні операційної системи. Ці методи зазвичай дуже ефективні, коли використовуються для оцінки вразливостей як окремих дій. Однак вони не пропонують необхідного рівня захисту від зловмисних дій, які виконуються разом, що призводить до складних (і загалом більш потужних) типів атак. Щоб протистояти складним атакам, компанії можуть створити спеціалізовану групу безпеки (або CERT), але це часто досить дорого, а її діяльність може потребувати часу та ресурсів. З цих причин нова парадигма безпеки полягає у прийнятті нових типів технологій на основі стратегії захисту рівня. Основна ідея полягає в тому, щоб закодувати знання про конкретні комплексні атаки у відповідну формальну модель, яка описує поведінку зловмисника як комбінацію менших атак. Отримана модель використовується для цілей аналізу та/або як прогностична модель для виявлення майбутніх атак. Насправді найкращі практики безпеки демонструють, що моделі атак (наприклад, графіки атак, дерева, гіперграфи) можна застосовувати для підтримки наступальних (напр., тестування на проникнення) та/або захисних (напр., посилення мережі) стратегій у широкому спектрі безпеки. контексти, включаючи аналіз вразливості [134, 108], кореляцію тривоги про вторгнення [178, 179] і відповідь на атаку [74]. Наприклад, такі моделі, як графіки атак, успішно використовуються для визначення всіх потенційних шляхів уразливості, тим самим демонструючи, як зловмисники можуть проникнути через мережу [41, 42, 45]. Підхід полягає в моделюванні конфігурації мережі (топології, пристроїв, що обмежують з'єднання, таких як брандмауери, уразливості тощо), а потім у моделюванні атак (зокрема, проникнень) через мережі. Набори шляхів атаки (для успішних атак) можна зібрати та організувати в структуру на основі графіка, яку можна повторно використовувати як прогнозну дорожню карту для реальних атак. У контексті виявлення вторгнень моделі атак також експериментували для моделювання комп'ютерних мереж, які захищені IDS, і для співвіднесення великої кількості попереджень, створених цією IDS, із діями в моделі атаки [142, 181, 182]. Сповіщення, які надходять у передбаченій послідовності під час проходження одним шляхом атаки, можуть означати, що зловмисник успішно виконує кроки на цьому шляху. Ранні підходи також експериментували з використанням моделей атак у контексті виявлення аномалій, де модель, що кодує нормальну поведінку як комбінацію дій, використовується для автоматичного вивчення та виявлення нормальної/ненормальної поведінки в спостережуваних діях [180, 135].

Захід охорони на вимогу. У деяких країнах Інтернет-банки використовують рішення для автентифікації клієнтів, які також використовуються для автентифікації клієнтів на інших веб-сайтах. Іншими словами, є один сервер автентифікації, який обслуговує всі сайти. Рішення часто використовує коди OTP як частину автентифікації. Це означає, що будь-який код OTP буде дійсним для будь-якого з веб-сайтів, включаючи Інтернет-банкінг. Оскільки рішення автентифікації набуває поширення, все більше веб-сайтів запитують у клієнтів їхні облікові дані. Раніше облікові дані для автентифікації подавали лише в контексті Інтернет-банкінгу. Тепер люди отримують запити на введення облікових

даних у різних контекстах, наприклад, у контексті різноманітних онлайн-магазинів, у контексті входу в державні служби тощо. За цих нових обставин громадськості важче проявляти пильність і знати, хто стоїть за цим веб-сайтом і запитує їхні облікові дані. У результаті неможливості здійснювати контроль люди, як правило, стають менш критичними, коли справа доходить до того, кому надіслати облікові дані для входу. Це приклад фішингу. Зловмисник міг видати себе за інтернет-магазин і підманити облікові дані для входу, а потім повернутись і використати облікові дані для входу в Інтернет-банкінг. Крім того, веб-сайт, уповноважений приймати облікові дані для автентифікації, може використовувати облікові дані для неавторизованих цілей, обманюючи клієнта. Щоб боротися з цією загрозою, організація, що стоїть за рішенням автентифікації, придумала ідею контекстно-залежного MAC. Це означає, що одноразовий пароль видаватиметься для кожного веб-сайту, тобто фішинговий одноразовий пароль буде дійсним лише в контексті одного конкретного веб-сайту. MAC, отриманий у зв'язку з онлайн-покупками, не можна використовувати для входу в онлайн-банк. Це, звичайно, усуне основну мотивацію для фішера.

Роумінг автентифікації. Багато рішень для автентифікації онлайн-банкінгу є роумінговими, тобто клієнт може отримати доступ до Інтернет-банку з будь-якого ПК, використовуючи той самий механізм автентифікації. Це є підставою для фішингу, оскільки підроблені облікові дані автентифікації можуть бути миттєво використані зловмисником із ПК зловмисника. Щоб протистояти цьому аспекту переносимості автентифікації, відомо, що банки створили таблицю з MAC-адресами та відповідними ідентифікаторами входу. Вони створили цю таблицю, записавши MAC, які користувач регулярно використовує. У разі атаки, шукаючи будь-якого клієнта в цій таблиці, банк перевірить MAC-адресу та дозволить доступ лише з цієї адреси або обмеженої кількості інших машин, якими клієнт користується.

3.5 Підходи до зменшення несправностей

Завдяки ролі, яку відіграє в економічному розвитку, фінансову систему можна вважати одним із найбільш регульованих секторів. Задіяна нормативна база використовує фінансові IT-вимоги та процеси управління ризиками для створення надійної фінансової системи. Насправді фінансова IT-інфраструктура в основному використовується для обробки, зберігання та обміну важливою та конфіденційною інформацією, тому вона характеризується суворими вимогами безпеки. Системи, мережі, дані та обмінювана інформація повинні бути захищені від будь-якого типу зловмисної діяльності (наприклад, перехоплення, вставлення підробленої інформації, оновлення, видалення). Актуальність вимог безпеки у фінансовому контексті підкреслюється як на рівні фірм (фінансових посередників/установ), так і на рівні інфраструктур фінансових ринків, зосереджуючись на управлінні операційними ризиками та/або управлінні безперервністю бізнесу. Управління операційним ризиком зосереджується на кожному можливому ризику, який потенційно може вплинути на безперебійну роботу системи чи служби. У фінансовому секторі операційний ризик має різноманітні системні наслідки, враховуючи дедалі більший розмір, взаємопов'язаність і складність фінансових установ, що збільшує ймовірність помилок і шахрайства. Збої в надходженні фінансових послуг через знецінення всієї фінансової системи або її частини можуть призвести до системного ризику та можливого переливу на реальну економіку. Керування безперервністю бізнесу розглядає один аспект, операційні збої, які можуть порушити надання ключових послуг. Тому ці дві дисципліни мають загалом схожість і перетинаються: управління безперервністю бізнесу можна розглядати як спеціалізовану дисципліну, яка доповнює та є частиною загального процесу управління операційним ризиком. Визнані найкращі практики та стандарти свідчать про те, що ефективна програма управління безперервністю бізнесу, як правило, повинна включати наступні чотири ключові елементи: і) аналіз впливу на бізнес з метою визначення критичних видів діяльності

та визначення цілей відновлення; ii) чітко визначена стратегія безперервності бізнесу; iii) відповідні плани та процедури для забезпечення безперервності критичних послуг; iv) тестування, підтримка та перегляд існуючих планів з метою підтвердження їх ефективності та забезпечення їх актуальності.

Стосовно фінансових посередників, зокрема банків, основні нормативні приписи у сфері операційного ризику містяться в нових угодах про капітал, так званих Базель II і III [4] (BIS). Збитки, спричинені порушенням безпеки фінансової IT-інфраструктури, як правило, підпадають під цю категорію ризику, як визначено в першій основі Базель III[3] і Додатку 9[2]. Зокрема, проблеми безпеки системи (такі як хакерські дії та викрадення даних) розглядаються як приклади зовнішнього шахрайства, визначеного (серед іншого) в межах операційних ризиків.

Після фінансової кризи, яка спалахнула в 2008 році, Європейський комітет банківського нагляду (CEBS) видав рекомендації, які повністю або частково охоплюють аспекти внутрішнього управління кредитними установами та інвестиційними компаніями; зокрема, у п'ятому розділі «Системи та безперервність» було додано нові рекомендації щодо інформаційних та комунікаційних систем та управління безперервністю бізнесу. Замість того, щоб формулювати розширені вимоги до IT-систем, керівництво посилається на загальноприйняті стандарти в цьому питанні. Принципи безперервності бізнесу узгоджуються з «Принципами високого рівня безперервності бізнесу» BCBS. В Італії Банк Італії (відповідальний за видання вторинного законодавства з технічних питань щодо фінансових посередників і за втручання пруденційного характеру) забезпечує дотримання як національного законодавства, так і європейських директив і нормативних актів, усіх вимог, необхідних для досягнення комплексного управління IT системи як з точки зору безпеки, так і надійності. У цьому відношенні 15-те оновлення (2 липня 2013 р.) «Циркуляру № 263 – Нові правила пруденційного нагляду за банками» є одним із найновіших довідкових документів у цій галузі; він дисциплінує організацію внутрішнього контролю, функціонування, ролі та обов'язки, пов'язані з розробкою та управлінням італійськими фінансовими інформаційними системами. Це втручання транспонує керівні принципи CEBS до італійської нормативної бази. Серед інших найважливіші нововведення стосуються:

- ***Дисципліни інформаційних систем***. Дисципліна інформаційних систем, враховуючи основні події, які виникли на міжнародній арені та встановлюють основні складові управління та організації інформаційної системи, управління IT-ризиками, усі вимоги щодо забезпечення безпеки та управління системою даних. Положення також передбачають, що визначення безпеки принципалів для доступу до критичних систем і послуг через Інтернет-канал застосовуються Рекомендації ECB у сфері безпеки онлайн-платежів.

- ***Дисципліни безперервності бізнесу***. Дисципліна безперервності бізнесу шляхом реорганізації положень, які зараз містяться в різних нормативних джерелах. Серед іншого було визначено процес швидкої ескалації аварії в надзвичайних ситуаціях, щоб гарантувати, що оголошення кризового стану відбулося в найкоротший час з моменту виявлення аварії. Загальний час відновлення не перевищуватиме чотирьох годин, включаючи час на етапах аналізу, прийняття рішень, технічної допомоги та верифікації.

- ***Формалізації ролі робочої групи CODISE***. Формалізація ролі робочої групи CODISE (робочої групи з безперервності бізнесу, створеної в 2002 році) як структури, відповідальної за координацію антикризового управління, що діє в італійській фінансовій системі. Групу координує Banca d'Italia за погодженням з CONSOB (Італійська біржова комісія) і складається з представників провідних

банківських груп і компаній, які керують інфраструктурою, необхідною для нормальної роботи фінансової системи.

Концепції пом'якшення помилок втілені в процесі аналізу ризиків і в розділах документа про доступність інформації. Нижче наведено основні принципи:

Аналіз ризиків. Аналіз ризиків ІКТ-ресурсів є інструментом для забезпечення ефективності та результативності стратегій їх захисту. Це дозволяє регулювати заходи пом'якшення на основі сфери, в якій працює система. Необхідно оцінити ризик, якому піддаються ресурси ІКТ. Це передбачає як розвиток нових структур, так і оновлення існуючих. Аналіз ризиків забезпечить рівні класифікації, потенційні ризики та залишки, списки розглянутих загроз, списки індивідуальних активів і періодично повторюватиметься відповідно до критичності ресурсів ІКТ.

Доступність інформації. Доступність інформації та доступність ресурсів ІКТ гарантується користувачам відповідно до угод про рівень обслуговування[2]. З цією метою всі процеси:

- проектування архітектурних моделей;
- розвиток програмного забезпечення та інфраструктури;
- управління несправностями;
- планування можливостей передачі та моніторинг;
- планування та моніторинг можливостей обробки;
- управління провайдерами;

необхідні враховувати наступні вказівки:

Моніторинг SLA

Рівні обслуговування, яких слід дотримуватися, формально визначені, особливо щодо програм, які мають вищий рівень критичності. Необхідно регулярно контролювати продуктивність компонентів і активів, необхідних для отримання цільового рівня обслуговування.

Резервне копіювання за межами сайту

Відповідно до вимог доступності кожного активу, програмного забезпечення або послуги, необхідно визначити процедури резервного копіювання програмного забезпечення та конфігурацій, даних і апаратних систем. Зовнішнє резервне копіювання має бути готове та превентивно індивідуальне.

Жодної точки відмови

Що стосується попереднього пункту, кожна архітектура повинна бути розроблена з урахуванням профілів безпеки розміщених програм. Усі ресурси ІКТ та допоміжні ресурси (електроживлення, системи охолодження тощо) мають бути належним чином резервованими та надійними, не повинно бути єдиної точки відмови. Вищу доступність слід надавати для програм із вищим рівнем критичності, також відповідно до планів аварійного відновлення.

Резервування з'єднань

Відповідно до профілювання ризиків комунікаційних систем, додатків і послуг, до яких здійснюється

доступ, кожен банк або фінансова установа має відновити зв'язки ІКТ, а також спеціальні рішення для виявлення та блокування зловмисного трафіку, а банк повинні оцінити процедури та інструменти динамічного розподілу передавальної та обчислювальної потужності.

Стандартизація

Управління системами ІКТ належним чином автоматизоване та використовує, здебільшого, стандартні процедури. Операції планового та позачергового технічного обслуговування повинні бути спланованими та своєчасно охоплювати всіх зацікавлених користувачів.

[2]Слід брати до уваги профіль використання клієнтів (відомий або передбачуваний) протягом робочих годин і потенційні стрибки використання.

Площа	**Основний зміст**
Загальна організація	Принцип 2 щодо управління вимагає, щоб FMI мала надійні механізми управління, які зосереджуються на безпеці та ефективності FMI і підтримують стабільність ширшої фінансової системи, інших міркувань суспільного інтересу та цілей відповідних зацікавлених сторін.
	Принцип 3 щодо основи комплексного управління ризиками вимагає від ІФР комплексного та всебічного уявлення про свої ризики, включно з тими, які вона несе від своїх учасників, їхніх клієнтів та інших організацій.
Операційний ризик	Принцип 17 посилює вимоги до експлуатаційної надійності та стійкості[3].
Доступ	Принцип 18 містить вказівки для FMI щодо встановлення належної політики доступу, яка забезпечує справедливий і відкритий доступ, одночасно забезпечуючи власну безпеку та ефективність FMI.
Ефективність	Принцип 22 щодо використання комунікаційних процедур і стандартів. FMI має використовувати або, як мінімум, відповідати міжнародно прийнятим процедурам і стандартам комунікації для підвищення ефективності[4].

Таблиця 3.2: Принципи PFMI щодо безпеки. Джерело: CPSS-IOSCO, 2012.

Планування потужностей

Інформація, отримана за допомогою моніторингу ресурсів ІКТ, регулярно надходить у планування потужностей і повинна використовуватися при проектуванні та оновленні інформаційної системи.

Тим не менш, важливу роль відіграє комплексний план безперервності бізнесу (BCI), який завжди слід дотримуватися, щоб забезпечити доступність критичних фінансових послуг.

Як повідомлялося вище, FMI є важливими учасниками усунення фінансових ризиків, але вони повинні гарантувати, що вони самі не стануть джерелами неприйнятного ризику у фінансовій системі, особливо в умовах серйозного стресу. У цій сфері Комітет з платіжних і розрахункових систем (CPSS) і Технічний комітет Міжнародної організації комісій з цінних паперів (IOSCO) зробили внесок у набір стандартів, кодексів і найкращих практик, які вважаються важливими для зміцнення фінансової архітектури в усьому світі. .

У квітні 2012 року було видано важливий документ «Принципи інфраструктури фінансового ринку»[5].

24 принципи, викладені в цьому звіті, поділяються на 9 широких категорій: (a) загальна організація, (б) кредитний ризик і ризик ліквідності управління, (c) розрахунки, (d) центральні депозитарі та системи розрахунків за обміном вартості, (e) управління дефолтом, (f) загальне управління діловими та операційними ризиками, (g) доступ, (h) ефективність та (i) прозорість. Ці широкі категорії охоплюють основні елементи, критичні для безпечного та ефективного проектування та роботи FMI. Таблиця 3.2 висвітлює найважливіші принципи, пов'язані з нашою сферою досліджень.

[3]Наприклад, управління безперервністю бізнесу має бути спрямоване на своєчасне відновлення роботи та виконання зобов'язань ІФР, у тому числі у випадку широкомасштабного чи значного збою. Плани забезпечення безперервності бізнесу мають бути розроблені таким чином, щоб ІФР могла завершити врегулювання до кінця дня збою навіть у екстремальних обставинах, а критичні системи мають бути розроблені таким чином, щоб операції могли бути відновлені протягом двох годин після збою.

[4] Для FMI, яка здійснює транскордонну діяльність або надає транскордонні послуги, використання міжнародно прийнятих процедур і стандартів зв'язку є особливо важливим.

CPSS та IOSCO також нещодавно (серпень 2013 р.) опублікували для публічного обговорення консультативний звіт щодо відновлення інфраструктури фінансового ринку. Доповідь призначена на:

- надання додаткових вказівок та меню інструментів для дотримання PFMI, враховуючи різні типи FMI;
- відповідання Ключовим характеристикам ефективних режимів санації фінансових установ FSB;
- надання вказівок щодо процесу планування відновлення та змісту планів відновлення.

На європейському рівні, розглядаючи FMI, ми можемо розглянути три сфери основних вимог:

- ***Роздрібні платіжні системи***: RPS використовуються для більшості платежів фізичним особам і від них, а також між фізичними особами та фірмами; ці системи наразі підлягають серйозним змінам у результаті впровадження Єдиної зони платежів у євро (SEPA). Навіть якщо багато з них не мають системного значення, вони відіграють важливу роль як для безпеки та ефективності фінансової системи в цілому, так і для довіри громадян до євро. Визнаючи актуальність роздрібних платіжних систем, Євросистема запровадила «Стандарти нагляду для роздрібних платіжних систем у євро», які розрізняють системно важливі платіжні системи, надзвичайно важливі платіжні системи та інші, і визначають, які з Основних принципів також є актуальні для важливих роздрібних платіжних систем. Щоб забезпечити послідовне застосування цих стандартів нагляду різними NCB та ECB, Євросистема випустила загальну методологію для оцінки систем за відповідними стандартами.

- ***Платіжні системи великих сум***: LVPS утворюють основу ринкової інфраструктури єврозони. Євросистема застосовує Основні принципи для системно важливих систем CPSS і вдосконалила їх, опублікувавши «Очікування щодо безперервності бізнесу для системно важливих платіжних систем», де детально розкриваються аспекти безперервності бізнесу Основного принципу щодо безпеки, операційної надійності. і безперервність бізнесу.

- ***Системи клірингу та розрахунків за цінними паперами та деривативами***: збої системи та процесів є особливо небезпечними, якщо вони відбуваються під час клірингу та розрахунків за фінансовими операціями, а також під час торгівлі та ціноутворення фінансових інструментів. Інфраструктури та механізми обробки цінних паперів є певною мірою складнішими, ніж інфраструктури обробки платежів. Оскільки цінні папери, як правило, доставляються в обмін на оплату, слід враховувати дві сторони поставки: готівкову сторону та цінних паперів. Робота з цінними паперами також включає ширше коло функцій та учасників.

[5]The new standards replace the three existing sets of international standards set out in the Core principles for systemically important payment systems (CPSS, 2001); the Recom- mendations for securities settlement systems(CPSS-IOSCO, 2001); and the Recommenda- tions for central counterparts (CPSS-IOSCO, 2004)

Рівень втручання	**Документи**	**Основний зміст**
Платіжні системи	Основні принципи для системно важливих платіжних систем, Банк міжнародних розрахунків (прийнятий Радою керуючих ЕСВ у січні 2001 р.).	Зокрема Основні принципи VII: Система повинна забезпечувати високий рівень безпеки та експлуатаційної надійності та повинна мати механізми на випадок непередбачених ситуацій для своєчасного завершення щоденної обробки
	Очікування щодо нагляду за безперервністю бізнесу для системно важливих платіжних систем (SIPS), (ЕСВ, червень 2006 р.).	Документ представляв собою переглянуту Керівні принципи, описані в цьому документі у формі наглядових очікувань, визначають ключові елементи управління безперервністю бізнесу. Вони сприятимуть забезпеченню рівня стійкості з боку SIPS у всій єврозоні, який відповідає меті, встановленій CP VII.
	Розпорядження №260/2012	Common technical standards established for processing SEPA payments, necessary to allow interaction and interoperability between IT systems and to ensure an automated process- ing of euro-denominated transactions between payment service providers (PSPs), referred to as “straight-through processing”. The reg- ulation requires the use of certain common standards and technical requirements, such as the financial services messaging standard ISO 20022 XML for all credit transfers and direct debits in euro in the EU.
Платіжні інструменти	Гармонізований підхід до нагляду та стандарти нагляду за платіжними інструментами (ЕСВ, лютий 2009 р.)	Стандарт 3: Схема повинна забезпечувати достатній рівень безпеки, операційної надійності та безперервності бізнесу. Для пом’якшення операційних ризиків повинні бути встановлені адекватні засоби контролю безпеки. У зв’язку з цим, керівний орган повинен переконатися, що всі відповідні учасники схеми зосереджені на управлінні ризиками та безпекою, безперервності бізнесу та аутсорсингу, забезпечивши наявність відповідних технічних стандартів і процедур.
	Структура нагляду за схемами прямого дебету, жовтень 2010 р	Метою наглядової системи для схем прямого дебету та схем кредитних переказів є забезпечення надійності та ефективності платежів, здійснених за допомогою таких інструментів. Було визначено п’ять стандартів, які стосуються правових питань, прозорості, операційної надійності, належного управління та надійних клірингових і розрахункових процесів; зокрема стандарт n. 3 говорить про необхідність забезпечення належного рівня безпеки, операційної надійності та безперервності бізнесу.
	Структура нагляду за схемами кредитних переказів, жовтень 2010 р	

	Том стандартизації карток SEPA - Книга вимог, версія 6.0 (EPC, січень 2012 р.)	Том визначає вимоги стандартів до карток і терміналів. Він також визначає функціональні вимоги та вимоги до безпеки, включно з вимогами до методології та архітектури оцінки та сертифікації, які рекомендовані EPC для прийняття в усьому ланцюжку створення вартості карткових платежів для забезпечення сумісності в рамках SEPA. Вимоги до безпеки (зокрема «картка відсутня» та інноваційні платежі), а також сертифікати включені до Тома.
	Рекомендації щодо безпеки мобільних платежів. проект документа для публічних консультацій (ECB, листопад 2013 р.)	У звіті викладено 14 рекомендацій, що становлять мінімальні очікування щодо сприяння безпеці мобільних платежів, згрупованих у три категорії.
Клірингові та розрахункові системи	Лінія політики Євросистеми щодо консолідації в клірингу центрального контрагента (ECB, вересень 2001 р.)	Рекомендації спрямовані на просування ефективних, безпечних і надійних загальноєвропейських пост-торгових механізмів з метою підвищення довіри до ринків цінних паперів, забезпечення кращого захисту інвесторів, стримування системного ризику та сприяння фінансовій стабільності
	Заява Євросистеми про центральних контрагентів і взаємодію, технічне завдання (ECB, березень 2008 р.)	

Таблиця 3.3: Перелік стандартів і найкращих практик на рівні ЄС щодо платіжних систем.

Таблиця 3.3 підсумовує найбільш релевантні джерела стандартів і нормативної бази щодо FMI в Європейському Союзі.

Нарешті, останнім часом більша увага приділяється стороннім постачальникам послуг, яким платіжні та розрахункові системи доручають виконання всіх або частини своїх операцій (наприклад, їхня IT-інфраструктура); ці постачальники можуть мати вирішальне значення для функціонування цих систем. Для Євросистеми ключовим принципом є те, що окремі системи зберігають повну відповідальність за будь-яку діяльність, яка є суттєвою для їх діяльності, включаючи відповідальність за забезпечення дотримання постачальником послуг застосовної політики нагляду. Лише тоді, коли постачальник послуг надає важливі послуги більш ніж одній ключовій системі, здійснюватиметься безпосередній нагляд. Наприклад, це стосується SWIFT, глобального постачальника міжбанківських фінансових телекомунікаційних послуг.

3.6 Відкриті проблеми

Фінансові послуги та організації за своєю природою підлягають низці проблем безпеки. Багато стандартів і правил зараз активно впливають на те, як організації керують внутрішньою та зовнішньою безпекою. Використання вразливостей програмного забезпечення є поширеним вектором загроз, відповідальним за ряд порушень, які, на жаль, часто залишаються непоміченими жертвою протягом тривалого часу [50]. У цих випадках зловмисне програмне забезпечення, бекдор, кейлогер

або інше зловмисне програмне забезпечення може залишатися оперативним і непоміченим у системі-жертві місяцями, якщо не роками. Шкода, яку це може завдати фінансовій установі та її клієнтам, може бути величезною. З цієї причини такі стандарти, як Стандарт безпеки даних платіжних карток (PCI-DSS), регулюють, які вразливості має виправляти організація (за допомогою процесу, що називається виправленням). Серед найважливіших причин відповідності вимогам, відповідальність у разі нещасних випадків, безперечно, є одним із головних факторів, які підштовхують організацію до сертифікації.

Зберігаючи PCI-DSS як приклад, організації повинні виправляти вразливості відповідно до свого рейтингу CVSS, галузевого стандарту для оцінки ризику вразливості [131]. Оцінка CVSS використовується в цьому контексті, щоб забезпечити «поріг ризику», вище якого необхідно усунути всі вразливості. Очевидно, що цей поріг є предметом компромісу. З одного боку, потрібно виправити якомога більше вразливостей, щоб покрити найбільш «ризиковані» вразливості. З іншого боку, встановлення надто низького граничного значення призведе до створення кількості вразливостей, якими неможливо керувати. Насправді системним адміністраторам часто доводиться мати справу з сотнями вразливостей, що є нетривіальним завданням.

На жаль, оцінка CVSS виявилася поганим показником фактичного використання [43], що генерує дуже велику кількість хибно-позитивних і хибно-негативних результатів: відповідність вимогам безпеки змушує вас виконувати набагато більше роботи, ніж ви повинні робити, щоб залишатися в безпеці. , а також вводить вас в оману, пропускаючи вразливості, які ви дійсно повинні виправити [44]. Іншими словами, незважаючи на величезний обсяг роботи, яку вимагає забезпечення відповідності, неясно, наскільки це стосується фактичної безпеки. У результаті, щоб підтримувати відповідність, багато організацій змушені наймати цілі команди, єдина мета яких – обґрунтувати, чому певні вразливості не було усунено.

Це додає додаткові витрати та організаційні накладні витрати, і навряд чи сприяє підвищенню безпеки організації: заходи безпеки для забезпечення відповідності та управління безпекою все ще мають багато можливостей для вдосконалення як у сенсі виявлення загроз, так і в організаційній ефективності.

Глава

4 Електромережа

Енергетичний сектор являє собою важливий актив у більшості сучасних країн, які базують свій промисловий і суспільний розвиток на постійній доступності енергії в її різних формах. Як наслідок, більшість галузей, які працюють у цьому секторі, вважаються критично важливою інфраструктурою. Енергетичний сектор зазначений як один із двох секторів, що представляють ECI в Європі (див. Розділ 1.1). Це також один із 16 секторів критичної інфраструктури, створених президентською політичною директивою 21 (PPD-21) [8] у США.

У цьому розділі аналізується енергетичний сектор. Він починається з представлення енергетичної мережі, її основних зацікавлених сторін і гравців, а також її вимог. Він продовжується описом деяких стратегій захисту, спрямованих на запобігання будь-якому ефекту від атак, а потім завершується оглядом відкритих проблем у цій галузі.

4.1 Опис критичної інфраструктури

Енергетичний сектор включає активи, пов'язані з трьома ключовими енергетичними ресурсами: електроенергією, нафтою та природним газом. Електромережа — це взаємопов'язана мережа для доставки електроенергії від постачальників до споживачів. Він складається з трьох основних компонентів: електростанції, підстанції передачі та розподільної мережі. Електростанція виробляє одночасно три різні фази змінного струму зі зміщенням одна відносно одної на 120 градусів. Трифазна мережа живить підстанцію електропередачі. Ця підстанція використовує великі трансформатори для підвищення напруги генератора до надзвичайно високої напруги, щоб зменшити втрати в лінії електропередачі на великих відстанях. Розподільча мережа є завершальним етапом перетворення енергії перед постачанням електроенергії кінцевим споживачам. Електромережі були розроблені відповідно до вимог, які були визначені в 20-му столітті, коли метою було «тримати світло ввімкненим». Сьогодні змінилися вимоги до електромереж. Зростаюче навантаження та вимоги до споживання збільшують проблеми з електроенергією, такі як відключення електроенергії та перевантаження. У липні 2012 року протягом двох днів Індія пережила відключення електроенергії, які охопили велику частину електромережі країни. Зокрема, було оцінено розрив у 9% між ефективними потребами в енергії та доступною кількістю енергії [158] [164]. У другій половині дня 8 вересня 2011 року в південно-західній частині Тихого океану стався 11-хвилинний збій в системі, що призвело до каскадних відключень і залишило близько 2,7 мільйонів споживачів без електроенергії.

Збій в роботі електромережі стався через поганий перерозподіл потоку електроенергії через аварію лінії електропередач. Інші приклади знеструмлення електромережі через різні типи несправностей наведені в [29] [175] [112] [146]. Крім того, за оцінками, відключення електроенергії та порушення якості електроенергії коштують економіці від 75 до 180 мільярдів доларів США щорічно. Зростання попиту на електроенергію є лише однією з мотивацій, яка робить енергомережу застарілою технологією. Фактично, у 2009 році Міністерство енергетики визначило інші вимоги до сучасного дизайну електромережі, відомої як розумна мережа [144] [118]. Вимоги такі:

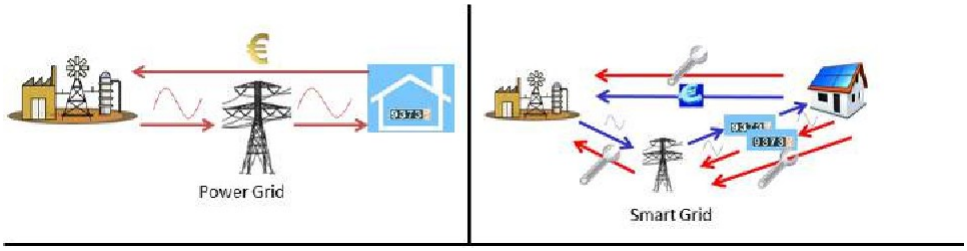
- ***Забезпечення інформованої участі клієнтів***. Традиційні електромережі забезпечують модель одностороннього зв'язку між електростанцією та кінцевими користувачами, тому клієнти беруть на себе пасивну роль в інфраструктурі електромережі. Замість цього заохочується модель двосторонньої комунікації за участю користувачів. Насправді завдяки двонаправленим потокам енергії та координації через механізми зв'язку розумна мережа допомагає збалансувати попит і пропозицію та підвищити надійність, змінюючи спосіб використання та купівлі електроенергії споживачами. Розумна мережа стає активним ринком електроенергії, який дозволяє клієнтам переключати навантаження, генерувати та накопичувати енергію на основі цін майже в реальному часі та інших економічних стимулів.

- ***Підтримка всіх варіантів генерації та зберігання***. Майбутня електромережа не може ґрунтуватися лише на централізованому виробництві електроенергії, але також має використовувати різноманітні та широко поширені розподілені джерела енергії, такі як сонячна, гідро-електростанція та вітер. Звичайно, мережева архітектура інтелектуальних мереж повинна бути розроблена гнучким способом для підтримки різних типів енергетичних ресурсів. Неоднорідність енергетичних ресурсів дозволяє зменшити пікове навантаження та забезпечити резервну енергію під час надзвичайних ситуацій.

- ***Створення нових продуктів, послуг і ринків***. Двонаправлений зв'язок між кінцевими користувачами та оперативним центром інтелектуальної мережі дозволяє створювати нові продукти та послуги, адаптовані до клієнтів. Використовуючи орієнтовані на споживача інтелектуальні пристрої або інтелектуальні електронні пристрої (IED), наприклад, клієнти або постачальники послуг можуть дистанційно контролювати споживання енергії IED. Ринки діють як координатори, керуючи серією незалежних параметрів мережі, таких як час, пропускна спроможність, швидкість змін, якість обслуговування тощо..

- ***Забезпечення якості електроенергії для різноманітних потреб***. Якість електроенергії є дуже важливим аспектом сучасної електромережі. Зокрема, мають бути реалізовані механізми для уникнення мерехтіння напруги та короткочасних перерв. Також необхідно розрізняти якість електроенергії, яка потрібна промисловості та побутовим споживачам. Отже, архітектура інтелектуальної мережі повинна бути розроблена таким чином, щоб відповідати широкому діапазону якості електроенергії.

- ***Оптимізація використання активів і ефективна робота***. Розумна мережа — це складна система, що складається з різних підсистем, які співпрацюють для забезпечення описаних вимог. Кожна підсистема керує різноманітними приладами, засобами та розподіленими енергетичними ресурсами. Таким чином, оптимізація використання цих активів зменшить весь життєвий цикл, інвестиційні витрати та енергоспоживання.



Малюнок 4.1: Еволюція від електромережі до інтелектуальної мережі

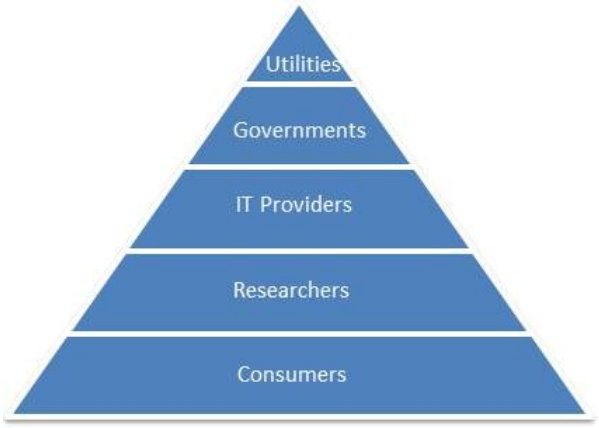
На малюнку 4.1 показана спрощена схема класичної електромережі (ліворуч) і сучасної інтелектуальної мережі (праворуч). Комунікаційний потік класичної електромережі є односпрямованим, тоді як розумна мережа використовує двонаправлену модель зв'язку, тобто інтелектуальна мережа вводить зворотний зв'язок для регулювання розподілу електроенергії, виробництва та діагностики проблем у мережі. Тим не менш, посилене підключення стає все більш критичним для кібербезпеки енергетичної системи. Насправді багато організацій зараз займаються розробкою вимог безпеки інтелектуальної мережі, включаючи Північноамериканську корпорацію з електричної надійності – захист критичної інфраструктури (NERC CIP), Міжнародне товариство автоматизації (ISA), Національний план захисту інфраструктури (NIPP) і NIST. Аналіз [102], проведений у співпраці між Університетом штату Айова та Університетом Іллінойсу в Урбана-Шампейн, зосереджений на визначенні вимог безпеки для інфраструктури розумної мережі. Зокрема, для кожного компонента інфраструктури інтелектуальної мережі визначені наступні вимоги безпеки:

- ***Розширена інфраструктура вимірювання*** (AMI). Будинки споживачів будуть розширені за рахунок інтелектуальних лічильників, які забезпечуватимуть двосторонній зв'язок між клієнтом і комунальними службами. AMI висуває власні унікальні вимоги до безпеки [28]. Конфіденційність викликає більше занепокоєння, ніж в інших мережевих доменах, через велику кількість платіжних даних кінцевих користувачів і конфіденційних даних. Цілісність необхідна як для роботи лічильника, так і для контролю, а також для передачі інформації про ціни та статус. Автентифікація та неспростування діяльності як комунального підприємства, так і споживача є критично важливими.

- ***Системи управління розподілом (DMS)***. Системи управління та автоматизації стають все більш важливими для задоволення вимог інфраструктури розподілу енергії. Системи DMS територіально розподілені; вони спілкуються за допомогою мережі та в основному виконують контрольні програми. Отже, DMS вимагає як високої цілісності, так і доступності всіх допоміжних ресурсів керування та зв'язку. Окрім вимог до цілісності та доступності, усі критичні системні функції та повідомлення мають бути автентифіковані, щоб зловмисники не могли надсилати шахрайські дані чи команди.

- ***Системи енергоменеджменту (EMS)***. На відміну від систем DMS, EMS зосереджується на системі виробництва та передачі електроенергії. EMS історично використовувала зв'язок у реальному часі для контролю та моніторингу з такими додатками, як автоматичне керування генерацією (AGC), оцінка стану та гнучкі системи передачі змінного струму (FACTS). EMS і мережі підтримують очевидні вимоги до високої цілісності та доступності. Ці атрибути є особливо важливими через критичність додатків, що керують основною системою живлення. Крім того, слід підтримувати надійну автентифікацію для всіх зв'язків, пов'язаних з електромережею, особливо для віддалених польових пристроїв, таких як IEDs та PLCs.

- ***Вимірювання, захист і контроль великої зони (WAMPAC)***. Фазорні вимірювальні пристрої (PMU) — це пристрої, які використовуються для моніторингу та захисту сучасної електромережі. Здатність виконувати вимірювання стану мережі в режимі реального часу дозволить розробити все більш ефективні схеми захисту та функції керування. Однак системи WAMPAC будуть надзвичайно залежати від високошвидкісних мереж, крім того, фазових концентраторів даних (PDC) і шлюзів, які можуть як автентифікувати, так і дозволяти обмін показаннями PMU з різними комунальними службами та незалежними системними операторами. Проблеми кібербезпеки та вимоги до WAMPAC добре задокументовані [27]. Автентифікація відіграє вирішальну роль у середовищах WAMPAC. Запропоновані архітектури, такі як NASPInet, визначили потребу в складних механізмах контролю доступу, щоб обмежити передачу вимірювань PMU лише авторизованим сторонам. Доступність і цілісність знову є критичними для високошвидкісного зв'язку. Нарешті, вимірювання PMU залежать від технології GPS для даних часових позначок. Ця залежність успадковує додаткові проблеми безпеки через потенційні глушіння або підробку атак.



Малюнок 4.2: Основні гравці в контексті Smart Grid

4.1.1 Основні зацікавлені сторони та гравці

Особливу увагу необхідно приділити визначенню основних зацікавлених сторін, залучених до розвитку інтелектуальної мережі. Зацікавлені сторони варіюються від виробників комунальних послуг та енергії до споживачів, політиків, постачальників технологій і дослідників [133] [86]. Основна перевага розвитку інтелектуальної мережі для цих зацікавлених сторін стосується зниження цін на енергію, зменшення залежності від іноземної нафти, підвищення ефективності та надійності електропостачання. На рисунку 4.2 показано категорії зацікавлених сторін.

- ***Комунальні послуги***. Вони зосереджені на впровадженні та встановленні технологій. Вони можуть забезпечити більш надійну енергію, особливо під час складних надзвичайних умов.

- ***Уряди***. Вони встановлюють нові стандарти роботи, моніторингу та сумісності, а також відповідають за створення нових правил для покращення інфраструктури інтелектуальної мережі. Нарешті, вони задовольняють потреби всіх сторін, залучених до розвитку інтелектуальної мережі.

- ***IT-провайдери***. Вони розробляють нові технології для вдосконалення електромереж. IBM і CISCO є основними гравцями у сфері постачання IT-обладнання для розумних мереж на глобальному

рівні. У 2008 році компанія IBM була обрана ініціатором IT-підтримки та послуг для програм енергоефективності розумних мереж від American Electric Power, Michigan Gas and Electric і Consumers Energy. Компанія CISCO розробила нову архітектуру IP.

CISCO описує інтелектуальну мережу як мережу передачі даних, інтегровану в електричну мережу, яка збирає та аналізує отримані дані майже в реальному часі про передачу, розподіл і споживання електроенергії.

- Споживачі. У контексті розумної мережі вони стають і споживачами, і виробниками. Фактично їх називають просьюмерами. Ця нова роль споживача створює нові можливості для бізнесу. Насправді класичний споживач може генерувати енергію (наприклад, за допомогою сонячних панелей) і подавати накопичену енергію в мережу.

4.1.2 Сценарій інтелектуального вимірювання

Цей сценарій зосереджений на прототипі моделі приватного домогосподарства з розширеною інфраструктурою вимірювання. У цьому контексті ми визначили наступний список ключових компонентів: інтелектуальний лічильник (SM), система управління енергією (EMS), розумний прилад (SA), домашня мережа (HAN) і домашній шлюз (HG). , які знаходяться всередині домашнього домену; мережа передачі даних (DCN), мережевий шлюз (NG) і сервер постачальника енергії (ESS), які знаходяться в домені постачальника енергії. Два інших, дистанційний пристрій для управління будинком (REMS) і генератор енергії (EG) знаходяться в окремих доменах.

- SM. SM — це пристрої, які реєструють енергоспоживання приладів у домашніх умовах і передають цю інформацію постачальникам енергії через DCN. Додаткову інформацію дивіться нижче.

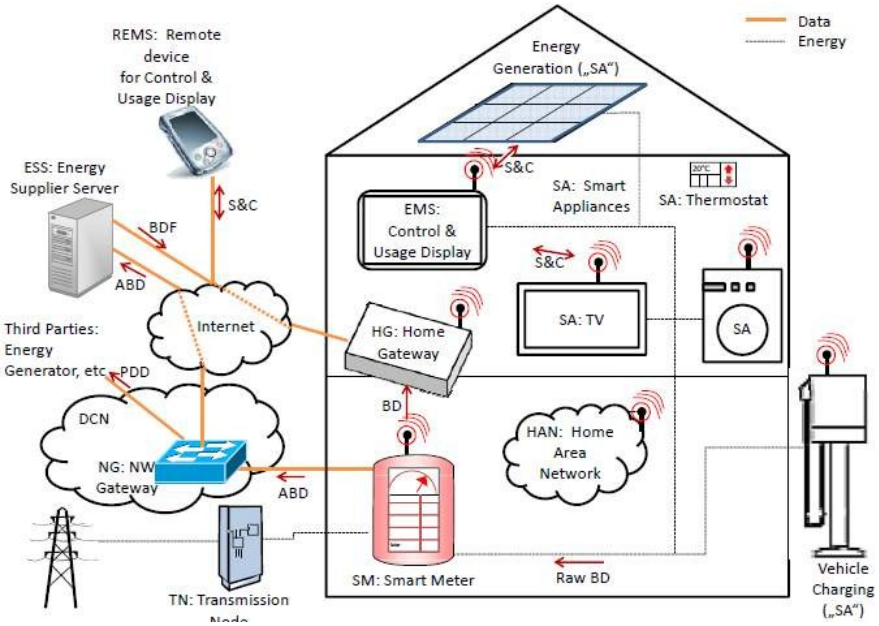
- (Дім) EMS. Передбачається, що EMS — це один виділений комп'ютер, точніше, це веб-сервер, який дозволяє користувачеві спостерігати, скільки споживають окремі прилади чи кімнати, а також їх виробництво та зберігання. Тут користувач також може визначати політику, детально описуючи, коли купувати, продавати, зберігати або споживати енергію. Він також розміщує програми керування даними та прямо чи опосередковано (через SM) контролює SA, див. [32]. Для простоти передбачається, що він спілкується з усіма іншими елементами в будинку через бездротову мережу HAN і підключений до Інтернету через HG. Користувач може увійти на персональний пристрій (ПК, планшет тощо) і отримати доступ до функцій EMS.

- REMS. Користувачі можуть віддалено отримувати доступ через деякі мобільні програми до своєї EMS, отримувати доступ до своїх даних або змінювати свої політики.

- SA. SA — це пристрої, які можна віддалено контролювати та контролювати; як такі, вони за своєю суттю включають відповідні модулі моніторингу. Для цілей цього звіту термостати, пристрої для вироблення енергії (наприклад, сонячні батареї) або зарядні станції розглядаються як SA: вони отримують керуючі повідомлення (скажімо, команди) і надсилають інформацію про стан.

- HAN. Бездротовий HAN, який використовується SM та інтелектуальними пристроями для зв'язку з EMS і EMS для зв'язку з HG.

- HG. HG – це пристрої, які можуть отримати доступ до Інтернету, а також через HAN, SA, електричні комутатори та SM.
- ESS. Це збирає агреговані платіжні дані (ABD) з розумних лічильників, а також інші дані з домашнього шлюзу для додаткових послуг. ESS (або інший сервер того самого домену) також зберігає інформацію ABD.
- Оператор пункту обліку (МПО). МРО відіграє особливу роль, передану та контрольовану постачальником енергії, з метою встановлення та обслуговування основних пристроїв розширеної інфраструктури вимірювання, а саме SM та EMS.
- DCN. Це забезпечує двосторонній зв'язок між SM на стороні споживачів та NG постачальників енергії. DCN зазвичай реалізується за допомогою публічної IP-мережі.
- NG. NG з'єднує ТГ в межах певної території з іншими компонентами розумної мережі, такими як постачальники енергії або оператори систем передачі.
- EG. Вони, як правило, працюють на звичайних або регенеративних електростанціях (викопних, атомних, сонячних електростанціях тощо). Їх важливість полягає в тому, що вони отримують зведені дані від домогосподарств, тобто скільки енергії було спожито або вироблено в районі міста (скажімо, принаймні 30 домогосподарств) протягом регулярного періоду часу (скажімо, кожні 5 хвилин).



Малюнок 4.3: Огляд справи: сутності та кроки.

4.6. Open Problems

Опис сценарію середовища

У цьому сценарії домогосподарство може виробляти, зберігати та споживати енергію, а також регулювати відповідну кількість енергії, яка береться з мережі або подається в мережу залежно від ринкових цін. Він також може передавати дані для енергетичної мережі та інших послуг, використовувати SA, які пристосовуються до поведінки домогосподарства, реагуючи на особисті уподобання, і використовувати інфраструктуру зарядки електричних транспортних засобів, яка підтримує стабілізацію інтелектуальної мережі, надаючи енергію. зберігання для сітки. На малюнку 4.3 зображено огляд середовища. Можна вважати, що весь зв'язок надсилається в зашифрованому вигляді, але для деяких з'єднань витрати на забезпечення відповідної інфраструктури безпеки (програмне забезпечення, обладнання, розповсюдження ключів тощо) можуть бути занадто великими. Можна припустити, що ключі в інтелектуальних лічильниках і HG розміщуються MPO, а ключі HAN керуються клієнтом (кінцевим користувачем), але інші варіанти можуть бути кращими. Загалом цікавим, але складним питанням є ключове питання управління, див. розділ 4.1.2.

- Необроблені платіжні дані (BD). Необроблені дані, що стосуються споживання, зберігання та виробництва енергії, збираються SM. Як саме, не має відношення до цього звіту, і передбачається, що тут немає проблем.

- BD. Потім SM обробляє та зберігає дані. Він передає дані до EMS (через HAN), так що споживання, зберігання та виробництво енергії можуть бути проаналізовані та скориговані споживачем у домогосподарстві. Дані також зберігаються (місцевою) EMS.

- ABD. З іншого боку, SM надсилає ABD до NG через публічний DCN, який пересилає його постачальнику енергії. У деяких сценаріях, як-от читання за вимогою, BD можна збирати на низьких частотах (щодня/щотижня/місяця), але оскільки метрики потужності потрібні для забезпечення стимулів для економії енергії в режимі реального часу під час піків споживання, BD надсилаються з високою частотою. частоти в залежності від розрахунку ціни. ABD слід розглядати як особисту інформацію: її можна легко пов'язати з користувачами в домогосподарстві.

- Виробництво та розподіл електроенергії (PDD). Постачальники та виробники енергії використовують дані для цілей PDD, щоб отримати прогнози споживання для певних секторів. ПТД – це агрегований BD від кількох домогосподарств. На відміну від ABD, PDD має містити особисту інформацію лише до моменту агрегування, навіть якщо частота збору є високою. Очевидно, що потрібен достатньо великий набір агрегацій різних домогосподарств і гідна довіри сторона агрегації. Вибрана деталізація для агрегації (територія міста) виглядає відповідною. Таким чином, майбутнє виробництво енергії може бути розраховане та регуляризоване.

- Відгуки про платіжні дані (BDF). Можна припустити, що кожні п'ять хвилин користувачі отримують інформацію про споживання енергії або обсяг генерації, витрати, доходи та поточні ставки. Таким чином, EMS розраховує ціну енергії, необхідної для свого робочого навантаження, на основі державних тарифів на електроенергію.

- Повідомлення про стан і контроль (S&C). Користувач локально входить до свого EMS, переглядає стан своїх пристроїв і надсилає команди до SA або змінює політику управління енергією. Наприклад, клієнт запускає активацію пральної машини. Історія дій також зберігається (локальною) EMS у журналі. Крім того, SA надсилають повідомлення про статус до EMS. Повідомлення S & C також

надсилаються та отримуються, коли користувач не ввійшов у систему через правила політики, тайм-аути тощо. Наприклад, EMS реагує на запити приладів або активує SA, лише якщо від сонячної панелі доступно достатньо енергії. або державні тарифи на енергопостачання низькі.

- Віддалений S&C (RS&C). Користувач віддалено входить у свою EMS через Інтернет, використовуючи REMS, скажімо, мобільний телефон або віддалений ПК, який може бути в інтернет-кафе. Це надає користувачеві доступ до (значної частини) функціональності нативної EMS. Історія дій зберігається ШМД (вдома, не віддалено) в журналі.

У домогосподарстві живуть різні люди, чий розпорядок життя відрізняється від розпорядку людей в інших домогосподарствах. Схеми споживання енергії тісно пов'язані зі звичками та вподобаннями людей, оскільки SA адаптують рівні енергії відповідно. Такі заняття у вільний час, як перегляд телевізора, а також зарядка акумулятора електромобіля можуть значно змінити обсяг споживання. Пристрої обліку та генерування енергії (наприклад, сонячні батареї) встановлюються MPO та калібруються щорічно. Після встановлення пристрої залишаються без нагляду в розпорядженні клієнта, якщо не буде виявлено виняткову поведінку. В цікавому варіанті сценарію два домогосподарства знаходяться в одній будівлі, а CM розміщені в загальній кімнаті як підвалі.

Пропозиції щодо найгірших випадків, нападників і загроз

Наступні запитання повинні допомогти проаналізувати середовище, а точніше, визначити основні вимоги безпеки, можливі загрози (не лише від зовнішніх зловмисників, але й від інсайдерів або звичайних учасників системи), небажані ситуації (тут згадуються як найгірші випадки, хоча вони можуть бути просто небажаними), і можливі вимоги до глибокої безпеки.

- Запитання 1: Уявіть домогосподарство, в якому проживає сім'я з дітьми в приміщеннях, описаних у розділі 4.1.2. Наскільки легко зловмиснику дізнатися, хто і скільки людей у будинку? Які дані, пов'язані з розумним вимірюванням, йому знадобляться? Як зловмисник може відстежити особи всередині, використовуючи інфраструктуру SM? Який зловмисник може це зробити? Чи міг зловмисник використати цю інформацію для планування або планування крадіжки зі зломом? Як міг бути можливий такий напад? Чи домогосподарство, зокрема діти, неправомірним використанням, скажімо, платіжних даних?

- Запитання 2: У наш час слід припустити, що в різних домогосподарствах є прилади різних типів, які забезпечують різні функції. В одному домогосподарстві SM, SA та/або домашня служба швидкої допомоги відстежують або контролюють замки вхідних дверей або вікна, духовку, мікрохвильову піч, електроприлади тощо. Крім того, одна домогосподарство може мати Smart Android TV, який є повноцінним комп'ютером з усіма його можливими типовими вразливими місцями. Пристрої підключені до Інтернету (через шлюз) і можуть отримувати оновлення програмного забезпечення та ключів, повідомлення керування системою та надсилати звіти про стан. Чи створюють SA нові загрози для інфраструктури SM? Якщо так, то які моделі зловмисників і загрози можна ідентифікувати в цьому сценарії? Які вимоги безпеки та конфіденційності потрібно встановити?

- Запитання 3: Сценарій спочатку передбачає, що весь зв'язок зашифрований. Але навіть якщо це правда, чи достатньо шифрування всього зв'язку, щоб гарантувати вимоги конфіденційності від внутрішніх і зовнішніх загроз?

Запитання 4: чи життєздатні атаки з уособленням в інфраструктурі SM? Чи може в деяких випадках

клієнт видати себе за іншого? Чи може зловмисник видати себе за сервер? Що може статися? У яких випадках це може стати критичним?

- Запитання 5: сценарій передбачає, що кожне повідомлення зашифровано. Як слід керувати шифруванням зв'язку? Хто вибирає ключі? Коли та як ключі передаються відповідним сторонам? Принаймні один вибір реалізації може бути релевантним: система повинна використовувати спільні симетричні ключі чи асиметричні? Інші варіанти можуть бути такими: має бути шифрування на нижчих рівнях (мережевий або транспортний рівень) чи на прикладному рівні? Як закріпити ключі всередині пристроїв? (І проти кого?) Беручи до уваги всі залучені сторони та їхню можливість (не)навмисного виходу з ладу, може бути важливо ще раз взяти до уваги гнучкість і економічну ефективність рішення, щоб його можна було реалізувати у великому масштабі інфраструктури SM.

- Запитання 6: Електромобільність та інфраструктура зарядки транспортних засобів стануть невід'ємною частиною майбутньої інтелектуальної мережі. Уявіть, що станції зарядки транспортних засобів і транспортні засоби обмінюються унікальними ідентифікаторами транспортних засобів (uvID). До яких порушень безпеки та конфіденційності може призвести такий підхід? Які вимоги слід встановити, щоб уникнути порушень?

4.2 Типові рішення забезпечення КІ

У контексті розумних мереж немає загальнодоступних і визнаних рішень для вирішення проблем кібербезпеки. Це пояснюється тим, що технології розумних мереж вводять багато нових компонентів в електричну мережу. Отже, контролювати глобальну інфраструктуру є дуже важким завданням. Крім того, багато з цих компонентів розроблені різними виробниками з різними стандартами якості. Через це дуже важко забезпечити взаємодію та надійність глобальних систем. Зауважте також, що двонаправлений зв'язок відбувається у звичайних мережах. Таким чином, під час використання цієї нової моделі зв'язку повинні бути забезпечені такі вимоги безпеки, як конфіденційність, цілісність і доступність (CIA) інформації. Крім того, стійкість критичної інфраструктури може бути сильно підірвана залежностями між компонентами інфраструктури, процесами та процедурами. Тому розуміння складних інфраструктурних взаємодій, їх залежностей і наслідків цих залежностей є важливим для досягнення стійких систем, як при їх проектуванні, так і при вирішенні кризи. Електромережі, будучи одними з видатних представників критичної інфраструктури, були та все ще залишаються предметом численних досліджень та ініціатив щодо вирішення проблеми взаємозалежності, особливо після великих інцидентів, які сталися за останнє десятиліття (вже описано на початок цієї глави). Насправді більшість інцидентів у цьому секторі мали серйозні наслідки через наявність залежностей, які посилили явище каскадних збоїв. Наприклад, більшість великих відключень електромережі, які мали місце в минулому, були ініційовані однією подією (або декількома пов'язаними подіями, такими як збій обладнання електромережі, який не обробляється належним чином SCADA), що поступово призводить до каскадних збоїв і кінцевий крах усієї системи. У Звіті та Рекомендаціях NIAC 2009 концепція стійкості інфраструктури вводиться як здатність зменшити масштаб, вплив або тривалість збою. Серед рекомендацій щодо підвищення стійкості наголошується на необхідності розуміння взаємозалежностей у реальному часі та очікувань і обмежень взаємопов'язаних секторів, щоб мінімізувати непередбачені обставини. Підходи до аналізу взаємозалежностей критичної інфраструктури передусім включають ряд методів моделювання, моделювання та аналізу. Огляд досліджень у сфері моделювання та аналізу взаємозалежності інфраструктури можна знайти в [153], тоді як деякі конкретні дослідження, що стосуються сектору

енергомереж, наведено в [77, 47, 82, 156, 159, 65, 53]. NIST [25] містить ключові концепції та припущення, які є основою для логічної архітектури безпеки.

- Стратегія поглибленого захисту: безпека повинна застосовуватися на рівнях, із запровадженням одного або кількох заходів безпеки на кожному рівні. Мета полягає в тому, щоб зменшити ризик того, що один компонент захисту буде скомпрометований або обійдеться. Це часто називають глибоким захистом. Підхід до поглибленого захисту зосереджується на захисті інформації, активів, систем живлення, комунікацій та IT-інфраструктури за допомогою багаторівневого захисту (наприклад, брандмауери, системи виявлення вторгнень, антивірусне програмне забезпечення та криптографія). Через велику різноманітність методів зв'язку та характеристик продуктивності, а також через те, що жоден захід безпеки не може протистояти всім типам загроз, очікується, що буде реалізовано кілька рівнів заходів безпеки.

- Доступність енергосистеми: Стійкість енергосистеми до подій, які потенційно призводять до збоїв, була основним напрямком проектування та експлуатації енергосистем протягом десятиліть. Існуюча конструкція та можливості системи живлення успішно забезпечують доступність для захисту від ненавмисних дій і стихійних лих. Ці існуючі можливості системи живлення можуть бути використані для задоволення вимог кібербезпеки.

Рішення, широко прийняте науковим співтовариством, полягає у використанні інформації, наданої системами глобального моніторингу (WAMS), для моніторингу мережі передачі та запобігання поширенню збурень. WAMS використовують пристрої, розподілені по всій енергосистемі, які вимірюють ключові параметри для виявлення аномальних умов. Сьогодні PMU є найбільш часто використовуваними пристроями в WAMS. Зокрема, PMU – це пристрої, які виконують вимірювання векторів напруги та струму в реальному часі для надання інформації про стан електромережі. Синхронізація часу між різними PMU необхідна для розуміння глобального статусу електромережі одночасно. Це пояснюється тим, що події, що відбуваються в одній частині мережі, впливають на роботу в інших місцях, а також поширюються на інші системи за межами мережі, які покладаються на стабільне живлення. Синхронізовані в часі вимірювання, вироблені PMU, називаються синхрофазорами. Щоб отримати одночасні вимірювання векторів, виявлених різними PMU, встановленими на великій території енергосистеми, необхідно синхронізувати ці часи, щоб усі вимірювання векторів, що належать до одного часу, були дійсно одночасними. Кожен PMU використовує приймач GPS [85] для отримання унікальної мітки часу в глобальній системі. Надаючи інформацію в режимі реального часу про стабільність і робочі запаси безпеки, WAMS дає ранні попередження про збої в системі для запобігання та пом'якшення великих відключень електроенергії. Постійна присутність існуючих вимірювальних пристроїв і часткова видимість окремих PMU призводять до того, що деякі комунальні підприємства стверджують, що WAMS не є кібернетично критичними системами, як визначено NERC CIP [143], і тому PMU та PDC не потрібно розглядати як кібернетичні активи (CCA). Дані WAMS також використовуватимуться для нових систем візуалізації та зберігатимуться безпечним способом для аналізу після інцидентів [121]. WAMS також може включати додатки класифікації подій енергосистеми, такі як семантичні керовані алгоритми виявлення знань.

Схеми захисту цілісності системи (SIPS) [136] встановлюються для захисту цілісності енергосистеми або стратегічних частин, на відміну від звичайних систем захисту, які призначені для захисту конкретного елемента енергосистеми. SIPS потребують кількох пристроїв (приводів і детекторів), встановлених на великій території, які обмінюються даними через мережеву інфраструктуру. Ця схема керування корисна для виявлення змін у навантаженні, генерації чи конфігурації системи, а також для спроб вжити заходів

керування для підтримки стабільності системи.

Системи виявлення вторгнень (IDS) [102] в електричній мережі привернули значну увагу в останні роки. Використовуються два типи IDS, які виявляють аномалії або неправильне використання. Ефективність IDS продемонстрована в [75], де автори ідентифікували зловмисні події в системах керування, зосереджуючись на відомих статичних шаблонах мережевого зв'язку. Крім того, [57] продемонстрував, як методи виявлення вторгнень на основі специфікацій можна використовувати в розгортаннях AMI для виявлення зловмисних шаблонів зв'язку.

Системи безпеки та управління подіями (SIEM) уже широко застосовуються для захисту критичної інфраструктури, тому їх також можна використовувати для захисту інтелектуальної мережі. Потужність системи SIEM полягає в тому, що вона аналізує та співвідносить різні події, надані багатьма джерелами інформації, щоб виявляти кібератаки. Архітектура SIEM складається з трьох основних компонентів: датчиків, сервера та системи зберігання. Датчики розгортаються в інфраструктурі з метою моніторингу. Основна мета датчиків — збирати події та надсилати їх на сервер. Інтелектуальні датчики, запропоновані в літературі, наприклад, [157], дозволяють: збирати синтаксично різнорідні формати подій для обробки даних, згенерованих кількома рівнями інфраструктури; кореляція багаторівневих даних на основі різної семантики, наприклад, не лише IP-адрес, номерів портів, типів протоколів, підписів корисного навантаження; обробка даних на межі архітектури SIEM для фільтрації мікроподій, створених інфраструктурою. Сервер виконує складну кореляцію подій, що надаються різними датчиками, щоб виявити нові атаки. Система зберігання зберігає тривоги та згенеровані події. Система зберігання є дуже важливим компонентом системи SIEM. Насправді аналіз, який виконується в режимі онлайн і офлайн сервером або будь-яким інструментом аналізу, є правильним, якщо забезпечується цілісність і непідробність даних. Отже, архітектура зберігання повинна бути розроблена таким чином, щоб забезпечити цілісність і непідробність даних, навіть якщо деякі компоненти архітектури зберігання скомпрометовані [38, 39].

4.3 Типи атак і використовувані вразливості

У [103] описано системи WAMS та їх основні вразливості. Система GPS є однією з найважливіших вразливостей систем WAMS, яка впливає на пристрої PMU. Насправді кожен PMU використовує GPS-приймач

[85] для отримання унікальної позначки часу в глобальній системі. Однак GPS піддаються впливу трьох основних джерел перешкод: блокування, перешкоди та підробка. Перешкоди та блокування – це процеси генерації шумових сигналів, які об'єднуються з сигналами GPS, створюючи нові сигнали, які приймач не може зрозуміти [88, 154]. Ці типи атак є розпізнаними, тому що мета полягає в тому, щоб відмовити в конкретній пропонованій послузі, у даному випадку – у визначенні часу. Підробка GPS

[98] — це процес передачі GPS-приймачу неправдивої інформації, щоб він обчислив помилковий час або місцезнаходження. Цей тип атаки складно виявити, оскільки сигнал GPS підробляється, щоб ввести в оману приймач GPS, який його використовує. Підробка GPS була виявлена та виділена в 2001 році Міністерством транспорту США під час дослідження вразливості транспортної інфраструктури, яка використовує сигнал GPS [15].

Першим кроком, необхідним для здійснення атаки GPS-спуфінгу, є отримання та відстеження сигналів GPS для отримання опорного сигналу. Потім генерується підроблений сигнал, який сумується з вихідним сигналом GPS. Новий сигнал використовується для синхронізації підробленого сигналу з отриманим автентичним сигналом. Таким чином, зловмисник створює сигнал, ідеально узгоджений з автентичними сигналами, але з меншою потужністю. Згенерований підроблений сигнал за потужністю можна порівняти з шумом цільового приймача. Потім зловмисник збільшує потужність підробленого сигналу, поки він не

подолає автентичний сигнал. Таким чином, підроблений сигнал показує вище співвідношення сигнал/шум (SNR). Таким чином, приймач GPS відстежує фальшивий сигнал GPS (замість справжнього сигналу) через його вищий SNR. Після цього зловмисник успішно заволодів GPS-приймачем. Потім він повільно переміщує підроблений сигнал від автентичного сигналу. Отриманий сигнал GPS вважається повністю захопленим, якщо підроблений сигнал затримується на 2 мікросекунди від автентичного сигналу, як описано в [163]. Таким чином зловмисник може збільшити час затримки до десинхронізації PMU. Якщо зловмисник підробить мітки часу, надані GPS для PMU, це може спричинити варіації виміряних фазових кутів. Різниця у фазовому куті між двома PMU вказує на те, що потужність між областями, виміряна кожним PMU, змінилася. Ці варіації можуть поставити під загрозу стабільність системи таким чином, що оператори мережі або системи автоматичного реагування прийматимуть неправильні рішення, як-от увімкнути чи вимкнути генератори. Неправильні рішення можуть призвести до знеструмлення або пошкодження. У [102] описані можливі атаки, які можуть бути здійснені з метою скомпрометувати інфраструктуру інтелектуальної мережі. Ці атаки включають:

- Protocol attacks: The network protocols used in the power system, suchas ICCP, IEC 61850, and DNP3, could be potentially exploited to launch cyberattacks if they are not secured properly. Since these protocols areused to control remote devices and substations, once an attacker is ableto gain network access they could manipulate the communications to inject malicious system state and controls. Therefore, the grid requiressecure versions of these protocols that not only provide security guaran- tees, but also meet the required latency and reliability guarantees needed by the grid applications.

- Атаки маршрутизації: Це відноситься до кібератак на інфраструктуру маршрутизації Інтернету та інших глобальних мереж. Маніпулюючи маршрутизацією пакетів, зловмисники можуть виконувати атаки типу "людина посередині" (MITM), підмінювати або затримувати доставку автентичного трафіку. Масована атака маршрутизації може мати наслідки для роботи мережі в реальному часі та для ринків у реальному часі, які покладаються на глобальний зв'язок.

- Вторгнення: Це відноситься до використання вразливостей у програмному забезпеченні та комунікаційній інфраструктурі мережі, яка потім забезпечує доступ до критичних системних елементів. Вторгнення в мережу викликають особливе занепокоєння через нещодавні звіти, в яких виявлено численні недоліки програмного забезпечення та мереж, що використовуються в комунальній галузі. Прикладом сценарію вторгнення є отримання доступу до станції керування в обхід засобів захисту (міжмережеві екрани, системні паролі).

- Зловмисне програмне забезпечення: це стосується зловмисного програмного забезпечення, яке використовує вразливості системного програмного забезпечення, програмованих логічних контролерів або протоколів. Зловмисне програмне забезпечення зазвичай сканує мережу на наявність потенційних машин-жертв, використовує певні вразливості в цих машинах, копіює корисне навантаження зловмисного програмного забезпечення на жертви, а потім саморозповсюджується. Останніми роками зростає кількість та складність атак зловмисного програмного забезпечення (наприклад, Stuxnet), і це викликає серйозне занепокоєння для систем критичної інфраструктури, включаючи електромережі..

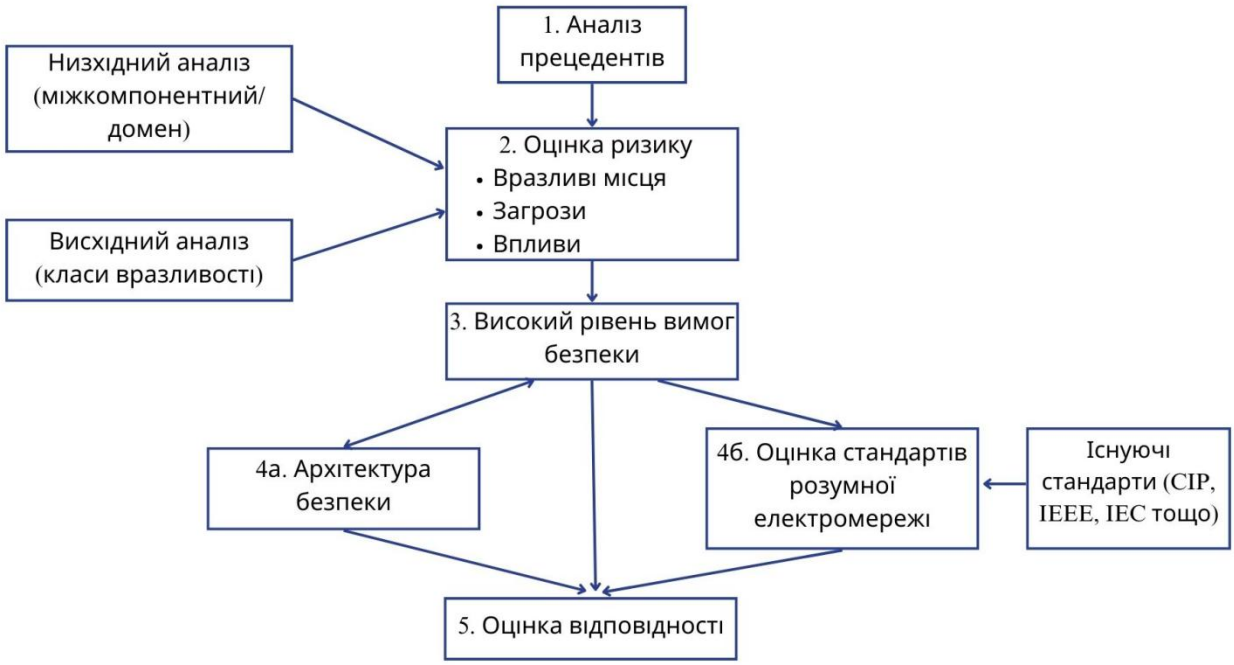
- Атаки на відмову в обслуговуванні (DOS): DOS – це будь-яка атака, яка відмовляє в наданні звичайних послуг законним користувачам. Це також може означати відмову від контролю або спостереження в контексті електромережі. Ці атаки, як правило, створюються через атаки масового виснаження

ресурсів, які переповнюють комунікаційну мережу або сервер величезними обсягами трафіку або помилкових робочих навантажень, таким чином відмовляючи в обслуговуванні законним користувачам.

- Внутрішні загрози: електрична мережа також стикається з ризиком внутрішніх загроз, таких як ті, що визначені у звіті NERC HILF. Зловмисний інсайдер, який має доступ до мережі системи керування, може легко зловживати своїм довіреним статусом, щоб установити зловмисне програмне забезпечення або безпосередньо ввести зловмисні команди в мережу. Зловмисні інсайдери особливо небезпечні, оскільки вони також володіють детальними знаннями про топологію та роботу системи, а тому можуть легко розробити сценарій атаки, який змусить систему працювати поза безпечними робочими точками.

Інші можливі атаки стосуються AMI, справді, у цьому контексті з'являється кілька нових викликів безпеці [127, 130, 56]. Основними елементами AMI є інтелектуальні лічильники, які сильно відрізняються від традиційних лічильників тим, що вони дозволяють дистанційно контролювати споживання електроенергії та попит. Однак, оскільки інтелектуальні лічильники повинні бути встановлені в будівлі кожного клієнта, AMI складатиметься з мільярдів таких пристроїв, які через величезний розмір території, яку потрібно охопити, повинні бути дешевими (часто за рахунок якості). Крім того, вони будуть розміщені у фізично незахищених місцях і під контролем часто незацікавлених, недосвідчених або іноді зловмисних користувачів. З цієї причини, навіть незважаючи на те, що кожен лічильник піддається ретельній перевірці перед встановленням, після розміщення в приміщеннях замовника він більше не може вважатися надійним. В основному ризик, пов'язаний із використанням інтелектуальних лічильників, пов'язаний як з тим фактом, що вони не були побудовані відповідно до певної політики безпеки, так і з тим, що доступ до них здійснюється віддалено за допомогою різних комунікаційних технологій. Часто мережева інфраструктура, що лежить в основі AMI, має сітчасту топологію, що покладається на різні бездротові мережі та протоколи, такі як WiFi, стільниковий зв'язок, WiMAX, супутниковий зв'язок тощо. Це створює додаткові проблеми безпеки, оскільки атакуваний лічильник може поширювати шкідливий код на інші лічильники по сусідству. Дослідники вже показали, що інтелектуальні лічильники вразливі до атак, які можуть призвести до відключення електроенергії, шахрайства з використанням енергії тощо. Зокрема [130] описує різні типології атак, які можуть бути виконані для обману електричної мережі шляхом маніпулювання системою AMI. tems. Автори звіту демонструють, що крадіжка енергії все ще можлива в системах AMI і що сучасні пристрої AMI надають нові можливості для досягнення цієї мети. Розумні лічильники оснащені новими антитамперними рішеннями, але хоча цих рішень достатньо для звичайних чесних людей, вони не заважають зловмисникам їх обійти. Підхід, описаний у [130], базується на маніпулюванні даними попиту. В основному існує три способи маніпулювання такими даними, кожен з яких адаптований до певного стану даних під час вимірювання: (i) дані зберігаються в пристрої, (ii) дані архівуються в пристрої, (iii) дані передаються мережею, щоб досягти комунальних служб, які керують споживанням енергії. На основі конкретного стану, на який покладаються атаки, останні можна класифікувати за трьома відповідними категоріями. Перша та друга категорії атак вимагають доступу до пристрою таким чином, щоб перезаписати мікропрограму лічильника (перша категорія) або змінити збережені дані (друга категорія). Це завдання є дуже важким і вимагає інтенсивного зворотного проектування. Атаки, що належать до третьої категорії, працюють шляхом введення змінених значень у зв'язок між лічильниками та комунальними службами. Крім того, оскільки інформація, що надсилається декількома лічильниками, часто збирається в колекторні вузли, розташовані між лічильниками та комунальними службами, атаки на цьому боці мережі дозволяють модифікувати велику кількість даних попиту, таким чином збільшуючи шкоду. У [56] різні реальні розумні лічильники розглядаються та аналізуються з точки зору безпеки. Кожен лічильник розглядається як датчик, тому загальний AMI можна розглядати як мережу датчиків. Зв'язок відбувається через бездротову персональну мережу низької швидкості зі схемою маршрутизації з кількома стрибками. Цей вибір дешевий, але збільшує площу поверхні для атаки. У цій ситуації можна здійснити декілька атак, наприклад, атаки на чорну

діру, сіру діру та сибілу. Вищезазначені автори зосереджуються на атаках на чорні діри та показують деякі запобіжні заходи, які постачальники лічильників повинні прийняти, щоб уникнути такого роду атак.



Малюнок 4.4: Завдання в Стратегії кібербезпеки Smart Grid.

4.4 Стратегії захисту

Дослідження NIST [25] визначило деякі завдання, які необхідно виконати, щоб зробити розумну мережу безпечною. Реалізація стратегії кібербезпеки вимагає визначення та реалізації загального процесу оцінки ризиків кібербезпеки. Ризик — це потенційна можливість небажаного результату в результаті інциденту, події чи події, що визначається його ймовірністю та пов'язаним з ним впливом. Процес оцінки ризику інтелектуальної мережі базується на існуючих підходах до оцінки ризику, розроблених як приватним, так і державним секторами, і включає ідентифікацію активів, вразливостей і загроз, а також визначення впливу для проведення оцінки ризику розумної мережі та її доменів і суб - домени, такі як будинки та підприємства. Оскільки інтелектуальна мережа включає системи з IT, телекомунікацій та електроенергії, процес оцінки ризиків застосовується до всіх трьох секторів, оскільки вони взаємодіють у розумній мережі. Завдання, які були визначені та повинні бути виконані під час реалізації стратегії кібербезпеки, показані на рисунку 4.4 і детально описані нижче.

- Аналіз варіантів використання: набір варіантів використання забезпечує спільну структуру для виконання оцінки ризиків, розробки логічної еталонної моделі, а також вибору та адаптації вимог до безпеки.
- Оцінка ризику: Оцінка ризику включає виявлення вразливостей, активів і загроз. Можливі два підходи: аналіз зверху вниз і аналіз знизу вгору. Підхід «знизу вгору» зосереджується на добре зрозумілих проблемах, які необхідно вирішити, наприклад, системі виявлення вторгнень для енергетичного обладнання,

авторизації та автентифікації користувачів для доступу до управління підстанцією. Низхідний підхід фокусується на логічній моделі, яка має бути забезпечена на архітектурному рівні. Результати фази оцінки ризику корисні для вибору вимог безпеки, які необхідно забезпечити.

- Вимоги високого рівня безпеки: для оцінки конкретних вимог безпеки та вибору відповідних технологій і методологій безпеки потрібні як експерти з кібербезпеки, так і експерти з енергосистем. Експерти з кібербезпеки мають широкі знання про IT та технології безпеки систем керування, тоді як експерти з енергетичних систем мають глибоке розуміння традиційних методологій енергетичних систем для підтримки надійності енергетичних систем.
- Архітектура безпеки: безпечна архітектура інтелектуальної мережі розроблена та розроблена відповідно до вимог, описаних у попередніх кроках.
- Оцінка стандартів інтелектуальної електромережі: на цьому етапі оцінюються стандарти, які були визначені як потенційно відповідні групами Плану пріоритетних дій (PAP). Цей процес підкреслює прогалини між вимогами безпеки та визначеним стандартом. Також будуть надані рекомендації щодо усунення цих прогалин.
- Оцінка відповідності: Останнім завданням є визначення програми оцінки відповідності для безпеки.

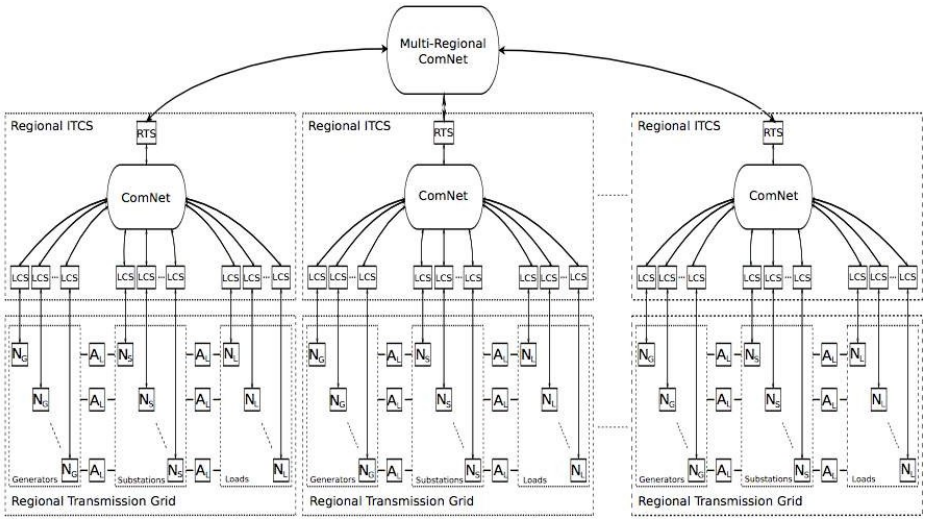


Figure 4.5: High-level model of a electric power grid.

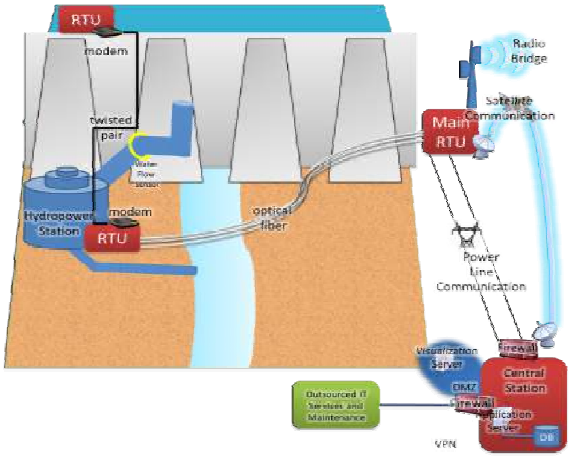
4.5 Підходи до пом'якшення несправностей

Інтелектуальні електромережі зазвичай оснащені системою глобального моніторингу (WAMS), яка часто використовується для уникнення катастрофічних збоїв, таких як відключення електроенергії через перевантаження.

WAMS використовує різні PMU, встановлені в різних місцях, щоб виконувати розподілені вимірювання в енергосистемі. PMU — це пристрої, які виконують вимірювання векторів напруг і струмів у реальному часі, щоб надати інформацію про глобальний стан електромережі. Синхронізовані в часі вимірювання, вироблені PMU, називаються синхрофазорами. Кожен PMU використовує приймач GPS для отримання

унікальної мітки часу в глобальній системі. Таким чином, можна використовувати різні вектори, надані різними острівцями електромережі, щоб перевірити правильну поведінку глобальної електромережі та уникнути перевантажень, які викликають збої. Зокрема, запропонована стратегія [166, 167] дозволяє уникнути збоїв шляхом аналізу варіації векторів, виявлених різними PMU в одному часовому інтервалі. Насправді, якщо вектори розходяться, одна або кілька ліній електропередачі електромережі перевантажуються, і ризик, пов'язаний з можливим відключенням електроенергії, зростає. Коли системи моніторингу виявляють, що різниця між векторами перевищує порогове значення, вони повідомляють станцію керування про аномалію. Тоді станція керування може автоматично переналаштувати електромережу, щоб уникнути збоїв.

Інші зусилля, спрямовані на підвищення надійності інтелектуальних мереж, були зосереджені на застосуванні прогнозування несправностей, особливо для оцінки вразливості електричних мереж ескалаційними та каскадними збоями через притаманні взаємозалежності між електричною та інформаційною інфраструктурою. Прогнозування несправностей дозволяє аналізувати критичні сценарії, в яких внутрішні або зовнішні несправності в сегменті інформаційної інфраструктури провокують серйозний вплив на контрольовану електроенергетичну інфраструктуру [53, 77]. З цією метою взаємозалежності між об'єктами інфраструктури можна представити за допомогою моделі, яка дозволяє описувати інфраструктуру в термінах об'єктів і взаємозалежностей з точки зору високого рівня (див. рис. 4.5). З цієї моделі високого рівня можна отримати стохастичну модель для кількісного аналізу впливу різних типів збоїв, які можуть виникнути за наявності випадкових і зловмисних збоїв у цих об'єктах. Наприклад, ймовірність (з точки зору ймовірності) потенційного явища поширення відмови між об'єктами можна оцінити за допомогою такого підходу до моделювання.



Малюнок 4.6: Моніторинг ГЕС.

Випадок диспетчерської станції DAM. Інфраструктура, така як греблі або електрогенератори, контролюється станцією керування (Рисунок 4.6). Як правило, для моніторингу цього типу інфраструктури використовується система SCADA.

Для проведення вимірювань у різних місцях встановлено кілька датчиків. Датчики підключаються до віддалених терміналів (RTU), які зчитують вимірювання аналогових і цифрових сигналів і надсилають їх до основного RTU. RTU обмінюються даними через RS-232, Ethernet, оптоволокно, GPS або GPRS.

Головний RTU надсилає інформацію, зібрану RTU, на станцію керування, щоб оцінити безпеку/безпеку DAM. Головний RTU використовує лінію живлення для передачі інформації на станцію керування. У цьому сценарії лінія електропередач є дуже важливим активом IT-інфраструктури. Насправді втрата лінії живлення з будь-якої причини може призвести до переривання передачі даних.

Техніка уникнення збоїв зв'язку базується на концепції резервування. Зокрема, система передачі даних розроблена для використання більш ніж одного каналу зв'язку. У цьому контексті основним каналом зв'язку є лінія електропередач. Якщо опір каналу нескінченний, зв'язок не може бути здійснений. Основний RTU виявляє цю проблему та встановлює вторинний канал на основі супутникового зв'язку для надсилання тієї самої інформації. У цьому випадку резервна система зв'язку вважається механізмом холодної реплікації.

4.6 Відкриті проблеми

Мережеві підходи, які використовуються в сучасних інтелектуальних мережах, обмежуються аналізом мережевого трафіку з метою виявлення, пом'якшення та усунення атак DoS. Однак дійсні засоби протидії атакам на цілісність і конфіденційність часто надаються лише як доповнення до існуючих систем, і це може призвести до слабких місць у результаті інтеграції різнорідних компонентів (як правило, наданих кількома постачальниками). Необхідно проаналізувати вплив класичних алгоритмів криптографії на продуктивність мережі, щоб оцінити компроміс між безпекою та часовими обмеженнями, щоб прийняти найбільш відповідні схеми автентифікації в інтелектуальній мережі.

Як уже обговорювалося, атака підробки GPS представляє реальну загрозу безпеці інтелектуальної мережі. Сьогодні було запропоновано кілька методів для виявлення такої атаки [183]. Такі прийоми в основному базуються на:

- моніторинг абсолютної сили сигналу GPS. Ця методика заснована на порівнянні між спостережуваною і очікуваною силою сигналу. Якщо їх різниця перевищує фіксоване порогове значення, генерується сповіщення.

- моніторинг потужності сигналу, отриманого від кожного супутника. Ідея полягає в тому, щоб порівняти спостережувану силу сигналу з очікуваною силою сигналу для кожного супутника. Зловмисник генеруватиме підроблений сигнал однакової сили для кожного штучного супутника через симулятор супутника GPS. Натомість сигнали, що надаються реальними супутниками, змінюватимуться з часом для кожного супутника. Таким чином, сповіщення генерується, якщо характеристики сигналу є постійними з часом для кожного супутника.

- моніторинг відносної потужності сигналу GPS. Цей метод передбачає, що середня потужність сигналу періодично записується та порівнюється. Якщо виявлено значну зміну відносної сили сигналу, генерується сповіщення.

Однак методи відновлення недоступні, щоб уникнути збоїв PMU.

Оскільки інтелектуальні системи обліку є новими, для них не існує повної бази даних атак. Тому дуже важливо розробити та впровадити систему виявлення та діагностики, здатну точно виявляти невідомі атаки. Зокрема, для захисту інтелектуального вимірювання можна розглянути підходи, засновані як на методах підпису, так і на методах аномалій. Крім того, комунікаційна мережа AMI не є однорідною, і для обміну повідомленнями між компонентами AMI використовуються різні технології та протоколи. Щоб усунути таку неоднорідність, було б корисно реалізувати систему, здатну збирати важливу для безпеки інформацію з будь-якого важливого компонента інфраструктури та аналізувати багатопротокольну інформацію з метою виявлення нових атак.

4. The Power Grid

Як описано вище, AMI зазвичай складається з мільярдів розумних лічильників, розміщених у фізично незахищених місцях, потенційно вразливих до кібератак. Значний розмір мережі цього типу, а також необхідність для лічильників і компонентів керування постійно обмінюватися повідомленнями для збору даних, контролю та нагляду за пристроями призводить до того, що цей сценарій вважається дуже схожим на сценарій традиційної системи SCADA. Використовуючи розподілені електронні засоби керування та датчики для виконання пакетних або повторюваних завдань, SCADA попереджає оператора, якщо якийсь компонент системи потребує уваги або перевищив попередньо встановлені параметри. У той час як перші системи SCADA виконували всі операції на одному комп'ютері (зазвичай, мейнфреймі), а функції SCADA були обмежені лише датчиками моніторингу, пізніші системи SCADA використовують розподілену архітектуру, оскільки вони часто ділять функції керування кількома невеликими комп'ютерами. Крім того, якщо в перших розподілених системах SCADA вузли були з'єднані локальними мережами, то нинішні системи SCADA зазвичай об'єднані в мережу, спілкуючись через глобальні мережі, і часто клієнти можуть отримати доступ до системи за допомогою Інтернету та Інтернету, також через бездротове з'єднання. В даний час системи SCADA побудовані на основі бездротової сенсорної мережі. У такому контексті питання безпеки є ключовими питаннями при розробці програм SCADA, оскільки вони вразливі до кібератак. Зауважте, що ці два рівні компонентів у системах SCADA, а саме (i) основна сенсорна мережа та (ii) високий рівень нагляду та контролю, не є еквівалентними з точки зору проблем безпеки та можливих контрзаходів. Наприклад, система SCADA може збирати ряд вимірювань з різних датчиків і може їх деталізувати, так що просте виявлення викидів у часових послідовностях датчиків не можна відразу поширити на інші високі рівні SCADA, оскільки неправильна поведінка датчика Вузол SCADA вищого рівня може бути набагато складнішим порівняно з вузлом датчика. Таким чином, вищезазначені підходи, що працюють на рівні сенсорної мережі, не відразу застосовуються до всієї системи SCADA. Ці проблеми також виникають у випадку інтелектуальної системи вимірювання, в якій компоненти нагляду та контролю можуть бути реалізовані як система SCADA. На основі вищезазначених міркувань можна проаналізувати можливість застосування техніки для виявлення скомпрометованих вузлів у системі інтелектуального вимірювання, використовуючи стратегію, засновану на довірі, отриману в результаті дослідження соціальних агентів. Ця можливість вже була досліджена в системах SCADA. Наприклад, були запропоновані деякі архітектури для стимулювання правильної поведінки маршрутизації [61]. У цьому підході кожен вузол отримує оплату за стрибок у кожному пакеті, який він пересилає. Вузли зберігають цю платіжну інформацію у внутрішньому лічильнику, і ця інформація передається вузлами, які безпосередньо взаємодіють, вводячи елемент співпраці в механізм безпеки. Цей тип підходу [123] пропонує пом'якшення неправильної поведінки маршрутизації шляхом виявлення вузлів, які не пересилають, і оцінювання кожного шляху, щоб уникати цих вузлів під час перерахунку маршрутів. Таким чином, немаршрутизуючі вузли не включаються в шляхи маршрутизації, оскільки вони не збираються співпрацювати, але вони все одно можуть просити інших пересилати їхні повідомлення. Ця схема виявляє неправильну поведінку, але не ізолює її. Інші версії цього підходу [61] запроваджують безпечний протокол маршрутизації, який сидить над обраним протоколом маршрутизації, що робить неправильну поведінку менш привабливою для вузлів, ніж правильна маршрутизація. Зокрема, вузли спостерігають за поганою поведінкою своїх сусідів і враховують цю поведінку за допомогою локальної системи репутації. Крім того, вузли також можуть інформувати своїх довірених сусідів про некоректну роботу вузлів. Також можна використовувати глобальну (замість локальної) систему репутації [138]: деяка інформація про репутацію про сенсорні вузли передається по всій мережі, щоб попередити всі вузли про неправильну роботу вузлів. У цьому підході скомпрометовані вузли виявляються та ізолюються, оскільки їхня репутація оцінюється як низька. У будь-якому випадку, всі перераховані вище підходи працюють на рівні сенсорних мереж, без залучення вузлів високого рівня. Розробка стратегії виявлення, яка враховує всі вузли системи AMI (а не тільки лічильники), може надати дві основні

переваги: (i) можна негайно виявити атаки, які безпосередньо адресовані вузлам AMI високого рівня; (ii) можна використовувати різні компоненти програмного забезпечення для вузлів високого рівня (які, як правило, є повністю обладнаним ПК) і для вузлів нижчого рівня (які мають обмежені ресурси).

Безпека зв'язку передбачає розробку схеми керування ключами. Проте визначення відповідної схеми управління ключами для інтелектуальних мереж все ще залишається відкритим питанням. Одним із основних каменів спотикання є те, що пристрої в системі розумної електромережі зазвичай мають обмежений обсяг пам'яті, низьку потужність і пропускну здатність, що вимагає, щоб схема керування ключами була ефективною та гнучкою. З цієї точки зору рішення на основі PKI ще далекі від того, щоб бути зрілими та ефективними з кількох причин. Перш за все, потреба в тривалому терміні дії сертифіката суперечить потребі в CRL керованого розміру [188]. Крім того, у пристроях з дефіцитом ресурсів рішення PKI може створити конфлікт між вимогами сумісності та масштабованості. Дійсно, щоб забезпечити значну взаємодію, пристрій повинен, принаймні в принципі, зберігати сертифікати всіх можливих суб'єктів сертифікації (наприклад, виробників, дистриб'юторів або навіть користувачів). Кількість цих сертифікатів може виявитися занадто великою для обмежених ресурсів пам'яті пристрою. Релевантним прикладом цього конфлікту є внутрішній профіль ZigBee Smart Energy Profile. Щоб подолати цю проблему, Діні та ін. запропонувати нову форму локальної перехресної сертифікації [84].

У сфері PKI шифрування на основі ідентифікатора (IBE) може бути особливо привабливим для інтелектуальних мереж, оскільки його можна розгортати без попередньої конфігурації, оскільки ідентифікатор (ID) пристрою використовується для генерації унікальних ключів. Це дозволяє легко розгортати малопотужні пристрої, такі як датчики, оскільки вони можуть почати надсилати захищені повідомлення без необхідності зв'язуватися з ключовим сервером. В якості альтернативи можна використовувати симетричне шифрування. Для методу симетричного ключа ризиковано, якщо всі пристрої використовують один і той самий попередньо завантажений ключ, оскільки якщо один із цих пристроїв зламано, зловмисник може знати спільний ключ кожного пристрою. Замість попередньо вибраного ключа краще налаштувати довірену третю сторону для розподілу спільного ключа між двома сторонами. Систему Kerberos можна використовувати в цьому середовищі для розповсюдження ключа для компонентів інтелектуальної мережі. Однак інтелектуальні мережі мають унікальні особливості щодо розподілених обчислювальних середовищ, для яких Kerberos спочатку був задуманий. Центр розповсюдження ключів (KDC) у системі Kerberos не може підтримувати розповсюдження ключів у разі перебоїв у мережі або електроенергії. Що ще важливіше, надто дорого та небезпечно мати резервний сервер для KDC, враховуючи розмір інтелектуальної мережі. Загалом може бути можливим поєднання ієрархічних, децентралізованих, делегованих або гібридних схем безпеки. Останніми актуальними прикладами такого роду схем управління ключами є [188, 113, 187]. Бажано, щоб схема-кандидат мала включати безпечні протоколи завантаження, тобто вона повинна забезпечувати ефективні засоби для ініціалізації нових пристроїв. Крім того, у критично важливих операціях безпеки, таких як оновлення ключів, бажано використовувати методи керування ключами групи. Знову ж таки, ZigBee Smart Energy Profile не відповідає належним чином цим вимогам і, зокрема, не відповідає вимогам безпеки вперед [188]. Насправді, після виходу з системи (вузол може бути звільнений, відправлений на технічне обслуговування, втрачений, скомпрометований або передбачуваний таким), вузол все ще може отримати доступ до зв'язку, оскільки вбудований ключовий матеріал не відкликано належним чином. Якщо відкликання не відкликано належним чином, зловмисник може використати ключі на пристрої для здійснення серйозних атак на цілісність системи та конфіденційність користувачів.

Інтелектуальні мережі запроваджують взаємозв'язки раніше незалежних підсистем. Як приклад, підсистема інтелектуального лічильника пропонує поточну інформацію про моніторинг споживання енергії, яка використовується контролерами балансування енергії, що працюють на рівнях середньої (СН) і низької напруги (НН). Ці інтерфейси забезпечують нові точки входу для зловмисних атак. Крім того, атаки можуть базуватися на впливі на взаємодію між цими підсистемами, і тому їх може бути

дуже важко виявити в межах окремого домену. Таким чином, підходи до виявлення та захисту повинні враховувати взаємодію раніше незалежних підсистем [25].

Інтелектуальні електромережі містять велику кількість компонентів датчиків і приводів, а також систем обробки та взаємозв'язку [91]. Окрім проблеми масштабу, не всі компоненти розгортаються під контролем однієї зацікавленої сторони. Таким чином, рішення безпеки для інтелектуальних мереж не можуть покладатися на обов'язкове розгортання функціональних можливостей на всіх елементах мережі, а скоріше потрібні рішення для визначення рівнів довіри компонентів і інформації, навіть якщо їх не можна змінити, а лише спостерігати.

Оскільки інтелектуальні мережі вводять додатковий інтелект і не всі зловмисні атаки можна запобігти, необхідно запровадити реактивні контрзаходи, які, можливо, повинні покладатися на відключення використання певної інформації та компонентів, якщо є підозра, що вони не заслуговують довіри. Тому необхідно підтримувати виявлення таких сценаріїв і підтримку резервних режимів роботи. Хоча це залежатиме від конкретної програми керування інтелектуальною електромережею, можуть бути допоміжні функції для виявлення та реконфігурації; це спонукає до підходу, який забезпечує проміжне програмне забезпечення безпеки з відповідними інтерфейсами, які можуть використовуватися додатками розумної мережі.

Електроенергетичній галузі бракує показників для кількісної оцінки безпеки інтелектуальної мережі. Без відповідних показників безпеки важко оцінити ефективність розгорнутих механізмів безпеки. Такі показники також допоможуть оцінити економічну ефективність різних рішень і забезпечать критерії для інвестицій.

Щодо розуміння та управління взаємозалежностями, було розроблено різноманітні моделі та симуляційні дослідження. Однак, порівнюючи вимоги до оцінки стійкості сучасної та майбутньої грід-інфраструктури з існуючими підходами, стає зрозуміло, що все ще потрібні подальші дослідження. Більшість досліджень моделювання в КІ (включаючи електромережі) використовують створені вручну блок-схеми надійності, дерева відмов або стохастичні мережі Петрі. Застосування стохастичних методів фіксує безперервну динаміку фізичного світу та дискретні характеристики інфраструктури керування. Однак для забезпечення масштабованості гібридних підходів необхідні подальші дослідження. Облік неоднорідності, гнучкості та динамічності сучасних інтелектуальних електромереж із сильним проникненням розподілених енергетичних ресурсів і відновлюваних джерел енергії вимагає передових зусиль моделювання, можливо, вимагаючи комбінації різних формалізмів/технік для опису різних компонентів системи та їхніх залежностей. Неоднорідність також необхідно розглядати на рівні вразливості, що виявляється різними підсистемами, що складають критичну інфраструктуру, і бути належним чином представлені в моделі, наприклад, використання підсистем, таких як бездротова SCADA, які, як відомо, зазвичай вразливі до помилок. і неправильне використання. Насправді прогрес у технологіях і системах SCADA покращив роботу критичних секторів, але створив додаткові вразливості, які необхідно проаналізувати та усунути, щоб належним чином захистити критичну інфраструктуру.

Глава

5 Транспорт

Транспортні системи переміщують людей і вантажі всередині країни та між країнами. Захист і безпека цих систем завжди були важливими, але стали критичними після терористичних нападів 2001 року. Знову в 2004 і 2005 роках Мадрид і Лондон були цілями атак, які стосувалися системи громадського транспорту. Сектори транспорту включають кілька підгалузей, наприклад, авіаційний, автомобільний, морський. У цьому розділі зосереджено увагу на трьох із них: диспетчерській системі повітряного руху (ATC), морській транспортній системі (MTS) і залізничній системі.

5.1 Управління повітряним рухом

Цей розділ організовано таким чином: 5.1.1 містить короткий вступ до інфраструктури УПР; 5.1.2 обговорює стандартні рішення для забезпечення безпеки інфраструктури УПР та відповідні відкриті проблеми; нарешті 5.1.3 пояснює відкриті питання (також розглядає пов’язані атаки) і обговорює деякі можливі рішення.

5.1.1 Опис критичної інфраструктури

Система УПР – це типова критично важлива система, що вимагає багато програмного забезпечення, яка відіграє ключову роль в управлінні повітряним рухом (ATM) [5]. Він надає засоби та послуги наземним диспетчерам і пілотам для безпечного керування польотами на землі та на маршруті з метою запобігання зіткненням, організації руху та надання допоміжної інформації операторам і пілотам. З точки зору архітектури дизайн системи УПР поділяється на дві основні підсистеми: на маршруті та в терміналі. Підсистема на маршруті розроблена для повітряних суден, що рухаються вздовж мережі повітряних шляхів, як правило, на великих висотах. У Європі, наприклад, ATC на маршруті сегментований у кількох районних диспетчерських центрах (ACC), кожен з яких відповідає за певну частину повітряного простору, а системи ATC у ACC співпрацюють, щоб гарантувати безпеку польотів. Підсистема зони терміналу обслуговує літаки, що летять на менших швидкостях і висотах, коли вони прибувають в аеропорти та відлітають з них. Він також повинен контролювати, згідно з правилами польотів за приладами (IFR), рух, що проходить через зону терміналу без посадки. ППП – це набір правил, які дозволяють літакам літати в несприятливих умовах, наприклад за наявності перешкод та інших літаків.

Основні зацікавлені сторони та суб'єкти

Контексти виробництва та використання систем управління повітряним рухом включають кілька зацікавлених сторін і гравців. Відповідно до EUROCONTROL1, залучені зацікавлені сторони є:

- Користувачі повітряного простору: авіакомпанії, пілоти, оператори повітряних суден і пасажири;
- Постачальники аеронавігаційного обслуговування: вони відповідають за організацію та управління потоком руху в повітрі та на землі у виділеному повітряному просторі;
- Аеропорти;
- Національні та міжнародні авіаційні регулюючі органи: національні наглядові органи та міжнародні регулюючі органи, такі як Європейське агентство з авіаційної безпеки;
- Авіаційна галузь: включаючи виробників літаків, авіоніки (авіаційної електроніки) та інфраструктури управління повітряним рухом (наприклад, радіоантени та супутники);
- Міжнародні авіаційні організації: такі організації, як Міжнародна організація цивільної авіації ООН (ICAO) або Європейська конференція цивільної авіації (ECAC).

Така кількість залучених суб'єктів вимагає надзвичайно високої уваги до можливих загроз безпеці та ризиків, які матимуть негайний вплив насамперед з точки зору безпеки, але також і в економічному плані.

Вимоги

Система АТС розроблена з використанням компонентного підходу; він має десятки тисяч вимог і складається з багатьох взаємодіючих елементів конфігурації комп'ютерного програмного забезпечення (CSCI). Основними компонентами обладнання, які підтримують ці засоби УПР, є оглядовий радар, бортові транспондери, засоби навігації, комп'ютери та лінії зв'язку.

Основні вимоги до сучасної системи УПР включають: надійність, надійність і безпеку, щоб запобігти (зловмисним або не зловмисним) загрозам, які спричиняють збої з потенційно катастрофічними наслідками, а також попередити збої в разі неочікуваних умов; продуктивність, яка стає все більш необхідною через все більш інтенсивний трафік і, як наслідок, потребу в вищій масштабованості (наприклад, здатність розробляти все більше і більше планів польотних даних за короткий час); оперативна сумісність, що передбачається як складністю та розміром загальної системи, включаючи кілька CSCI, так і необхідністю взаємодії з іншими системами УПР по всій Європі, що також є потребою, яку відчувають зацікавлені сторони; ремонтопридатність, щоб полегшити зміни через майбутні потреби інтеграції/сумісності.

[1] http://www.eurocontrol.int/articles/stakeholders

5.1.2 Стандартні рішення для захисту КІ та відкритих питань

Поточна система повітряного транспорту працює добре, але вона чутлива до збоїв (наприклад, через погоду), які можуть спричинити тривалі затримки. Крім того, система авіаційного транспорту наближається до своїх можливостей. Без трансформації очікуване зростання повітряного руху призведе до дорогих затримок рейсів і збільшення ризиків для безпеки польотів.

Поточна система банкомату в Європі фрагментована, що знижує ефективність і збільшує вартість перельоту. Оскільки до 2020 року прогнозується понад 40 000 щоденних рейсів на день, поточна система ATM не зможе ефективно впоратися з таким обсягом трафіку.

Еволюція систем УПР починається з концепції Єдиного європейського неба (SES), набору законодавчих пакетів з метою створення законодавчої бази для єдиної європейської авіації [12]. SES була створена для організації повітряного простору, спільного для європейських країн, у функціональні блоки. Основною метою проекту SES є взаємодію між європейськими банкоматами. Насправді, згідно з Регламентом (ЄС) № 549/2004 (рамковий регламент), оперативна сумісність означає набір функціональних, технічних і експлуатаційних властивостей, необхідних для систем і компонентів Європейської мережі організації повітряного руху (EATMN) і процедур для його функціонування, щоб забезпечити його безпечну, безперебійну та ефективну роботу. Інтероперабельність досягається шляхом забезпечення відповідності систем і компонентів основним вимогам. Регламент (ЄС) № 552/2004 (Регламент про сумісність) зосереджений на сумісності систем, складових і пов'язаних процедур EATMN. Це гарантує своєчасне та ефективне впровадження нових підтверджених концепцій і технологій.

Розглянуто наступні сім областей: (i) служби аеронавігаційної інформації, (ii) управління повітряним простором, (iii) управління потоком повітряного руху, (iv) обслуговування повітряного руху, (v) зв'язок, (vi) навігація, (vi) спостереження, і

(vii) метеорологічна інформація. Довгострокова програма Європейської системи управління повітряним рухом (eATMS) виконується для розробки нового покоління систем ATM/ATC, сумісних із структурою SES. Цілі eATMS включають: i) оптимізацію розгортання та обслуговування системи, ii) досягнення продуктивності, необхідної для управління збільшенням трафіку, і iii) наближення до сумісності з іншими європейськими системами ATM, як того вимагає проект SESAR (Single European Sky ATM Research) [9].]. Основні нефункціональні вимоги до eATMS стосуються: (i) надійності та безпеки для забезпечення постійної доступності та цілісності; (ii) міцність для запобігання відмовам у разі аномальних умов експлуатації; (iii) змінність, для підтримки довгострокової еволюції та інтеграції/сумісності з іншими системами, а також швидке реагування на зміни в робочому середовищі; (iv) продуктивність для підтримки збільшення повітряного руху в європейському небі; (v) безпека, для запобігання та протидії зловмисним атакам. У відповідь на ці зростаючі занепокоєння Федеральна авіаційна адміністрація США оновила наступне покоління (NextGen) і пропонує фундаментальну трансформацію, спрямовану на підвищення пропускної здатності та безпеки системи повітряного транспорту. Модернізація потребує фундаментальної трансформації всієї системи повітряного простору, включаючи впровадження супутникових технологій для операцій спостереження на заміну застарілих наземних систем, які зараз використовуються, а також модернізацію потужностей обробки ключових польотів на маршруті. компоненти, що відповідають за обробку даних польоту. Ключовими компонентами оновлення є система автоматичного залежного спостереження (ADS-B) і система процесора плану польоту (FDP).

5.1.3 Типи атак, використовувані вразливості (анатомія атаки) та економічні наслідки

FDP — це (під)система, відповідальна за обробку планів даних польоту, що містить таку інформацію,

як маршрут польоту, поточна траєкторія, інформація, пов'язана з літаком, і метеорологічні дані, і ця система передбачає напрямок кожного літака, що базується. На високому рівні загрози безпеці можуть стосуватися в основному зв'язку між бортовими системами та наземними станціями; якщо зловмисник змінить інформацію, якою обмінюється, наслідки можуть бути катастрофічними (наприклад, змінюється попередньо визначена траєкторія).

Питання безпеки в ADS-B

Поточна система повітряного транспорту працює добре, але, як зазначено вище, чутлива до збоїв (наприклад, через погоду), які можуть спричинити тривалі затримки. Крім того, система авіаційного транспорту наближається до своїх можливостей. Без трансформації очікуване зростання повітряного руху призведе до дорогих затримок рейсів і збільшення ризиків для безпеки польотів. У відповідь на зростаюче занепокоєння Конгрес США заснував Спільне управління планування та розвитку для управління оновленням NextGen. Основна мета модернізації NextGen – значно підвищити пропускну спроможність і безпеку авіаперевезень. Оновлення вимагає фундаментальної трансформації всієї національної системи повітряного простору, включно з використанням супутникових технологій для операцій спостереження на заміну застарілих наземних систем, які зараз використовуються. Аналогічну програму було запущено в Європі в рамках SESAR, технологічний та експлуатаційний вимір ініціативи SES для задоволення майбутніх потреб у пропускній здатності повітряного простору та безпеки (див. Розділ 5.1.2).

Ключовим компонентом оновлення є система ADS-B. ADS-B забезпечує безперервну трансляцію інформації про місцезнаходження літака, ідентичність, швидкість та іншу інформацію через незашифровані канали передачі даних для створення точної картини повітря для ATM. ADS-B містить методи спостереження для точного відстеження літаків, які замінюють застарілі можливості. Дійсно, оперативні плани стверджують значний прогрес у безпеці, ефективності та гнучкості в порівнянні з поточною інфраструктурою системи повітряного простору. ADS-B призначений для покращення ситуаційної обізнаності диспетчера повітряного руху, запобігання зіткненням, запобігання виходу на наземну злітно-посадкову смугу та управління повітряним рухом у нерадарних середовищах (наприклад, спостереження за океаном). Підвищена точність забезпечить жорсткіші стандарти ешелонування повітряних суден, вищу ймовірність запитів на дозвіл і покращені візуальні заходи на посадку, що все сприятиме більшій пропускній здатності літаків. Крім того, ADS-B призведе до більш прямих маршрутів і оптимізованих вильотів і заходів на посадку, що збільшить пропускну спроможність і заощадить час і паливо. Нарешті, інфраструктура ADS-B базується на простих радіостанціях, встановлення та обслуговування яких значно дешевше, ніж механічна інфраструктура, пов'язана з традиційними наземними радіолокаційними станціями.

ADS-B розроблено для перегляду поточних методів спостереження за повітряним рухом, одночасно надаючи нові можливості, які покращать ATM. ADS-B працює автоматично, оскільки не потребує втручання пілота чи диспетчера. Це залежне спостереження, оскільки літальний апарат отримує власну позицію від глобальної навігаційної супутникової системи. Крім того, він постійно транслює інформацію про положення літака та інші дані на найближчі наземні станції, літаки та наземні транспортні засоби (наприклад, літаки, що рулять). ADS-B також забезпечує кращу точність порівняно зі звичайними радарами (точність 200 метрів у порівнянні з 300 метрами на відстані 60 морських миль і з точністю, яка не погіршується зі збільшенням радіусу дії приймача).

У Європі впровадження ADS-B є частиною Пакету впровадження 1 (IP1), 2008–2013, Генерального плану ATM SESAR. В Італії ENAV розпочав програму, яка фінансується Європейським Союзом під назвою Programma di Implementazione Nazionale dell'ADS-B'

(Національний план впровадження ADS-B), у рамках Італійського плану впровадження зв'язку та спостереження IP1, який метою є посилення служб спостереження за допомогою технологій на основі ADS-B. План передбачає встановлення чотирнадцяти наземних станцій по всій Італії.

Стверджується, що експлуатаційні вимоги вимагають використання незашифрованих каналів передачі даних, і стверджується, що існує низька ймовірність зловмисного використання. FAA провело кілька аналізів аспектів безпеки ADS-B. Система підлягала сертифікації та акредитації згідно з рекомендаціями Національного інституту стандартів і технологій (NIST), що стосуються конфіденційності, цілісності та доступності, а також інших цілей безпеки. FAA дійшло висновку, що «використання даних ADS-B не піддає літак будь-якому підвищеному ризику порівняно з ризиком, який існує сьогодні» [93]. Крім того, FAA вважає, що шифрування без потреби обмежить міжнародне використання ADS-B.

Проте звіт FAA викликає деякі серйозні занепокоєння з точки зору безпеки [126]. Зокрема, історичні випадки продемонстрували, що незашифровані канали передачі даних можуть бути використані вмотивованим супротивником. Ще в 2006 році висловлювалися занепокоєння щодо здатності хакерів вводити до 50 помилкових цілей на екранах радарів авіадиспетчерів [186]. У 2010 році була випущена програма (додаток) для iPhone та Android під назвою Plane Finder AR, яка дозволяє точно відстежувати літак за допомогою передач ADS-B [140]. У 2012 році Костинг і Франсійон продемонстрували, що атаки на захист ADS-B є простими та практично здійсненними для помірно досвідченого зловмисника [80]. Атаки варіюються від пасивних атак (прослуховування) до активних атак (перешкода повідомленням, повторне відтворення ін'єкції). Нарешті, X. Teco нещодавно продемонстрував практичну демонстрацію того, як дистанційно атакувати літак і повністю контролювати його. На етапах виявлення та збору інформації використовувався протокол ADS-B [169].

З цих причин нещодавно було розпочато більш глибоке дослідження безпеки ADS-B. McCallie та ін. нещодавно проаналізували вразливості системи безпеки, пов'язані з впровадженням ADS-B, і надали таксономію атак, включаючи розвідку літака, заборону затоплення наземної станції, відмову затоплення цільової наземної станції, заперечення затоплення літака, фантомну ін'єкцію цілі літака та багаторазову фантомну ін'єкцію наземної станції [126]. Автори також досліджують потенційний вплив атак на авіаперевезення та надають рекомендації, які могли б підвищити безпеку, якщо їх інтегрувати в план впровадження ADS-B. Крім того, Finke et al. досліджували доцільність використання шифрування зі збереженням формату, зокрема алгоритму FFX, у середовищі ADS-B [94]. Здатність алгоритму плутати та розсіювати передбачувані вхідні повідомлення перевіряється з використанням ентропії повідомлення як метрики. На основі аналізу надаються рекомендації, які виділяють області, які слід вивчити для включення до плану оновлення ADS-B.

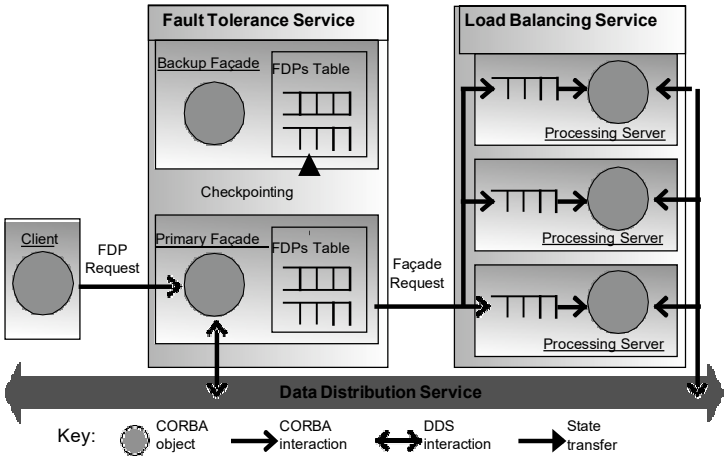
Однак важливі питання, такі як управління ключами, все ще залишаються відкритими. Один витік ключа ставить під загрозу всю систему. Дійсно, це серйозна перешкода, яку необхідно подолати перед тим, як розглядати можливість використання симетричного шифру в сильно розподіленій системі. Тим не менш, симетрична система ефективно використовується військовими для шифрування ідентифікаційних передач у режимі 4 (IFF) [111]. Рішення ADS-B, призначене для забезпечення конфіденційності спостереження, може бути змодельовано за цим прикладом.

Проблеми безпеки в процесорі Flight Fata (FDP)

Вимоги наступного покоління систем УПР включають удосконалення, пов'язані зі зв'язком між наземним персоналом і пілотами, які полягають у: (i) зміні ситуаційної обізнаності пілотів шляхом надання тієї ж інформації про повітряний рух у реальному часі, що й диспетчери УПР. ; (ii) запобігання конфлікту повітряного руху шляхом виявлення та вирішення; (iii) надання надзвичайно

точних даних про повітряний рух для пілотів і наземного персоналу. Системи УПР покладаються на системи спостереження для обміну та трансляції інформації про польоти серед диспетчерського персоналу та пілотів. Сучасні системи спостереження спрямовані на підвищення безпеки управління та контролю повітряного руху. На жаль, уразливості в системі спостереження та трансляції дозволяють зловмисникам використовувати програмні компоненти систем УПР, такі як FDP. FDP — це система, яка надає таку інформацію, як маршрут польоту, поточна траєкторія, інформація про літак і метеорологічні дані. Він обробляє детальну інформацію про літак, щоб передбачити профілі плану польоту (наприклад, напрямок) кожного літака. Ця інформація поєднується з сигналами (наприклад, радіолокаційним сигналом стеження) для вимог безпеки, таких як середньострокові та короткострокові попередження про конфлікти.

Бортові системи взаємодіють із системою адресації та звітування літаків (ACARS) для передачі повідомлень наземним станціям. У той же час наземні станції керують літаком під час місії, і він використовується для обміну текстовими повідомленнями між літаками та наземними станціями через всесвітню передачу по радіо (VHF) або супутнику. Спочатку ACARS використовувався для автоматичного виявлення та звітування про зміни в основних фазах польоту, які називаються OOOI (Out of the Gate, Off the Earth, On the Earth і Into the Gate). На початку кожної фази польоту на землю передавалося цифрове повідомлення, яке містило фазу польоту, час, коли вона відбулася, та іншу пов'язану інформацію, таку як кількість палива на борту або пункт відправлення та призначення рейсу. Ці повідомлення використовуються для відстеження стану літаків і екіпажів. Промисловість почала модернізацію бортових комп'ютерів технічного обслуговування в 1990-х роках для підтримки передачі інформації, пов'язаної з техобслуговуванням, у режимі реального часу через ACARS. Це дозволило технічному персоналу авіакомпанії отримувати дані в режимі реального часу, пов'язані з несправностями технічного обслуговування літака. Блок управління ACARS був представлений для автоматичного виконання всіх описаних вище обробок без втручання льотного екіпажу. Зловмисник може проникати в системи ACARS, щоб надсилати повідомлення бортовим системам літака або змінювати план даних польоту, керований FDP (наприклад, спричиняючи відхилення від попередньо визначеного шляху). Помилки в протоколі ACARS: (i) використання простих шифрів, (ii) обмін дуже детальною інформацією про літак, такою як публічна база даних, локальні дані та віртуальні літаки.



Малюнок 5.1: Спрощене подання архітектури FDPS

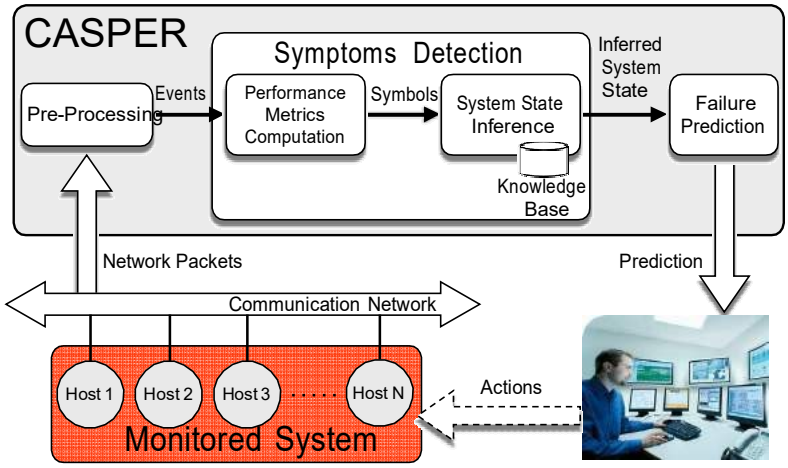
5.1.4 Підходи до пом'якшення несправносте

Релевантним прикладом відмовостійкої архітектури, прийнятої в домені АТС, є система обробки польотних даних (FDPS), описана нижче. FDPS — це розподілене програмне забезпечення, розроблене на C++, яке використовує CARDAMOM, відмовостійке проміжне програмне забезпечення, сумісне з CORBA [79]. Це частина системи УПР, яка відповідає за керування планами польотних даних (FDP). Мета FDPS – підтримувати FDP в актуальному стані. Наприклад, FDPS має аналізувати фактичне положення літаків, отримане з радіолокаційних слідів, і оновлювати маршрут польоту, щоб ефективно розподілити простір польоту та уникнути зіткнень.

Архітектура FDPS (рис. 5.1) складається з фасадного компонента, який діє як інтерфейс системи та відтворюється службою відмовостійкості CARDAMOM (FT), а також набором із трьох серверів обробки (PS), керується службою балансування навантаження (LB). Сервісні запити для вставки, видалення та оновлення FDP доставляються на фасад через проміжне програмне забезпечення. Фасад пересилає запити до конкретного PS відповідно до циклічного планувальника. Вибраний сервер отримує зазначений екземпляр FPD із служби розподілу даних (DDS), сумісного зі стандартом служби розподілу даних OMG [145], виконує обчислення, пов’язані з запитом, і повертає оновлений екземпляр FDP на фасад. Нарешті, фасад поширює оновлений FDP через DDS і відповідає клієнтам.

Стан запитів для кожного FDP зберігається в таблиці FDP на фасаді. Служба FT виконує гарячу реплікацію процесу фасаду: таблиця FDP перевіряється під час кожного оновлення та передається до резервних реплік, які активуються у разі збою основної репліки. Цей механізм гарячої реплікації, реалізований у FDPS, використовує CARDAMOM FT API. У разі несправності головного фасаду, наприклад збою процесу, CARDAMOM виявляє несправність і активує повторений фасад, який замінює основний фасад і забезпечує безперервність обслуговування.

Представлена вище відмовостійка архітектура реагує на несправності, щойно вони виникли та були виявлені. У деяких випадках збої в системі можуть виникати непоміченими, уникаючи механізмів відмовостійкості та призводячи до системних збоїв. Таким чином, онлайн-прогнозування відмов є заслуговуючим на увагу підходом для подальшого покращення доступності критично важливих систем, таких як системи УПР. Він передбачає виникнення короткочасних збоїв під час виконання системи. Коли прогнозується, що збій станеться найближчим часом, предиктор створює сповіщення, яке дозволяє своєчасно запустити певний (людський або автоматичний) механізм відновлення. Прогнозування збоїв базується на моніторингу симптомів під час виконання, тобто поведінки системних параметрів, що виходить за межі норми, що є побічним ефектом збоїв у системі. CASPER (рис. 5.2) — це онлайнова система прогнозування відмов, яка була прийнята для прогнозування відмов у системах УПР [52]. CASPER — це ненав’язлива система моніторингу, оскільки для неї не потрібно ні встановлювати програмне забезпечення, ні входити в систему на хостах контрольованої системи, що дозволяє уникнути проблем конфіденційності та безпеки. Крім того, це підхід моніторингу «чорної скриньки». Він розглядає компоненти системи, що контролюються, як чорні скриньки, не вимагаючи знання про внутрішні елементи та логіку системи, що контролюється, і не намагається розпізнати шляхи причинності між скриньками.



Малюнок 5.2: Архітектура прогнозування несправностей CASPER.

5.2 Морська транспортна система

Цей розділ організовано таким чином: 5.2.1 містить короткий вступ до інфраструктури системи морського транспорту (MTS); 5.2.2 обговорює стандартні рішення для забезпечення безпеки інфраструктури МТС та відповідні відкриті проблеми; нарешті 5.2.3 пояснює на прикладі набір атак, які можна здійснити з використанням відомих уразливостей.

5.2.1 Опис критичної інфраструктури

Враховуючи визначення CI, наведені в Розділі 1, і той факт, що морський сектор підтримує суспільство та економіку через рух людей і життєво важливих товарів, таких як енергія (транспортування нафти і газу) і продовольство, морський сектор слід вважати критична інфраструктура [89].

З одного боку, морська інфраструктура має вирішальне значення для використання національної морської сили, з іншого боку, вона є можливою мішенню для терористичних актів. Дійсно, успішна атака на порт може завдати серйозної економічної та військової шкоди, призвести до збільшення кількості жертв і мати серйозні довгострокові згубні наслідки для національної економіки.

Захист критичної морської інфраструктури (MCIP) представляє багато проблем у сучасному асиметричному середовищі [184]. Попередні моделі морської оборони були зосереджені на захисті кораблів від традиційної морської атаки, яка йде з моря: навіть якщо цілями вважалися порти та допоміжна інфраструктура, наголос робився на захист від військової загрози.

Сценарій після 11 вересня створив новий погляд на морську оборону. Багато цілей, які не мають жодного військового значення в звичайній війні, наприклад символічні будівлі та місця, тепер повинні враховуватися в стратегічному плануванні оборони. Можливі загрози з моря широкомасштабні та різноманітні, вони покладаються на комбінацію асиметричної наступальної

тактики з використанням різноманітності прибережної зони.

Основні категорії загроз для безпеки портового засобу стосуються [147]:

- Крадіжки та диверсії;
- Тероризм;
- Нелегальна торгівля та міграція;
- Екологічні загрози та масштабні аварії.

Крім того, необхідно враховувати нові та нові асиметричні загрози [147]:

- Політичний транснаціональний і міжнародний тероризм;

Дії, які можуть завдати шкоди безпеці національних і міжнародних транспортних систем;

- Індивідуальні чи групові дії щодо незаконного доступу до інформаційних систем;

Навмисні дії, які можуть вплинути на довіру та серйозність нації;

- Умисні акти екологічного саботажу.

У зв’язку зі складністю діяльності та великими територіями для обстеження в порту, вкрай необхідним є впровадження Об’єднаних портових операційних центрів (JHOC) як компонента захисту морських антитерористичних сил [184]. Розробка мультиагентних систем внутрішньої безпеки на морі є логічним наступним кроком у проблемі безпеки та захисту портів, що розвивається.

Основні зацікавлені сторони та суб'єкти

Безпека критичної інфраструктури морського сектору все більше стає пріоритетом для ключових європейських зацікавлених сторін, включаючи Європейську комісію, уряди європейських держав-членів і головних гравців з приватного сектора [89].

На глобальному рівні відповідні зацікавлені сторони включають, не обмежуючись цим, різні міжурядові організації, такі як Міжнародна морська організація (IMO), Всесвітня митна організація (WCO) і Міжнародне морське бюро ICC (IMB), яке є спеціалізованою відділ Міжнародної торгової палати (ICC). Крім того, також важливо згадати про актуальність Міжнародної корпорації морської безпеки (IMSC), яка зосереджена на діях, спрямованих на захист суден, їхніх екіпажів і вантажу від різноманітних загроз.

Відсутність координації між зацікавленими сторонами на різних рівнях, наприклад, європейському та національному, призводить до серйозних розбіжностей у тому, як розглядається питання безпеки на морі.

Список гравців у цьому секторі включає як приватних, так і державних агентів:

- Власники та оператори промислових об’єктів;
- Працівники промислового(их) об’єкта(ів);
- Постачальники, клієнти, користувачі;
- Організації та персонал з реагування на надзвичайні ситуації;

- Екіпажі суден;
- Судноплавні компанії;
- Рибне господарство на території;
- Туристичні компанії;
- Поромні компанії;
- Місцеві громади;
- Прибрежні уряди;
- Спільноти, користувачі та компанії вниз по ланцюгу поставок;

З вищевикладеного стає зрозумілим, що захист критичної морської інфраструктури є складною проблемою, яку важко вирішити, і що лише синергетичні, спільні та скоординовані зусилля можуть бути ефективними.

Вимоги

Інтегрована система безпеки (ICO) для району морського порту має досягати наступних завдань [147]:

1. Розширене виявлення будь-яких спроб вторгнення в зони безпеки порту;
2. Передача сигналів тривоги та диверсії програмному забезпеченню, надаючи йому можливість дистанційно контролювати активацію та деактивацію зон безпеки та підтверджувати сигнали тривоги;
3. Спостереження за загрозами;
4. Поширення даних про безпеку на місцевому та центральному рівнях порту, а також в інших установах, залучених до розповсюдження подій безпеки.

Щоб реалізувати ISS для критичної морської інфраструктури, необхідно вказати, що будь-яка портова територія може бути фізично охарактеризована різними частинами, а саме межами периметра, точками доступу та інфраструктурою (такою як транспорт, система зв'язку, комунальні послуги тощо).

Щоб забезпечити безпеку та безпеку всіх цих частин, основною функцією системи безпеки є контроль потоку доступу всередині порту, що передбачає необхідність запобігання несанкціонованому доступу через точки доступу.

Можливість стеження може бути об'єднана в одну мультиагентну систему:

- Береговий радар;
- Система обслуговування руху суден (VTS);
- Процесор автоматизованої системи ідентифікації (AIS);

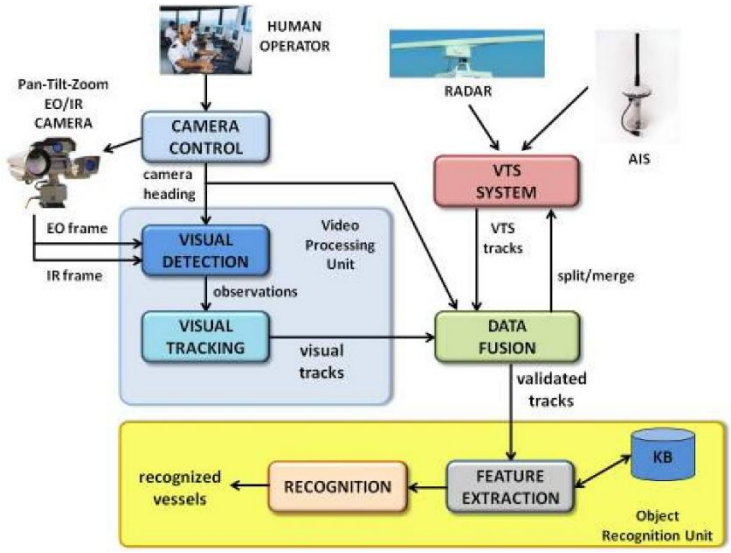
- Система камер управління портами;

- Тепловізійна система для роботи в нічний час.

Показано загальну структуру для багатоагентної автоматичної системи спостереження, що дозволяє об'єднувати дані інформації, що надходить з різних джерел, а саме радарів, електрооптичних (ЕО) камер денного світла та інфрачервоних (ІЧ) камер нічного часу. на малюнку 5.3.

Візуальний пристрій EO-IR є основним датчиком, і оператор може переміщати його через модуль керування. Модуль керування забезпечує орієнтацію та поле зору (FOV) від пристрою до VPU, який відповідає за виявлення та відстеження судин за допомогою візуальної інформації. Модуль об'єднання даних отримує дані як від VPU, так і від системи VTS. Його мета полягає в тому, щоб пов'язати візуальні треки, отримані в результаті аналізу відео, із треками, згенерованими з радара та даних AIS. Таким чином, можна надати користувачеві новий візуальний вимір на додаток до традиційного геоприв'язаного радарного вигляду VTS. Крім того, модуль об'єднання даних надсилає інформацію зворотного зв'язку до системи VTS, щоб підвищити точність виявлення радара.

Треки, згенеровані модулем об'єднання даних, вважаються дійсними, і блок розпізнавання об'єктів може класифікувати їх відповідно до їхніх візуальних характеристик.



Малюнок 5.3: Функціональна архітектура пропонованого каркаса. Модуль об'єднання даних керує інформацією, що надходить від блоку візуальної обробки та системи VTS, і надсилає перевірені треки до блоку розпізнавання об'єктів.

5.2.2 Стандартні рішення щодо захисту КІ та відкритих проблем

Модель оборони часів холодної війни покладає відповідальність за порти та розвантажувальні операції на ВМС і берегову охорону. Оборонними операціями керують шляхом спільного розміщення персоналу берегової охорони та військово-морського флоту в оперативних центрах, які будуть контролювати всі військові операції (включаючи операції з розвантаження та захист критичної інфраструктури) у порту під час надзвичайної ситуації.

У стандартній моделі оборони часів холодної війни ризик значною мірою був питанням

пропорційності, а загроза критичній морській інфраструктурі була виключно військовою. Розглядаючи найгірший сценарій, планувальники передбачали дії ворога на узбережжі, зосереджуючись на атаках підводних човнів, наступальному мінуванні та атаках спеціальних операцій на критичну військову інфраструктуру. Передбачалося, що терористичні дії будуть спонсоровані ворожою державою і, як частина ворожої стратегії, не будуть спрямовані проти об'єктів, які мають обмежене військове значення або взагалі не мають такого значення.

До 11 вересня берегова охорона порту та морські тактичні споруди були розділені на дві окремі зони відповідальності залежно від типу правоохоронних заходів. Регуляторні функції, такі як огляд судна, реагування на навколишнє середовище, ліцензування тощо, виконували інспектори суден, які виконували свої обов'язки без зброї. Операції більш традиційного різновиду правоохоронних органів, такі як боротьба з наркотиками або рибальство, пошук і порятунок, а також інші офшорні операції були відповідальністю озброєного персоналу.

Терористична атака 11 вересня продемонструвала крихкість цього стандартного оборонного підходу. Різниця між до та після 11 вересня полягає в тому, як інтерпретувати концепцію потенційних цілей. Наприклад, у сценарії до 11 вересня суто цивільна ціль, така як Всесвітній торговий центр, не вважалася б дійсною ціллю в Нью-Йорку. Дійсно, головний пункт завантаження зброї в Ерлі, штат Нью-Джерсі, був Першим пріоритетом для захисту інфраструктури. Очевидно, що це змінилося: морська інфраструктура, яка не вважалася б критичною за сценарієм холодної війни, тепер має потенціал стати мішенню для досягнення економічної чи психологічної перемоги.

Оскільки терорист може вибрати потенційно нескінченний список невійськових цілей, неможливо мати достатньо оборонних сил для захисту всіх потенційних цілей. Це не означає, що модель холодної війни абсолютно недійсна або що ми не можемо навчитися з уроків історії. У моделі до 11 вересня військовій розвідці доводилося мати справу з конкретною військовою загрозою проти відомих цільових районів, з відповіддю, яка була чітко військовою. Нова загроза вимагає, щоб оборонна модель була розширена, щоб врахувати всіх гравців у порту, життєво важливих для повного захисту.

Відкриті питання

Можна виокремити два основних відкритих питання:

- Існуючі стандарти, методології та інструменти морської безпеки є монолітними та зосереджені виключно на фізичній безпеці;
- Торговельні порти не розглядаються як критична інфраструктура, а безпека їх інформаційних та телекомунікаційних систем не організована.

Уроки минулого показують, що ключем до ефективної оборони є тактична координація через спеціальне багатоагентне командування та контроль [184]. До 11 вересня моделлю командування й управління було протидіяти військовій загрозі з моря, але це змінилося з появою нових асиметричних загроз. Концепція JHOC довела свою ефективність у багатовідомчому об'єднанні розвідувальних даних і скоординованих тактичних портових операціях, необхідних для захисту критичної морської інфраструктури, і її слід розглядати як модель скоординованої оборони порту.

5.2.3 Типи атак, використовувані вразливості (анатомія атаки) та економічні наслідки

Асиметричні загрози портам, зокрема терористичні, є відносно новим елементом у спектрі

морської війни. До недавнього часу порти складалися з інфраструктури, яку було відносно легко замінити або відтворити, що робило їх відносно низькопріоритетними цілями для ворога, спрямованого на нанесення ударів по морській силі [184].

Сьогодні порти стали центрами високотехнічної, добре інтегрованої інфраструктури, призначеної для швидкого завантаження та розвантаження вантажів, еволюція, яка стала дуже складною в епоху контейнеризації. Портові вантажні операції також сильно залежать від мережевих операцій, що значно спрощує зрив процесу для потенційного зловмисника. Це зробило великі порти більш важливими в економічному та стратегічному відношенні, водночас зробивши їх більш привабливими цілями для терористичних дій.

При оцінці атаки на портовий засіб слід враховувати наступні аспекти.

Економічний ефект. Імпорт і експорт залежать від перевезень морем. Успішна атака на морську інфраструктуру вплине на цю торгівлю набагато більше, ніж реальна фізична шкода. Атака на один порт матиме каскадний ефект на інші порти. Затримка відправлення при навантаженні та вивантаженні вантажу є одним з найбільш витратних елементів процесу доставки.

Висока видимість. Ports are not isolated areas, but rather major centers of commerce, usually surrounded by large cities and economic activities. An attack on a port could be highly visible and potentially the scene of mass con-flagration. As a result of urban development, most major ports are no longerconfined to strictly industrial areas, but rather have become well-developed centers of commerce and entertainment, surrounded by built up waterside ar- eas dedicated to tourism and recreation. Many of these facilities are located next to volatile maritime infrastructure (fuel tanks, docks, etc.) that could create mass conflagration if attacked through large explosive force. Sympa- thetic detonation, fires, and other catastrophic effects would certainly createmass casualties.

Легкість атаки. Торговельні порти не є фортецями. Океан сам по собі дає ряд явних переваг для цілеспрямованого зловмисника, особливо коли він використовує морський терорист-смертник або засоби для швидкої доставки великої вибухової сили. Вода є не тільки надзвичайно ефективним транспортним засобом (забезпечує швидкий транзит), але й великий обсяг законного комерційного та рекреаційного руху в портах дозволяє ворогу маскувати рухи перед нападом, ускладнюючи ефективний захист.

5.2.4 Стратегії захисту

Враховуючи важливість портів для економіки та військової могутності, цілком ймовірно, що порти стануть мішенню для майбутніх терористичних атак.

MCIP — це критична вразливість, яку необхідно усунути шляхом скоординованих зусиль різних агентів. Ця місія виходить за рамки традиційних операцій з безпеки портів або захисту антитерористичних сил і вимагає командно-контрольної структури, яка може по-справжньому об'єднати безліч обов'язків і операцій у портах.

Різноманітність загроз для портів і кількість регуляторних органів, які наглядають за критичною інфраструктурою, вимагає розширеної комплексної системи командування та управління, яка об'єднує багатовідомчі розвідувальні дані, має розуміння багатовідомчих можливостей і може забезпечувати напрямок цим силам у поле.

Багатоагентні JHOC пропонують кілька переваг для поєднання ефективних портових операцій і захисту критичної інфраструктури. Це очевидно в сферах злиття розвідувальних даних, скоординованого планування та тактичного командування й контролю. Європейські країни-члени повинні обмінюватися даними, пов'язаними з морським контекстом. Необхідна відповідна ідентифікація та категоризація відповідних даних, щоб полегшити угоду щодо обміну даними між

різними зацікавленими сторонами.

Однак, щоб розробити ефективну JHOC, необхідно подолати низку труднощів. Наприклад, щодо інцидентів кібербезпеки та інших пов'язаних з кіберзагрозами (наприклад, шахрайства, електронних злочинів тощо), з якими стикається морський сектор, відсутність обміну інформацією між залученими суб'єктами є критичною проблемою [89]. Кібербезпека не повинна бути спрямована лише на основні порти. Навіть менш розвиненим портам слід запропонувати можливість впровадження ініціатив з кібербезпеки.

Крім того, рівень зрілості впровадження ІКТ значно відрізняється від одного порту до іншого, а безпека не завжди є пріоритетом. Таким чином, першим кроком до досягнення кібербезпеки на рівні порту буде впровадження систем ІКТ, які є безпечними за своєю конструкцією.

5.3 Залізнична система

Цей розділ організовано таким чином: 5.3.1 містить короткий вступ до критичної інфраструктури залізниці; 5.3.2 обговорює типове рішення для забезпечення безпеки залізничної інфраструктури та відповідні відкриті проблеми; 5.3.3 пояснює на прикладах набір атак, які можна здійснити з використанням відомих уразливостей; нарешті 5.3.4 підсумовує відкриті проблеми, пропонує деякі оновлення системи та вводить аналіз ризиків для пом'якшення майбутніх атак і загроз.

5.3.1 Опис критичної інфраструктури

Залізничні системи перевозять людей і вантажі всередині країни та між країнами. Однак до 1989 року в Європейському Союзі застосовувалися різні, часто несумісні механізми контролю. Європейська система управління залізничним рухом (ERTMS) — це ініціатива, яка має на меті подолати цю ситуацію шляхом визначення спільного стандарту для підвищення сумісності між залізничними системами різних країн. ERTMS складається з Європейської системи управління поїздами (ETCS) і GSM-R. ETCS — це стандарт для керування поїздом у кабіні, який включає системи сигналізації та захисту поїзда. GSM-R, розширення GSM, є радіосистемою для забезпечення передачі голосу та даних між колією та поїздом.

Оскільки «порушення роботи залізничної інфраструктури можуть мати значний негативний вплив на економіку та безпеку окремої країни» [51], а поточна залізнична система залежить від ІКТ (зазвичай для підвищення продуктивності), аспекти безпеки та безпеки (особливо для бездротового зв'язку). комунікації) стають критичними.

Основні зацікавлені сторони та суб'єкти

Залізнична система є наднаціональною критичною інфраструктурою, яка має широкий спектр зацікавлених сторін та гравців. Розглядаючи європейську залізничну систему, основними зацікавленими сторонами є: Європейська Комісія, яка визначає керівні принципи інтеграції залізничної системи; Європейські країни-члени, які контролюють систему; приватні/державні компанії, які впроваджують і керують інфраструктурою (наприклад, Rete Ferroviaria Italiana, RFI), і місцеві громади, які отримують вигоду від послуг транспортування товарів і людей. Крім того, список гравців включає кілька акторів, від міжнародних/національних компаній до пасажирів. Проста, невичерпна класифікація включає: державні та приватні залізничні транспортні компанії для пасажирів і вантажів (наприклад, Trenitalia); компанії-постачальники: наприклад, система залізничної сигналізації, потяги, IT-послуги тощо; судноплавні компанії; пасажири; місцеві транспортні компанії (наприклад, Gruppo Torinese Trasporti, GTT); співробітники різних компаній (наприклад, Trenitalia,

GTT).

Оскільки залізнична система включає кілька зацікавлених сторін і гравців від місцевих громад до національних, економічні інтереси є дуже високими, а підривні проблеми (наприклад, тероризм) можуть наражати систему, а отже, людей і товари, на фізичні та електронні атаки.

Вимоги

Як відомо, надійність залізничної системи базується на надійності, доступності, ремонтопридатності, безпеці та безпеці (RAMSS). Ці атрибути керують визначенням вимог, які повинні бути виконані, щоб уникнути або обмежити нещасні випадки та атаки. Хоча залізнична система складається з різних компонентів і для забезпечення її надійності потрібен цілісний підхід, цей розділ головним чином зосереджений на аспектах зв'язку між електронними системами, які широко обговорювалися в літературі та були визначені європейськими залізничними стандартами.

Два стандарти, зокрема, застосовуються до зв'язку в електронних системах безпеки. Перший – це CEI EN 50159-1 [71] для закритих систем передачі (згідно з [71], закрита система передачі складається з фіксованої кількості або фіксованої максимальної кількості учасників, пов'язаних системою передачі з добре відомими та фіксовані властивості, де ризик несанкціонованого доступу вважається незначним) і CEI EN 50159-1 [72] для відкритих систем передачі (згідно з [72] це система передачі з невідомою кількістю учасників, що має невідомі, змінні та недовірені властивості, які використовуються для невідомих телекомунікаційних послуг і для яких буде оцінено ризик несанкціонованого доступу).

Стандарт EN 50159-1 містить набір вимог до закритих систем передачі. Коротко кажучи, є шість основних вимог, які повинні бути забезпечені:

- захист безпеки буде застосовано до генерації даних для передачі;
- реакція безпеки буде застосована у разі неправильної роботи. Це має відповідати вимогам безпеки приймача;
- механізм виявлення помилок буде застосований на приймачі та відповідатиме вимогам безпеки приймача;
- реалізація реакції безпеки буде функціонально незалежною від недовіреної системи передачі;
- частота залишкових помилок системи передачі, пов'язаної з безпекою, для кожного обміну інформацією між передавачем і приймачем буде меншою за заздалегідь визначене значення. Ця швидкість має бути сумісною з рівнем цілісності безпеки кожного приймача;
- рівень повноти безпеки пов'язаної з безпекою системи передачі буде відповідати найвищому рівню повноти безпеки процесів безпеки;

Зауважте, що ці вимоги пов'язані з безпекою та прямо не згадують про загрози безпеці, які можуть виникнути через втручання, зовнішніх зловмисників або зловмисних авторизованих користувачів. Це відповідає визначенню закритої системи передачі, наведеному вище.

Стандарт EN50159-2 містить набір інструкцій і вимог для відкритих систем передачі. Зокрема, визначено сім можливих загроз безпеці: повторення, видалення, вставка, повторна послідовність, пошкодження, затримка та маскарад. Стандарт містить вказівки щодо захисту безпеки системи передачі; це порядковий номер, позначка часу, час очікування, ідентифікатори джерела та призначення, повідомлення зворотного зв'язку, процедура ідентифікації, код безпеки та

криптографічні методи.

Зауважте, що цей стандарт розглядає лише неавторизованих користувачів, але не розглядає можливість зловмисних дій авторизованих користувачів.

5.3.2 Стандартні рішення для захисту КІ та відкритих питань

Залізнична система має вирішальне значення для економічного та соціального добробуту кількох, якщо не всіх, країн ЄС; Італійська залізнична система є однією з найважливіших частин інфраструктури Італії, загальна протяжність якої перевищує 24 000 км. У цьому розділі в загальних рисах обговорюється, до якої міри безпека вважається проблемою для залізничної інфраструктури та який поточний рівень захисту. У закритих системах передачі ризик втручання зазвичай вважається незначним, а потенційні дії зловмисних авторизованих користувачів пом'якшуються внутрішньою логікою системи: компоненти, які відповідають за прийняття рішень, наприклад, Європейський життєво важливий комп'ютер (EVC). , не допускають певних дій, якщо вони не підтверджені датчиками та іншими (незалежними від людини) індикаторами (наприклад, балізами або центром радіомовлення). Приклад закритої системи та пов'язані з нею проблеми безпеки наведено в розділі нижче.

Натомість у відкритій системі передачі безпека фактично вважається проблемою, хоча ми повинні пам'ятати, що стандарт EN50159-2 вимагає безпеки, щоб гарантувати безпеку. Тобто, доступність прямо не розглядається в стандарті: DOS-атаки можуть призвести до блокування зв'язку та, як наслідок, примусової зупинки поїздів, хоча це не впливає на безпеку. Цей підхід широко застосовувався в минулому, але його слід переглянути, враховуючи актуальність, яку зараз набуває критична інфраструктура. Неочікувана зупинка поїзда призводить до затримок (також із каскадним ефектом для всіх поїздів, які мають одну лінію) і, зрештою, втрати грошей: атаки на кібербезпеку, спрямовані на систему передачі, що призводять до недоступності, можуть бути неприйнятними. Насправді, можна використати безвідмовну поведінку ERTMS і створити ситуацію, яка призведе до зупинки поїзда [58]. Хоча DoS-атака на ERTMS може не вплинути на безпеку, вона може спричинити збої або дискомфорт для пасажирів. Тому DoS-атаки актуальні як мінімум для доступності сервісу.

Більш детально [58] розглядає різні компоненти (та їхні інтерфейси), які взаємодіють із бортовою системою ETCS. Інтерфейс машиніста та поїзда визначено лише на функціональному рівні, і жодних інших вимог для їх реалізації не передбачено. І машиніст, і потяг вважаються надійними компонентами, оскільки машиніст може перекрити всю систему ERTMS/ETCS і потяг, оскільки він міг бути саботований іншими способами (наприклад, скомпрометувати гальмівну систему). Однак важливою проблемою є те, що специфікації не визначають автентифікацію на каналах зв'язку, які використовуються для цих інтерфейсів. Хоча, чи є цей підхід прийнятним у закритій мережі (тобто інтерфейси, підключені лише до ETCS), у налаштуваннях, де бортові системи підключені до мережі, яка передає інші послуги, наприклад, доступ до Інтернету для пасажирів , ці компоненти можуть бути скомпрометовані (наприклад, шкідливим програмним забезпеченням). Балізи є частиною системи сигналізації та розміщуються на колії. Хоча балізи захищені від випадкових помилок передачі та перешкод, а ERTMS/ETCS забезпечують різні рівні перевірки узгодженості даних, механізм автентифікації не передбачено. Знову ж таки, це робить можливими зловмисні атаки, наприклад, зловмисник може підробити балізу та надіслати підроблені дані, підірвати існуючу балізу або розмістити нову балізу на доріжці.

ERTMS розрізняє пов’язані та незв’язані балізи. Розташування зв’язаних баліз передається по радіо по захищеному каналу в поїзди. Якщо поїзд не зустрічає пов’язану балізу в очікуваному місці, він зупиняється. Навпаки, незв'язані балізи можна було зустріти всюди. Навіть якщо поїзди приймають обмежену кількість команд від незв’язаних баліз, деякі DoS-атаки все ще можливі, а деякі команди можуть використовуватися для створення небезпечної ситуації. Метою протоколу Євророадіо [26] є передача зв’язаних повідомлень баліз до поїзда через мережу GSM-R. Зокрема, зв'язок встановлюється за допомогою спільного секретного ключа, що забезпечує автентичність і цілісність повідомлень. Однак протокол не гарантує конфіденційності переданої інформації, тому, якщо мережа GSM-R буде скомпрометована, зловмисник зможе підслухати повідомлення ERTMS і, можливо, отримати конфіденційну інформацію за допомогою атаки «людина в центрі» [58]. Крім того, Євророадіо пропонує використовувати як базовий криптографічний алгоритм Triple DES, а не більш ефективний алгоритм, як-от AES. Інша проблема полягає в управлінні розповсюдженням ключів, оскільки специфікації сумісності ERTMS/ETCS стосуються лише безпечного керування ключами між різними доменами керування ключами, залишаючи розподіл ключів у межах домену керування ключами для національного впровадження [58]. Хоча було запропоновано нову специфікацію для пом’якшення цієї проблеми, поточні стандарти використовують автономне рішення для керування ключами, яке неможливе для оновлення та відкликання ключів. GSM-R є розширенням GSM, який надає додаткові послуги, необхідні для залізничних операцій. Оскільки стандартизовані номери використовуються для адресації бортових функцій, коли зловмисник отримав доступ до мережі GSM-R, це може призвести до збою. Крім того, [152] аналізує безпеку системи GSM, дійшовши висновку, що дизайн безпеки GSM є слабким, оскільки він використовує деякі криптографічні алгоритми, які походять із підходу безпеки через невідомість. Знову ж таки, цю слабкість можна використати, використовуючи людину в центрі атаки. Крім того, атака на мережу GSM-R може вивести з ладу систему ERTMS/ETCS на великій території, створивши широкомасштабну DOS-атаку [58]. Нарешті, як і інші системи бездротового зв’язку, GSM-R також чутливий до радіоперешкод від зовнішніх джерел. У [51] Baldini та ін. обговорити той факт, що перешкоди можуть потенційно вплинути на всю залізничну інфраструктуру, оскільки рух кожного поїзда корелюється з позиціями інших поїздів у мережі, викликаючи потенційні збої в роботі.

Крім того, залізнична інфраструктура наразі значно піддається ризику тероризму, зокрема кібертероризму. Фактично, ключова частина системи залізничного транспорту є привабливою мішенню для терористичних атак [63]. Терористичні атаки та злочинні атаки обговорюються в [63], [171]: прикладами атак є залізничні колії та стрілочні переводи (вразливі до атак через відкручування стрижнів або неправильне розташування стрілочних переводів), мости (вразливі до атаки вибухівкою), тунелі (вразливі до атак вибуховими речовинами та хіміко-біологічними агентами), системи управління та диспетчеризації (вразливі до вибухівки та кібератак). Приклад аналізу безпеки у відкритій системі наведено в розділі нижче.

5.3.3 Типи атак і використовувані вразливості (анатомія атаки) та економічні наслідки

У цьому розділі обговорюються типи атак і вразливості, які можна використовувати, які впливають на залізничну інфраструктуру, на двох різних прикладах: безпека в закритих/відкритих системах і атаки на залізницю/метро. Зокрема, як обговорюється нижче, безпека закритої системи може впливати лише на доступність послуг (наприклад, зупинки поїздів), інакше у відкритій системі

безпека може стати проблемою. Наприклад, така ситуація може виникнути, коли IT-інфраструктура спільно використовується між критично важливою службою (наприклад, зв'язок між поїздом і радіоблоковим центром, RBC) і некритичною службою (наприклад, доступ до Інтернету для пасажирів).

Безпека в закритих системах: приклад

Двома основними компонентами залізничного бортового обладнання є європейський життєво важливий комп'ютер (EVC, у ETCS) та інтерфейс машиніста-машиніста (DMI).

EVC є основним ядром бортової автоматичної системи керування поїздом: він контролює рух поїзда та надсилає інформацію до DMI. Керування поїздом здійснюється за допомогою інформації, отриманої як від євробалізів (передавачів, розташованих уздовж колій), так і від РБК через мережу GSM-Залізниця. DMI діє як міст між машиністом поїзда та EVC. Він спілкується з EVC як підлеглий; він показує, використовуючи аудіо- та відеопристрої, повідомлення та інформацію EVC водієві та передає вхідні дані від водія до EVC. Машиніст взаємодіє з DMI, використовуючи РК-екран DMI, аудіопристрої та клавіатуру (або сенсорний екран); машиніст виконує дві ключові ролі: (i) приймача інформації для інформації, створеної EVC, яка відображається DMI, і (ii) джерела команд для команд, які будуть доставлені до EVC за допомогою DMI [68].

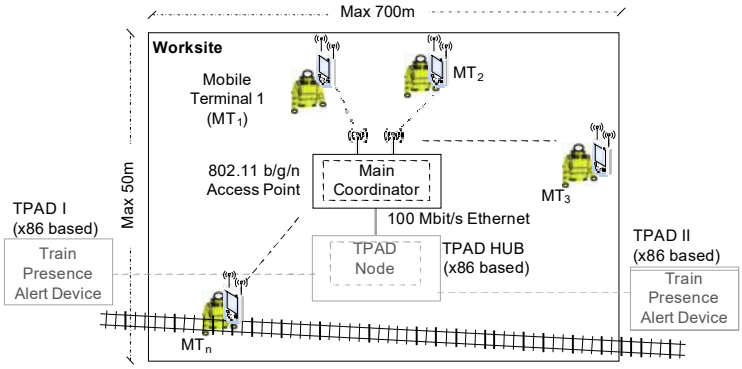
EVC є критично важливим компонентом безпеки, його безпека оцінюється відповідно до рівня безпеки 4 (SIL 4), як це передбачено відповідним стандартом CENELEC. Це означає, що допустимий коефіцієнт небезпеки за годину (THR) повинен бути між 10-9 і 10-8. Натомість DMI є компонентом SIL 0. EVC і DMI налаштовані як головний/підлеглий, де EVC є головним, а DMI виконує лише на основі наказів, надісланих EVC (аудіо- та відеоінформація). DMI надсилає дані до EVC лише за явного запиту, наприклад, через введення даних машиністом, для вибору опцій із меню, для підтвердження повідомлень. Застосований протокол

для зв'язку EVC-DMI описано в стандартах [173], [172]. Загрози безпеці в цьому випадку не вважаються проблемою, оскільки DMI-

Зв'язок EVC відповідає визначенню закритої системи, наведеному вище. EVC об'єднує інформацію від машиніста, баліз та RBC: EVC здатний гарантувати безпеку місії поїзда незалежно від поведінки машиніста та можливих неправильних вхідних даних, отриманих зіпсованим DMI. Зверніть увагу, що будь-яка неправильна поведінка машиніста, невідповідність отриманої інформації або затримка інформації призводять до того, що поїзд переходить у безпечний стан (наприклад, зупинка поїзда), що впливає на доступність.

Безпека у відкритих системах: приклад

Проект ALARP (система автоматичного попередження про колії на основі розподілених персональних мобільних терміналів [40]) передбачає проектування, розробку та перевірку автоматичної системи попередження про колії (ATWS), здатної: i) виявляти поїзди та рухомий склад, що наближаються до робоче місце, і ii) сповістити працівників про їхнє прибуття, таким чином підвищивши їх безпеку. Насправді безпека працівників на залізниці викликає серйозне занепокоєння, оскільки транспортні засоби притиснуті коліями, водії мають обмежені можливості для реагування в разі виникнення надзвичайних ситуацій. Наприклад, у період з 1993 по 2002 рр. на залізницях США було зареєстровано 460 смертельних нещасних випадків, пов'язаних із залізницею, серед залізничників і 761 смертельна травма, пов'язана з роботою на залізниці, за участю працівників не із залізничної галузі [87].



Малюнок 5.4: Огляд комунікаційної системи ALARP.

Архітектура ALARP базується на наступних компонентах (див. рис. 5.4). Один або кілька пристроїв сповіщення про присутність поїзда на колії (TPAD) розміщуються поза робочим майданчиком; TPAD визначають наближення поїздів (рухомого складу) на контрольованій колії. Працівники носять набір розподілених бездротових мобільних терміналів (MT) у режимі реального часу [67], які надають точну, безпечну інформацію в реальному часі про наближення поїздів і події, які можуть поставити під загрозу безпеку працівників (наприклад, , проблеми зі здоров'ям). TPAD і MT з'єднані через базову станцію.
Коли поїзд наближається, це виявляється TPAD, і сповіщення надсилається на MT. MT надсилає попередження працівнику, якщо він знаходиться в небезпечній зоні (так званій червоній зоні), яка розташована поблизу колії, до якої наближається поїзд, і попередження, якщо працівник знаходиться в ненебезпечній зоні (так званій зеленій зоні). зона).
Загальна архітектура зв’язку в ALARP дотримується централізованого налаштування зв’язку на основі стандарту IEEE 802.11. Це забезпечує кращу передбачуваність часу зв’язку та спрощену реалізацію синхронних каналів зв’язку на робочому місці. Це налаштування в основному базується на фіксованому координаторі, розташованому на робочому місці, з усіма MT, які спілкуються через координатора. Розгорнутий протокол надійного бездротового зв’язку з синхронізованим часом використовує координатор для впровадження свого централізованого алгоритму зв’язку та підтримки розподілу необхідних ресурсів зв’язку. Комунікаційні лінії між TPAD і робочим місцем можна покращити за допомогою допоміжної інфраструктури у формі додаткових вузлів ретрансляції (або повторювачів) на шляху передачі. На робочому місці інформація TPAD поширюється до MT через координатора [122].

Висока надійність, своєчасність і безпека, незважаючи на можливі суворі умови, є обов’язковими вимогами зв’язку ALARP, оскільки сигнали тривоги, викликані TPAD, є критично важливими для безпеки повідомленнями, які мають бути вчасно доставлені всім працівникам. З міркувань безпеки необхідно виявити порушення часових рамок, а працівникам подати сигнал про перехід у зелену зону; ця операційна процедура забезпечує безпеку, але впливає на робочий час, що призводить до втрати продуктивності [122].

Аналіз безпеки системи ALARP та її протоколу передачі було виконано в [66], спочатку використовуючи метод ADVISE, представлений у [115] для моделювання поведінки зловмисника, а потім поєднавши його з мережею стохастичної активності (SAN) [161] модель поведінки системи.

Для кількісної оцінки впливу зовнішніх атак було проаналізовано основні вразливості системи, приділяючи особливу увагу вразливостям комунікаційної архітектури: зокрема спостерігалися уразливості стандарту IEEE 802.11. Результати, наведені в [66], показують, що зовнішні атаки не впливають на ймовірність виникнення катастрофічного збою (потенційної шкоди працівникам), тобто вони не знижують безпеку ALARP. Але для захисту від атак кібербезпеки MT переходить у безпечний стан і попереджає працівника про перехід у зелену зону (безпечне положення). Як уже згадувалося, цей механізм сильно впливає на робочий час.

Слід зазначити, що це кількісне дослідження безпеки не вимагається стандартами сертифікації залізниць, але все ж воно вважається актуальним у контексті відкритої критичної інфраструктури з використанням компонентів COTS, де безліч загроз може призвести до серйозних загроз безпеці або доступність падає.

Напад на залізницю чи станцію метро: приклад

Як приклад програми розглянемо залізничну станцію або станцію метро. Загрози для інфраструктури, які слід враховувати, включають пошкодження майна та вандалізм, крадіжки та агресію щодо персоналу та пасажирів, мікрозлочинність, фальсифікацію та примусове переривання обслуговування (саботаж), бомбардування або поширення ядерного, бактеріологічного, хімічного або радіологічного (NBCR) зараження. - натори (тероризм). Аналітична систематика цих загроз виглядала б так:

- Вандалізм
- Крадіжки ПК
- Бомбардування
- Хакерство
- Газові атаки
- Пошкодження інфраструктури

Кожна з цих загроз може бути пов'язана з кількісними параметрами:

- частота P виникнення загрози [події/рік];
- вразливість V системи щодо загрози, тобто ймовірність того, що загроза спричинить очікувані наслідки (збитки) за умови, що загроза виникла;
- очікуваний збиток D, що виникає після успішної атаки в євро. Наприклад, очікуваний збиток, що стосується однієї атаки, може бути обчислений шляхом прогнозування витрат, необхідних для відновлення активів, і можливих наслідків переривання обслуговування.

Передбачається, що значення отримані шляхом аналізу історичних даних про успішні та невдалі атаки до та після вжиття конкретних заходів протидії; такі дані зазвичай доступні для порівнянних установок. З іншого боку, необхідно класифікувати наявні механізми захисту, наприклад, огороджувальні сигналізації, об’ємні детектори, відеоспостереження (внутрішнє), хімічні детектори, виявлення вторгнень, системні детектори вибухових речовин. Кожен із цих механізмів захисту має

бути пов'язаний із кількома кількісними параметрами:

- перелік категорій загроз, щодо яких ефективний механізм;
- очікувана ефективність захисту, стримування та раціоналізації, тобто відсоток зниження ризику, який забезпечує механізм;
- сайт, тобто географічна прив'язка, до якої застосовується механізм;
- розрахункове покриття, наприклад, відсоток фізичної площі або периметра ділянки;
- річні витрати (придбання, управління, обслуговування тощо).

Ці параметри враховують переваги, які приносять механізми захисту, а також витрати, які вони несуть. Однією з можливих цілей кількісного аналізу ризиків і процесу управління ризиками може бути визначення оптимальних варіантів дизайну, пов'язаних із безпекою, що дозволяє знизити рівень ризику нижче необхідного порогового значення за заданих обмежень щодо витрат.

5.3.4 Стратегії захисту

Незважаючи на те, що було докладено багато зусиль для підвищення безпеки та сумісності європейської залізничної системи (наприклад, стандарт ERTMS/ETCS), наявні на даний момент системи використовують широкий набір технологій, які, принаймні для деяких із них, слід оновити. Крім того, наявний стандарт визначає інтерфейси між компонентами без додаткових вимог до їх реалізації, якими зазвичай керують на національному рівні. Цей підхід може спрацювати для сумісності, але цього недостатньо, щоб гарантувати безпеку критичної інфраструктури. Хоча заміна або модернізація технологій не є дуже складним завданням, виявлення та розгортання спільних стратегій (наприклад, серед європейських країн) для захисту залізничної системи є досить складним. Тому, враховуючи європейську залізничну систему, необхідним є загальний і цілісний підхід до забезпечення безпеки. Застосування спільних підходів до аналізу ризиків допомагає визначити критичні аспекти та загрози сучасної та сумісної залізничної системи та керувати ними.

У наступних розділах представлені методи аналізу ризиків і набір технічних рішень і оновлень, корисних для залізничної системи.

Аналіз ризиків

Аналіз ризиків є центральною діяльністю у забезпеченні безпеки критичної залізничної транспортної інфраструктури та систем громадського транспорту. Аналіз ризику можна виконати з використанням якісних підходів, заснованих на експертному судженні та обмежених діапазонах атрибутів ризику [177]. Проте кількісні підходи на основі моделі [95] можуть знадобитися для точного визначення індексів ризику з урахуванням частоти виникнення загроз (наприклад, враховуючи історичні дані) та наслідків (пошкодження активів, переривання обслуговування, травмування людей). тощо). Кількісні підходи спричиняють кілька проблем, таких як доступність вихідних даних і методологія аналізу, яка є непростою. У літературі доступні кілька підходів до аналізу ризиків критичної інфраструктури [48, 60, 97, 117, 132, 137], хоча в більшості випадків вони або якісні, надмірно абстрактні та загальні, або пристосовані до застосувань, відмінних від залізничні перевезення. Оцінка ризику – це процес вимірювання очікуваного ризику як комбінації ймовірності виникнення загрози, вразливості системи та очікуваного збитку. Кожен із цих аспектів можна оцінити кількісно шляхом прийняття відповідних підходів, можливо, заснованих на добре

встановлених методах, запозичених із області надійності. Для цього необхідна відповідна модель частоти загроз (наприклад, на основі BN), яка кількісно визначає частоту виникнення загрози, виміряну в подіях/рік; модель уразливості загрози (наприклад, на основі SPN), що дозволяє кількісно визначити вразливість системи щодо кожної загрози, тобто ймовірність того, що загроза спричинить очікувані наслідки або збитки, якщо загроза виникла; модель наслідків загрози (наприклад, на основі дерев подій), яка оцінює в євро вплив очікуваної шкоди, що виникає після успішної атаки.

На жаль, вищезазначені параметри, задіяні в оцінці ризику, отримати нелегко. Аналіз потребує як процедурних аспектів, так і аспектів моделювання. Процедурні аспекти включають сеанси мозкового штурму, опитування сайтів, огляд дизайну, аналіз статистичних даних, експертне судження тощо. Формальні мови моделювання, які можна використовувати для аналітичного обчислення частоти загроз, уразливості та наслідків, включають дерева атак, байєсовські мережі, стохастичні мережі Петрі та, можливо, інші. формалізми, здатні врахувати невизначеність, невід'ємно пов'язану з ризиком, а також можливість стратегічних атак [141]. Насправді ці три параметри мають взаємозалежність, яку також слід моделювати. Управління ризиком (або пом'якшення) натомість використовується для позначення процесу вибору контрзаходів і прогнозування їх впливу на зниження ризику. Механізми захисту можуть зменшити ризик, оскільки вони мають три основні ефекти:

- захисні, спрямовані на зниження рівня вразливості;
- • тримуючий, спрямований на зниження частоти виникнення даної загрози;
- раціоналізаторська, спрямована на зменшення очікуваного збитку.

Кожен механізм певним чином впливає на одну або декілька загроз. Знову ж таки, необхідно кількісно визначити цей вплив, оцінюючи як частку активів або ресурсів у системі, яка фактично захищена механізмом, так і кількісне зниження ризику, яке він забезпечує. Крім того, для оцінки фактичної рентабельності слід враховувати вартість встановлення/експлуатації, пов'язану з кожним механізмом. Отже, у сценарії реального світу можуть знадобитися відповідні підходи для проведення аналітичних оцінок компромісів між витратами та вигодами та визначення точного вибору дизайну, пов'язаного з безпекою..

Технічні рішення

Пов'язані роботи [58, 51] обговорюють набір стратегій технічного захисту, які можуть зменшити загрози, що впливають на бездротовий зв'язок ERTMS.

Перш за все, протокол Euroradio побудований на основі GSM-R (розширення GSM), який має певні проблеми з безпекою, про що йдеться в [152, 58]. Доступні принаймні два рішення: оновити GSM і GSM-R або перейти на іншу бездротову технологію; мабуть, найпростішим рішенням є перше. Оскільки Єврорадіо не гарантує конфіденційності повідомлень [58], у разі зламу мережі GSM-R зловмисник міг би підслухати повідомлення ERTMS. Таким чином, навіть якщо GSM і GSM-R були оновлені, ця проблема залишається.

Як обговорювалося раніше, інтерфейси машиніста та поїзда в минулому вважалися довіреними, однак у поточних специфікаціях не потрібна автентифікація на каналах зв'язку, які використовуються для цих інтерфейсів [58]. Тому, розглядаючи сценарій, коли система ETCS була підключена до мережі, яка передає некритичні повідомлення (наприклад, підключення до Інтернету для пасажирів), рекомендована автентифікація. Balises, як і інтерфейси машиніста та поїзда, також не підтримують

автентифікацію. Ця ситуація відкриває можливість зловмисних атак через інтерфейс балізи, оскільки дані, отримані від балізи, ефективно довіряються системі [58]. Таким чином, також для баліз рекомендована автентифікація.

Бальдіні та ін. [51] обговорює проблему перешкод, яка впливає на GSM і GSM-R, викликаючи DoS-атаки на систему. Їх робота описує систему бездротового моніторингу для виявлення джерел перешкод і застосування відповідних заходів протидії. Надані ними результати підтверджуються серією експериментів, проведених на деяких італійських залізничних станціях.

5.3.5 Підходи до зменшення несправностей

У сфері залізниці компоненти, які розгортаються в інфраструктурі, повинні бути сертифіковані відповідно до суворих стандартів безпеки, щоб отримати дозвіл на роботу. Такі стандарти також містять вказівки щодо типів несправностей, які слід брати до уваги з метою сертифікації системи, а також надають загальні вказівки для того, щоб гарантувати, що система демонструє безпечну поведінку, незважаючи на виникнення несправностей.

Зокрема, концепція безвідмовності широко використовувалася з перших днів залізничних систем [70]. Ця концепція заснована на використанні компонентів, які мають чітко встановлені режими відмови, і на досягненні безпечного стану в разі відмови однієї з його частин. Для систем високої цілісності в залізничній інфраструктурі (тобто систем SIL3 і SIL4) стандарт CENELEC EN 50129 [69] передбачає застосування цього принципу для пом'якшення будь-якої окремої випадкової апаратної несправності, яка розпізнається як можлива. Згідно зі стандартом CENELEC EN 50129, принцип безвідмовності може бути досягнутий різними способами:

- *Композитна відмовостійкість* гарантує, що кожна пов'язана з безпекою функція виконується принаймні двома елементами. Кожен із цих елементів незалежний від інших, і необхідна кількість елементів узгоджується для прогресу.

- *Реактивний захист* від збоїв забезпечує безпечну роботу шляхом належного виявлення та усунення небезпечних несправностей, які виникають в одному елементі, який реалізує функцію. Виявлення розглядається як другий елемент, який має бути незалежним, щоб уникнути збоїв із загальної причини.

- *Внутрішня відмовостійкість* розглядається, якщо всі незначні види відмов одного елемента не є небезпечними.

Нижче наведено деякі підходи до відмовостійкості, які зазвичай застосовуються в обробних одиницях залізничної інфраструктури під час реалізації вищезазначених принципів.

- *Одноканальний з програмним самотестуванням*. В одноканальній архітектурі існує лише один потік обчислень на одній частині обладнання. Виявлення помилок виконується лише додатковими програмними функціями, які виконують самотестування. Якщо помилка виявлена, система примусово переходить у безпечний стан. Зауважте, що дуже важко довести, що несправний апаратний блок (мікропроцесор) може автоматично виявити сам по собі збій, виявити його, а потім забезпечити безпечний стан (наприклад, вимкнення). Одноканальні системи часто використовуються разом із резервним пристроєм, який бере на себе обчислення, коли в основному каналі виявлено збій.

- *Закодована обробка*. У цьому методі використовується одноканальна архітектура зі спеціальними кодами виявлення помилок. Усі змінні програми складаються з частини значення та

частини керування. Інструкції програми обробляють обидві частини змінних. І входи, і виходи знаходяться в цій закодованій формі. Наприклад, щоб охопити несправності, пов'язані з процесором, контрольна частина може складатися з таких кодів: (1) арифметичний код для виявлення обчислювальних помилок, (2) статична сигнатура для виявлення помилок адресації (помилка операнда, помилка оператора, змінна плутанина), (3) сигнатура синхронізації для виявлення помилок синхронізації (неправильна кількість циклів тощо), (4) сигнатура послідовності для виявлення певних помилок секвенування та розгалуження. У відмовостійкому контролері остаточна сигнатура порівнюється з попередньо обчисленою, і безпечний стан виконується, якщо вони відрізняються.

- *Багатоканальні архітектури*. Ці архітектури включають незалежні канали обробки (потоки обчислень) із засобами для перехресної перевірки між каналами для виявлення розбіжностей і прихованих помилок. Зазвичай фізична незалежність між каналами використовується для формування областей локалізації фізичних несправностей, тоді як розмаїття проектів використовується для досягнення областей локалізації дефектів конструкції в каналах. Вхідні дані копіюються в кожен канал або доступ до них здійснюється незалежно (і синхронізується перед обробкою). Два канали можна використовувати для забезпечення безпеки (використовуючи міжканальне порівняння та перемикання в безпечний стан) або покращеної надійності (на основі внутрішньоканальної самоперевірки та перемикання після відмови між каналами). Збільшення кількості каналів може бути мотивовано необхідністю терпіти складніші розломи (наприклад, у випадку візантійських розломів потрібно щонайменше чотири канали) або необхідністю вижити в заданому часі місії з високою ймовірністю. У загальній конфігурації один канал відповідає за вихід, який контролюється іншими каналами, і кожному каналу дозволено вирішувати, чи є вихід несправним (типова настройка - два з двох) . Звичайний механізм захисту від збоїв полягає у встановленні виходів каналів у заздалегідь визначений безпечний стан у разі збою. Якщо безпечного стану немає або потрібно підвищити надійність, можна використати голосування за більшістю, визначивши мінімальну кількість каналів, які мають узгодити (найпоширенішим варіантом є два з трьох).

- *Двоканальна архітектура з різноманітною сумкою безпеки*. Усі дії обробляються на двоканальній основі з різноманітним програмним забезпеченням. Два канали - це логічний канал і канал безпеки (мішок безпеки). Вхідні дані в логічному каналі перевіряються на робочі та безпечні умови, і обчислення починається лише в тому випадку, якщо результат є позитивним. Перед виведенням він ще раз перевіряється каналом безпеки, чи результат призведе до небезпечних умов експлуатації. Якщо проблем немає, обидва канали забезпечуватимуть вихід. Окреме порівняння виконується перед використанням виходів. Різноманітність між каналами забезпечується різними специфікаціями, різними мовами (наприклад, процедурними та на основі правил). Якщо будь-яке з порівнянь виявляє розбіжності, система переходить у безпечний стан.

- *Взаємне порівняння за допомогою програмного забезпечення*. Використовуються два резервних блоки обробки програмного забезпечення (потенційно на одному апаратному забезпеченні), які взаємно обмінюються даними (проміжними результатами, тестовими даними тощо), а порівняння даних здійснюється програмним забезпеченням для виявлення розбіжностей і переведення системи в безпечний стан . Це виконується в обох каналах незалежно (подвійне голосування), щоб забезпечити безпечне порівняння.

Важливо також увімкнути прогнозування несправностей на ранніх стадіях розробки комп'ютерної системи управління. Модель, яка використовується для представлення системи, повинна

забезпечувати багато, часто суперечливих вимог, тобто вона повинна забезпечувати реалістичний і детальний опис системи, має бути придатним для обслуговування, відносно простим у застосуванні та ефективним для обробки за допомогою відповідних інструментів аналізу. Декілька прикладів моделей, які використовуються для представлення системи з урахуванням вимог RAMSS, включають байєсовські мережі (BN), дерева несправностей (FT), ремонтні дерева несправностей (RFT), мережі Петрі (PN) і узагальнені стохастичні мережі Петрі (GSPN). . Класичні приклади ситуацій, коли вимоги RAMSS до системи управління залізницею можуть бути змодельовані за допомогою одного або кількох із цих формальних підходів, включають використання моделей надійності для бортових систем (наприклад, FT), моделей продуктивності для опису мереж і програмного забезпечення, (наприклад, за допомогою GSPN), моделі ремонтопридатності для колійних систем (наприклад, RFT) або комбіновані моделі (наприклад, GSPN, FT, BN) для оцінки безпеки резервованих архітектур за наявності недосконалого технічного обслуговування.

Глава

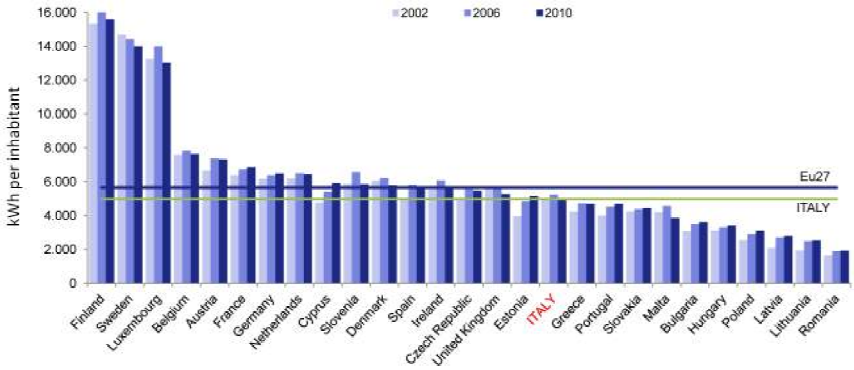
6 Зрілість італійської критичної інфраструктури

У світлі того, що було представлено в попередніх розділах, стає очевидним, що критична інфраструктура в цілому є досить важливою. Щоб краще зрозуміти, наскільки вони актуальні для Італії, цей звіт намагається відповісти на два прості запитання, які виникають майже спонтанно: і) Який ступінь зрілості італійської критичної інфраструктури? іі) Яке значення має критична інфраструктура для життя італійської нації? Відповісти на ці питання не так просто. З одного боку, важко дати повну та вичерпну відповідь через велику кількість різноманітної критичної інфраструктури, яку необхідно враховувати, і, крім того, не завжди можливо мати повний та оновлений огляд через те, що доступні дані не завжди актуальні, або тому, що дані є власністю приватних компаній, які не завжди надають їх доступні. Цей останній розділ має на меті надати відповіді, використовуючи статистичні дані, обмежені певною сферою інтересів, не вдаючись до деталей, які можна знайти в наданих посиланнях.

6.1 Актуальність КІ в суспільстві

Перш за все, ми можемо розрізняти фізичну та кібернетичну КІ. Фізична інфраструктура складається з широкого спектру систем і об'єктів, іншими словами, чогось конкретного, що легко оцінити (наприклад, енергетика, транспорт, телекомунікації, водопостачання тощо), що сьогодні доповнюється кіберчастиною. Cyber CI є більш абстрактним, нематеріальним, іноді віртуальним і зазвичай прив'язаним до IT (наприклад, фінансові послуги, електронна охорона здоров'я, електронний уряд тощо).

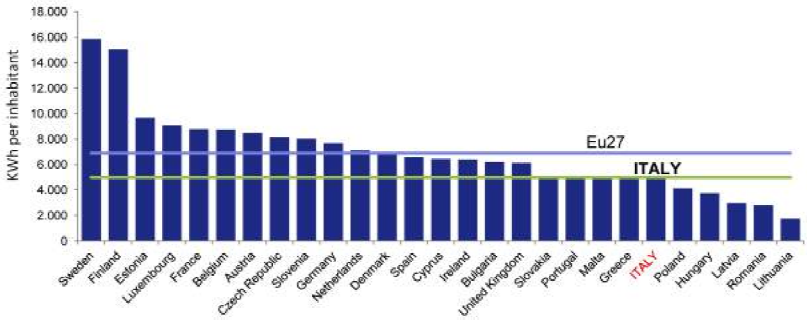
Різноманітні підмножини критичної інфраструктури надто численні, щоб усі їх можна було обговорити в цьому звіті. Таким чином, виробництво та розподіл енергії, транспорт і фінансова інфраструктура представлені як репрезентативні приклади підмножин КІ.



Малюнок 6.1: Використання енергії в країнах ЄС. Джерело: Istat [35]

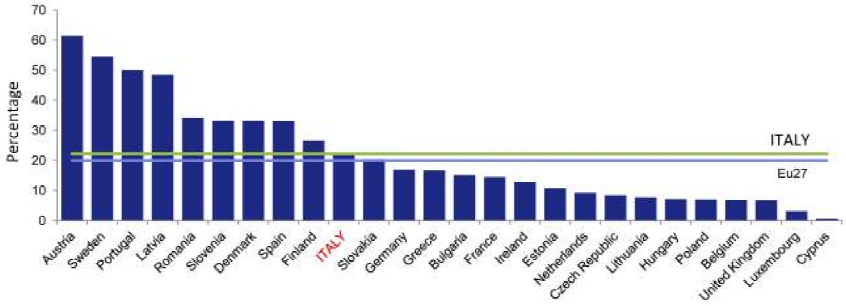
6.1.1 Енергетичний сектор

Енергетичний сектор відіграє ключову роль у сталому економічному розвитку країни як з точки зору доступності джерел, так і щодо його впливу на навколишнє середовище. У 2011 році споживання електроенергії в Італії склало 5094,1 кВт/год на душу населення, збільшившись порівняно з 2010 роком на 0,8 %. Споживання електроенергії являє собою енергію, що постачається кінцевим споживачам для всіх видів використання енергії. На рисунку 6.1 показано споживання енергії, у кВт-год на душу населення, у 2002, 2006 та 2010 роках у країнах-членах Європи, де середнє споживання у 2010 році становило 5652,4 кВт-год на душу населення. Італія має нижчу вартість, ніж інші великі європейські країни, такі як Великобританія, Іспанія, Німеччина та Франція.



Малюнок 6.2: Виробництво енергії в країнах ЄС (2010). Джерело: Istat [35]

Італія характеризується сильною залежністю від зовнішніх енергетичних ринків, тому має слабку інфраструктуру виробництва енергії. Внутрішнє виробництво електроенергії є мірою енергетичної автономності. Протягом 2011 року 86,3% загального попиту на електроенергію в Італії було задоволено за рахунок внутрішнього виробництва, а решта за рахунок балансу між імпортом та експортом. У європейському контексті з виробництвом 49,9 ГВт-год на десять тисяч осіб у 2010 році Італія є нижчою за середній показник ЄС-27, який становить 66,7 ГВт-год (див. рис. 6.2).



Малюнок 6.3: Споживання енергії з відновлюваних джерел у країнах ЄС (2010). Джерело: Istat [35]

У контексті європейської стратегії сприяння економічному зростанню розвиток відновлюваних джерел енергії є пріоритетною метою. В Італії у 2010 році відсоток кінцевого споживання енергії з відновлюваних джерел становив 22,2%. Вище середнього показника по ЄС, який становить 19,9% (див. рис. 6.3). У 2011 році цей відсоток зріс до 23,8%, збільшившись на 1,6 пункту. Ціль, яку потрібно досягти у 2020 році, становить 26%, що відображає той факт, що тенденція до інтенсифікації та експлуатації такої енергетичної інфраструктури зростає.

Дані за 2012 рік [37] показують сильний вплив на енергоспоживання, спричинений тривалою економічною кризою. Цей вплив значною мірою зосереджений на споживанні енергії промисловістю, тоді як він лише незначно вплинув на споживання побутовими споживачами. Однак більшість тенденцій, описаних вище, все ще актуальні; більш конкретно, останні дані підтверджують зростаючу важливість відновлюваних джерел енергії разом із зростанням відповідних ринків.

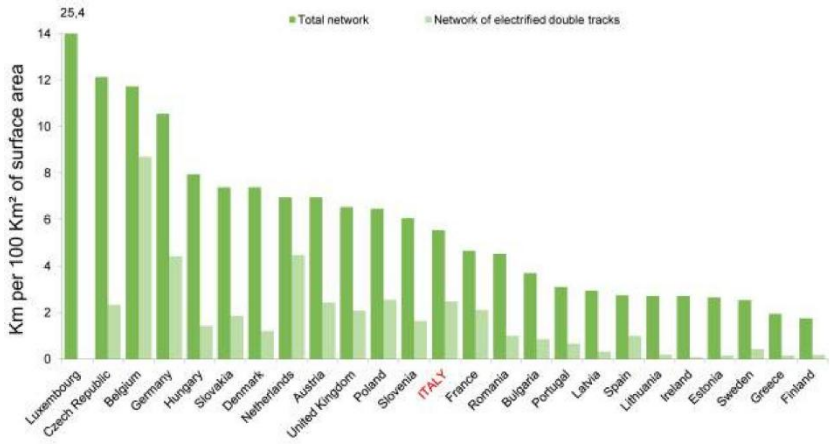
6.1.2 Транспортний сектор

Транспорт і відповідна інфраструктура відіграють ключову роль в Італії. Щоб навести деякі цифри, мережа автомагістралей Італії в 2010 році охоплювала 6668 кілометрів, що становить близько 10% європейської мережі. Це означає, що Італія має значення вище середньоєвропейського.

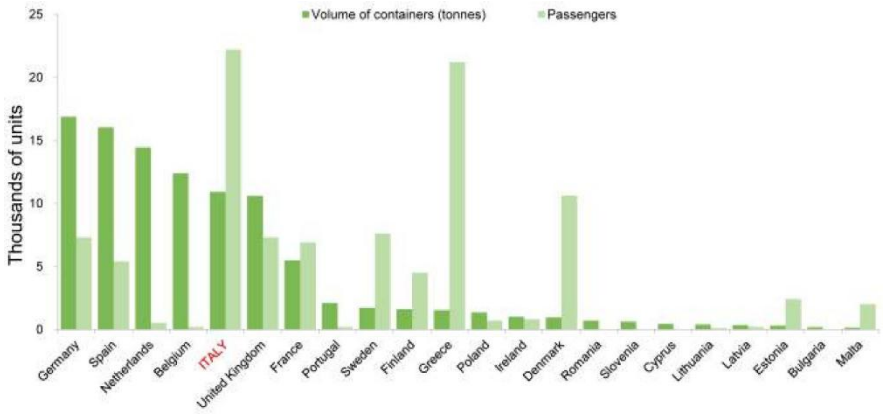
Залізнична мережа нараховує в середньому 5,5 км рейок на кожні 100 км2

площі поверхні (дані 2010 р.). Порівняно із середнім значенням ЄС (4,9 км), Італія посідає п’яте місце за шкалою ЄС за кількістю кілометрів електрифікованої двоколійної мережі. На рисунку 6.4 наведено дані про загальну залізницю та електрифіковану двоколійну мережу в країнах-членах ЄС у 2010 р. У червні 2012 р. високошвидкісна італійська лінія становила 1434 км колії, з яких 92 перебували на стадії будівництва [14].].

Що стосується морського транспорту, то портова інфраструктура набуває все більшого значення в контексті нової європейської політики щодо перевезення вантажів і пасажирів. На рисунку 6.5 наведено дані за 2010 рік щодо обсягу перевезених контейнерів і пасажирів, які прибувають у порти ЄС та відходять з них. З малюнка видно, що Італія посідає п’яте місце за обсягом контейнерних перевезень і перше – за пасажироперевезеннями (понад 87,6 млн пасажирів).



Малюнок 6.4: Залізнична мережа в країнах ЄС (2010 р.). Джерело: Istat [35]



Малюнок 6.5: Обсяг оброблених контейнерів і пасажиропотік у портах ЄС (2010). Джерело: Istat [35]

Повітряний транспорт [35] [30] використовується все більшими і більшими верствами населення для пересування на середні та великі відстані завдяки наявності дешевих тарифів. Порівняно з іншими видами транспорту повітряний транспорт має вищий рівень динамізму, але він обмежений тим, що його інфраструктура близька до рівня насичення. На рисунку 6.6 показано зростання у відсотках загального пасажирського повітряного транспорту країн-членів ЄС за 2011 та 2012 роки, причому Італія трохи нижча за середній показник. На рисунку 6.7 показано пасажиропотік на одного мешканця у 2011 році, причому Італія була значно нижчою за середній показник ЄС. Італійський трафік зосереджений у Римі з 37,4 мільйонами пасажирів і 25,3% італійського трафіку, а також у двох аеропортах Мілана: аеропорту Мальпенса з 19,1 мільйонами пасажирів і 12,9% італійського трафіку та аеропорту Лінате з 9,1 мільйонами пасажирів і 6,1% італійського трафіку.

це речення та оригінал дають зрозуміти, що в Римі є лише один аеропорт ....

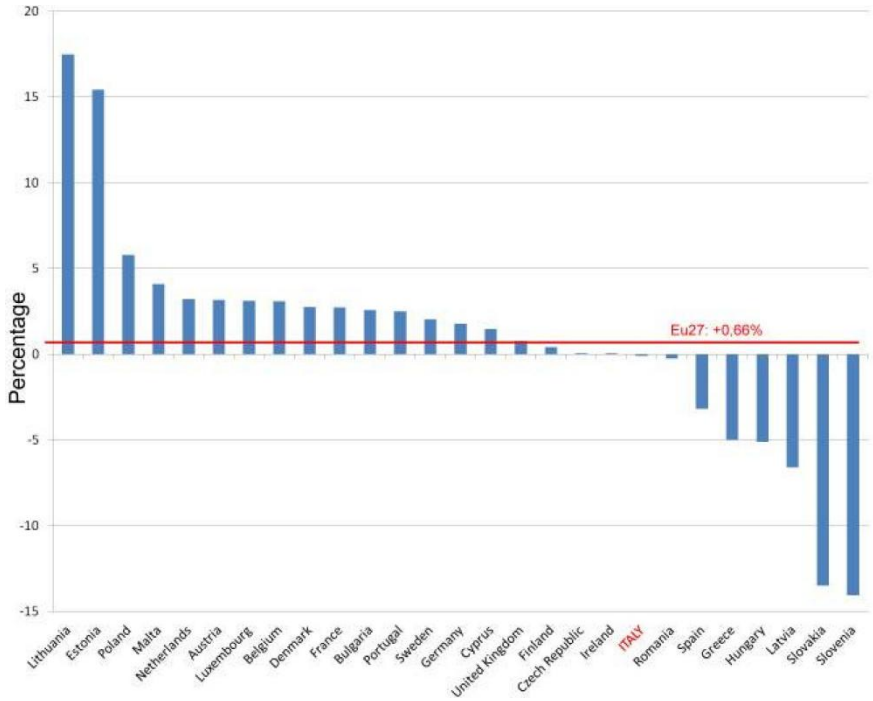
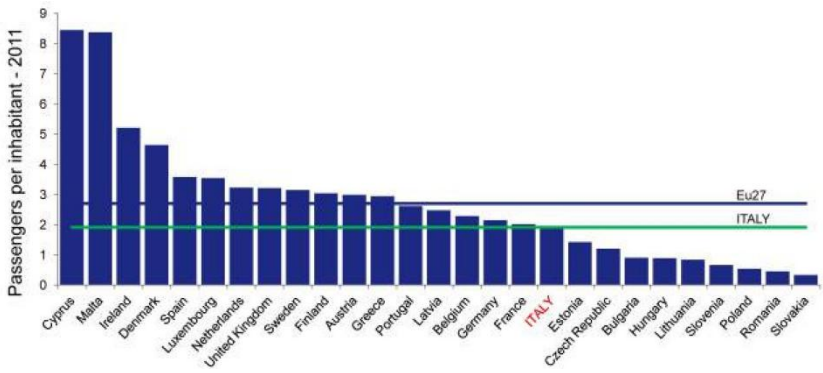


Рисунок 6.6: 2011/2012 рр. Зростання загального пасажирського повітряного транспорту країн-членів ЄС (у %). Джерело: Євростат [1]

6.1.3 Фінансовий сектор

Щоб оцінити важливість фінансової системи в Італії, необхідно спочатку розглянути деякі показники, які зазвичай використовуються для цієї мети: коефіцієнт фінансового взаємозв'язку, коефіцієнт фінансового посередництва, коефіцієнт кредитного посередництва, чистий коефіцієнт фінансового взаємозв'язку. Ці цифри порівнюються з даними інших країн ЄС, щоб краще зрозуміти рівень фінансового посередництва, досягнутого в Італії. Рівень фінансового посередництва економічної системи був глибоко проаналізований Голдсмітом з 1950-х років [101]. Зокрема, за допомогою коефіцієнта фінансового взаємозв'язку (FIR), заданого співвідношенням ваги фінансових активів до багатства всіх секторів, Голдсміт розробив міру ступеня фінансової інтенсивності економічної системи. Чим він вищий, тим ширше фінансове поглиблення економічної системи. Як показано на рисунку 6.8, є деякі докази постійного розвитку фінансової інтенсивності в італійській економіці, навіть якщо порівняно з іншими подібними банківськими системами, такими як Німеччина, Франція та Іспанія, Італія має нижчий відсоток; Велика Британія історично вважається країною з ринково орієнтованою фінансовою системою, і коефіцієнт FIR, здається, підтверджує цю точку зору.



Малюнок 6.7: Загальна кількість пасажирів на одного мешканця повітряного транспорту європейських держав-членів (2011) (2011) [35]

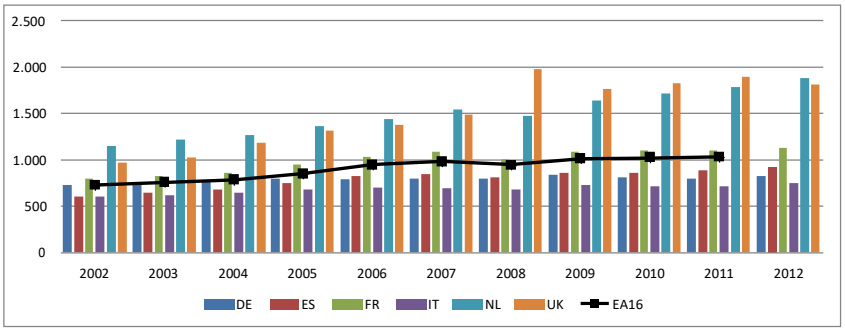
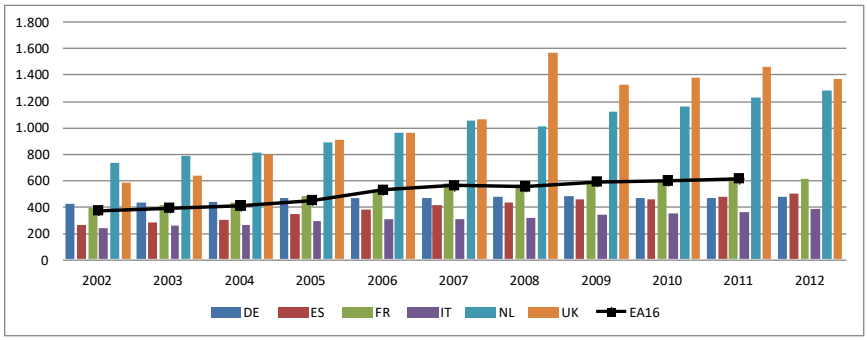


Рисунок 6.8: Коефіцієнт фінансового взаємозв'язку: активи загальної економіки у відсотках від ВВП. Джерело: Євростат (неконсолідовані дані).

На малюнку 6.9 показано співвідношення між загальними активами фінансових установ і ВВП, що свідчить про актуальність, яку припускають ці установи в різних розглянутих країнах. Італія знову відстає від інших країн.

Інший коефіцієнт Голдсміта, коефіцієнт фінансового посередництва (FIR), аналізує ефективну вагу зобов'язань фінансових корпорацій. Порівнюючи (див. мал. 6.10) значення, прийняті FIR в інших країнах ЄС, стає очевидним зростаюче значення посередництва в італійській економічній системі. Дійсно, він досягає рівня інших порівнянних країн.



Малюнок 6.9: Активи фінансових установ у відсотках від ВВП. Джерело: Євростат (неконсолідовані дані).

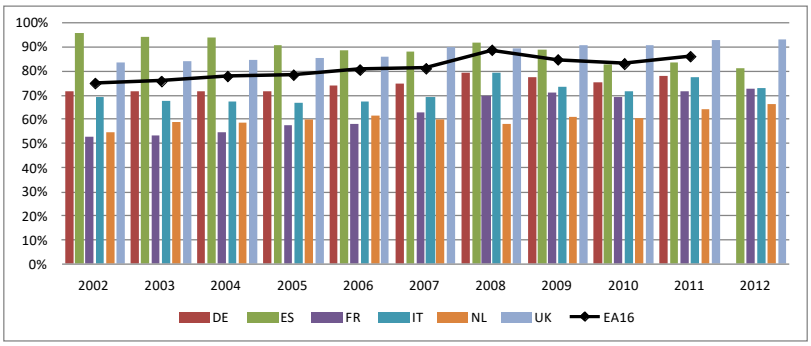
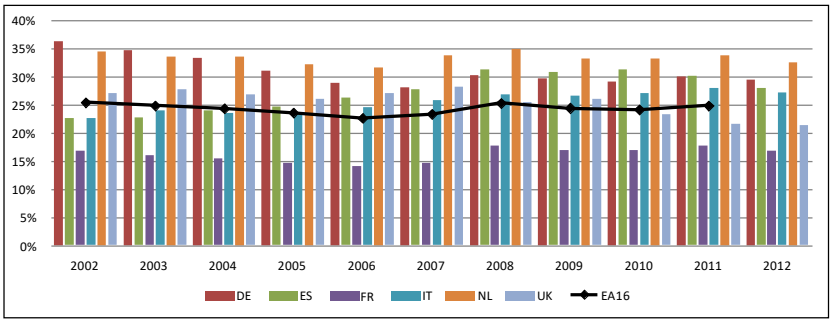


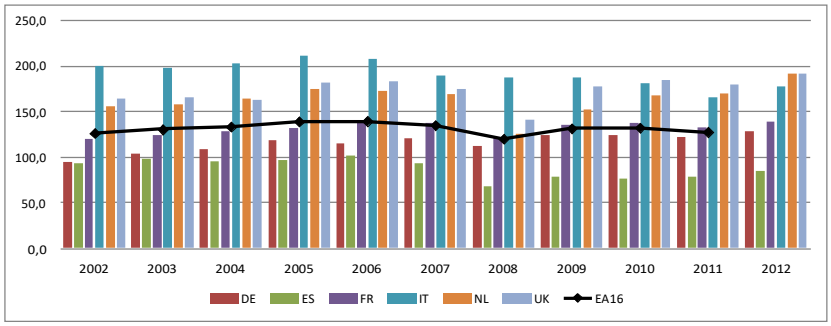
Рисунок 6.10: Коефіцієнт фінансового посередництва в окремих країнах ЄС. Джерело: Євростат (неконсолідовані дані)

Розглядаючи коефіцієнт кредитного посередництва, малюнок 6.11, роль, яку беруть на себе фінансові посередники в економічній системі, зосереджена на співвідношенні, яке представляє вагу позик, наданих фінансовими корпораціями, проти зобов'язань, виданих усіма іншими секторами [96]. Ми зазначаємо, що роль фінансових посередників в Італії співпадає з іншими країнами, розглянутими в аналізі.

Крім того, на рисунку 6.12 розглядається коефіцієнт чистого фінансового взаємозв'язку, щоб оцінити фінансове поглиблення в Італії порівняно з іншими країнами ЄС. Співвідношення, розраховане як чисте фінансове багатство приватного сектора (нефінансових корпорацій1 та домогосподарств2) до ВВП, підтверджує хороші показники Італії в період, що розглядається, навіть якщо спостерігається послідовне зниження рівня фінансового добробуту. порівняно з ВВП через фінансову кризу та економічний спад.



Малюнок 6.11: Коефіцієнт кредитного посередництва в окремих країнах ЄС. Джерело: Євростат (неконсолідовані дані).



Малюнок 6.12: Коефіцієнт чистого фінансового взаємозв'язку окремих країн ЄС (%). Джерело: Євростат (неконсолідовані дані).

На малюнку 6.13 представлено кількість і типологію фінансових посередників, які працюють в Італії за останні два роки.

[1]Сектор нефінансових корпорацій включає всі приватні та державні корпоративні підприємства, які виробляють товари або надають нефінансові послуги для ринку. Відповідно, державний сектор виключає такі державні підприємства та включає центральні, державні (регіональні) та місцеві урядові фонди та фонди соціального страхування. Сектор фінансових корпорацій включає всі приватні та державні установи, що займаються фінансовим посередництвом, такі як грошово-фінансові установи (загалом еквівалентні банкам), інвестиційні фонди, страхові корпорації та пенсійні фонди.

[2]Сектор домогосподарств включає всі домогосподарства та включає домогосподарства. Вони охоплюють одноосібні підприємства та більшість товариств, які не мають незалежного юридичного статусу. Таким чином, сектор домогосподарств, крім споживання, також генерує виробництво та підприємницький дохід. У європейських рахунках некомерційні установи, що обслуговують домогосподарства (NPISH), такі як благодійні організації та профспілки, групуються з домогосподарствами. Їхня економічна вага відносно обмежена.

	Кількість посередників	
	2011	**2012**
Банківські групи	77	75
Групи інвестиційних підприємств	20	19
Банки	740	706
банки з обмеженою відповідальністю	214	197
кооперативні банки (banche popolari)	37	37
спільні банки (banche di credito cooperativo)	411	394
філії іноземних банків	78	78
Інвестиційні підприємства	102	101
Компанії з управління активами та SICAVs	190	172
Фінансові компанії, внесені до спеціального реєстру відповідно до статті 107 Зведеного закону про банківську діяльність	188	186
Фінансові компанії, внесені до загального реєстру відповідно до статті 106 Зведеного закону про банківську діяльність	782	658
Установи з електронними грошима	3	3
Платіжні установи	34	44
Інші контрольовані посередники (Bancoposta and Cassa Depositi e Prestiti)	2	2
Страхові компанії		135
діяльність у сфері страхування життя		52
У секторі страхування, крім страхування життя		69
В обох секторах		14

Малюнок 6.13: Структура фінансової системи Італії (2011-2012 рр.). Джерело: Banca d'Italia.

Очевидно, що банківська система відіграє помітну роль у фінансовій системі Італії: на кінець 2012 року було 706 банків із загальними активами близько 220% ВВП, з яких 169 входили до 75 банківських груп і становили майже 85% загальних активів фінансового сектора. Сектор став дещо більш концентрованим за останнє десятиліття (п'ять найбільших груп володіють 49,4% активів банків і фінансових компаній, що працюють в Італії), після масштабної банківської реструктуризації на початку 90-х років, яка включала відчуження державних холдингів. Тим не менш, все ще існує багато невеликих кооперативних і місцевих банків, що працюють в різних регіональних економічних умовах. Частково через це система має вищу щільність філій (1806 мешканців на філію), ніж європейські аналоги (у середньому 2168 жителів на філію). Іншою важливою складовою фінансової системи є страхова галузь. На кінець 2012 року в Італії налічувалося 135 страхових компаній (52 працювали виключно у сфері страхування життя, 69 у страхуванні, крім страхування життя, і 14 в обох секторах). Ступінь концентрації страхової галузі є високим за європейськими стандартами, зокрема, у секторі страхування. Банки відіграють важливу роль у структурах власності італійських страхових компаній, хоча й не таку велику, як в інших секторах управління активами (інвестиційні фонди та індивідуально керовані портфелі)3. Банківський сектор також відіграє значну роль у

розповсюдженні стандартизованих страхових продуктів. За останні п'ятнадцять років страховий сектор відіграв помітну роль у галузі управління активами в Італії: технічні резерви з 1998 року зросли в чотири рази, досягнувши e486 млрд, а їхні активи під управлінням зросли з 17 до 35%.

[3]ЗУ 2012 році активи страхових компаній, підконтрольних вітчизняним банківсько-фінансовим групам, становили 19% від загального обсягу.

	Проблеми мережі			Акції			as a % of GDP
	2010	**2011**	**2012**	**2010**	**2011**	**2012**	
Банки	-11,8	66,33	83,153	807,045	873,618	956,739	61
Інші фінансові корпорації	-36,458	-4,328	-6,132	243,398	239,125	233,022	15
Нефінансові корпорації	12,373	-100	13,576	89,874	90,018	103,615	7
Всього	**-35,885**	**61,902**	**90,597**	**1,140,317**	**1,202,761**	**1,293,376**	**83**

Малюнок 6.14: Середньострокові та довгострокові облігації італійських банків і фірм (2010-2012). Джерело: Banca d'Italia.

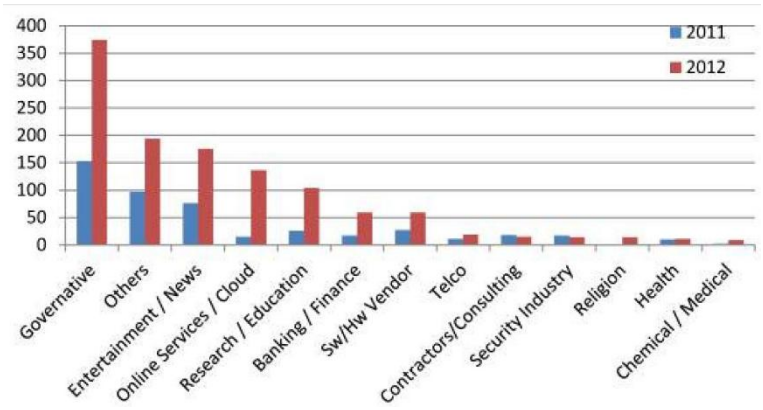
Незважаючи на це швидке зростання, страхова галузь Італії все ще менша порівняно з іншими європейськими країнами: страхові продукти складають 12% сімейного багатства в Італії (5% у 1998 році), порівняно з 33% у Франції та 18% у Німеччині. Ці відмінності в основному зумовлені структурою пропозиції: у той час як в Італії, Франції та Німеччині традиційні поліси, які пропонують підписникам мінімальний гарантований прибуток, є провідним продуктом компаній зі страхування життя, у Сполученому Королівстві основним сектором є індексний та пайовий поліси, за якими фінансовий ризик зазвичай несе застрахована сторона. Як підкреслювалося вище, банки, як правило, монополізують фінансування всієї економіки Італії; про це також свідчить те, що нефінансові корпорації рідко звертаються до ринку капіталу для фінансування своїх інвестицій як за допомогою боргового, так і акціонерного капіталу. У 2012 році італійські компанії здійснили чисті емісії на 91 мільярд євро (див. рис. 6.14), і більшість із них було здійснено банками (83 мільярди євро проти 66 мільярдів євро у 2011 році), тоді як інші фінансові установи продовжували здійснювати чисті викупи. Згідно з даними Dealogic, валові розміщення на міжнародному ринку емітентами, що належать до італійських нефінансових груп, зросли з 19 мільярдів євро до 29 мільярдів євро; майже 80% нових випусків припадало на шість великих груп (Enel, Eni, Fiat, Snam, Telecom Italia та Terna).

Кошти, залучені шляхом збільшення капіталу компаніями, зареєстрованими на біржі, дещо зменшилися порівняно з 2011 роком і склали 10,1 мільярда євро порівняно з 11,9 мільярда (рис. 6.15). Знову фінансові установи залучили більшу частину капіталу: один банк залучив приблизно три чверті загальної суми, страхові компанії – близько однієї п'ятої, а нефінансові корпорації – решту. У 2012 році відношення ринкової капіталізації італійських компаній до ВВП зросло з 21 до 23%, тоді як в інших великих розвинених країнах це співвідношення на кінець року було набагато вищим: 45% у Німеччині, 63% у Франції, 107% у Сполучених Штатах і 156% у Великобританії. Середньоденний оборот акцій на італійській фондовій біржі був значно нижчим, ніж у попередньому році.

Зміна цін	-48.7	20.7	-8.7	-24.0	10.2
Компанії, зареєстровані на біржі (кількість на кінець року)	336	332	332	328	323
з них: італ	*294*	*291*	*291*	*287*	*282*
Ринкова капіталізація італійських компаній	374,702	457,126	425,099	332,374	365,466
відсотків ВВП	*23.8*	*30.1*	*27.4*	*21.1*	*23.3*
Процентний склад:					
промислові підприємства	*33*	*37*	*41*	*45*	*47*
страхування	*11*	*9*	*7*	*7*	*8*
банківська справа	*25*	*26*	*20*	*17*	*18*
фінанси	*3*	*2*	*3*	*3*	*2*
послуги	*28*	*26*	*28*	*29*	*25*
Всього	100	100	100	100	100

Дивіденди	39,072	21,309	16,036	17,009	13,207
Співвідношення прибуток/ціна	15.6	5.3	7.6	9.0	7.2
Дивідендна дохідність	8.0	5.0	3.8	5.1	4.2

Рисунок 6.15: Основні показники італійської фондової біржі (2012 р.). Джерело: Banca d'Italia.



Малюнок 6.16. Відомі жертви кібератак в Італії. Джерело: Clusit [36].

6.2 Зрілість захисту від кібератак

Що стосується захисту КІ, то ми живемо в реальній глобальній надзвичайній ситуації, в якій ніщо і ніхто більше не може вважатися безпечним. Кожна сфера стала потенційною мішенню: громадяни, компанії, уряди. У звіті, представленому McAfee і CSIS [7] у 2011 році, підкреслюється неймовірне зростання кількості кібератак на критичну інфраструктуру, яка продовжує бути непідготовленою до боротьби з такими загрозами. Звичайний захист більше не є достатнім для блокування загроз, які стають все більш складними та виходять за межі більшості систем контролю.

На рисунку 6.16 показано відомі жертви кібератак в Італії, класифіковані за секторами компетенції. Для кожного класу показані числові дані за 2011 та 2012 роки, щоб підкреслити цю недавню тенденцію.

6.2. Maturity of protection against cyberattacks

Сектор	2011	2012	Всього	Дельта
Mil, LEAs, Intelligence	153	374	527	144%
Інше	97	194	291	100%
Розваги/Новини	76	175	251	130%
Онлайн-сервіси/Хмара	15	136	151	807%
Дослідження/Освіта	26	104	130	300%
Банківська справа/фінанси	17	59	76	247%
Постачальник програмного забезпечення/апаратного обладнання	27	59	86	119%
Телекомунікаційна компанія	11	19	30	73%
Підрядники / Консалтинг	18	15	33	-17%
Індустрія безпеки	17	14	31	-18%
Релігія	0	14	14	100%
Health	10	11	21	10%
Хімічний/Медичний сектор	2	9	11	350%
Всього	469	1183	1652	152%

Таблиця 6.1: Динаміка кількості атак за секторами. Джерело: Clusit [36].

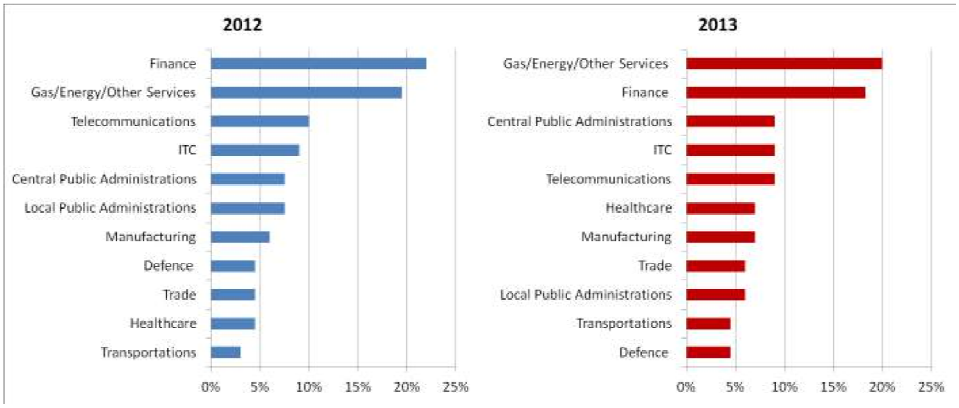
Дані показують, що лише в двох секторах кількість атак зменшилася, тоді як усі інші сектори постраждали від збільшення кількості атак, іноді навіть понад 500%. Дельти для кожної категорії детально наведено в таблиці 6.1. Ці дані корисні для розуміння того, наскільки явище інформаційної безпеки в кожній сфері, а отже, і в КІ, є дуже делікатним і потребує належного вирішення.

Усвідомлення такої потреби є очевидним, і, незважаючи на економічну кризу, можна спостерігати, що ринок безпеки ІКТ продовжує мати стабільну та позитивну тенденцію, як ознаку того, що компанії, користувачі та країни в цілому все більше і більше усвідомлюють потреби в безпеці і, отже, інвестувати в неї. Дані CLUSIT [36] забезпечують важливе порівняння, використовуючи вибірку італійських компаній, інвестицій, здійснених у 2012 році, та прогнозу інвестицій у 2013 році. Це показано на рисунку 6.17.

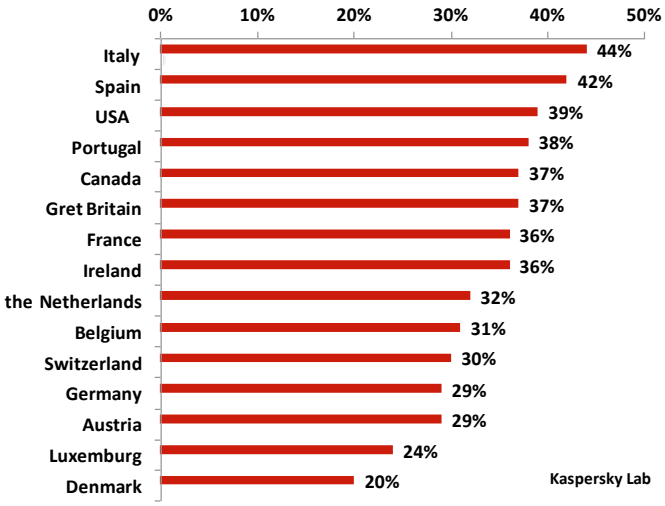
Водночас видається очевидним, що роль урядів має бути вирішальною у заохоченні безпеки шляхом співпраці з промисловістю та прийняття належних нормативних актів.

Стан поінформованості про комп'ютерну безпеку в Італії ще гірший, якщо взяти до уваги звичайних користувачів і те, наскільки вони захищені від кібератак і кібершахрайства. Незважаючи на широке поширення Інтернету серед італійців, рівень обізнаності щодо ризиків, пов'язаних з необережним використанням Інтернету, все ще низький. Як наслідок, люди купують продукти та послуги, які за своєю суттю є небезпечними, або впроваджують і налаштовують у небезпечний спосіб, без будь-якої гарантії чи захисту. Як показано на малюнку 6.18, основним наслідком [31] в Італії є те, що близько 44% ПК піддаються атакам зловмисного програмного забезпечення під час перегляду Інтернету, порівняно з 20% у Данії [110]. Основною причиною поширення атак є обмежене використання рішень захисту від загроз. Лише 33% італійських користувачів (цей відсоток зростає до 44% у

світовому масштабі) насправді використовують програмне забезпечення, здатне забезпечити необхідну безпеку їхніх даних, і лише 45% італійських користувачів використовують налаштування конфіденційності, щоб контролювати інформацію, якою вони діляться зі своїми контактами. . Крім того, 44% користувачів в Італії (приблизно 40% у світі) не використовують складні паролі або часто змінюють ключові слова. Кількість злочинних дій та рівень витонченості нападів не відповідає пропорційному зростанню уваги.



Маоюнок 6.17: Інвестиції в захист критичної інфраструктури (2012-2013). Джерело: Clusit [36].



Малюнок 6.18: Відсоток персональних комп'ютерів, атакованих зловмисним програмним забезпеченням під час перегляду Інтернету. Джерело Лабораторія Касперського, 2012.

6.3 Витрати на кіберзлочинність в Італії

Нещодавно повідомлялося про витрати, пов'язані з діяльністю кіберзлочинців [81]. Наразі в Італії немає офіційної статистики щодо вартості кіберзлочинності. Єдина доступна статистика надходить із приватного сектору. Відповідно до звіту Norton Cybercrime Report [33] (вересень 2012 р.), який аналізує вплив кіберзлочинності на споживчих користувачів, загальна чиста вартість споживчої кіберзлочинності в Італії за попередні 12 місяців становить 2,45 млрд євро, тоді як вартість на глобальному рівні становить 110 млрд доларів США (близько 85 млрд євро). У звіті оцінюється кількість жертв кіберзлочинів у 8,9 мільйона осіб, приблизно одна третина користувачів Інтернету, активних в Італії в 2012 році [36]. Це призводить до того, що середня вартість на одну людину становить 275 євро (більше, ніж світова середня вартість на одну людину, яка становить 197 доларів США). Зокрема, Norton реєструє зростаючу кількість жертв серед користувачів мобільних пристроїв і соціальних мереж, що свідчить про те, що кіберзлочинність розвивається в бік нових технологій. Дійсно, приблизно 17% дорослих в Італії стали жертвами соціальних чи мобільних кіберзлочинів у 2012 році, а близько 10% користувачів соціальних мереж хтось зламав їхні профілі.

У бізнес-контексті аналіз, проведений Ponemon Institute[107], оцінює вартість витоку даних в Італії з точки зору прямих, непрямих і альтернативних витрат, понесених організацією у відповідь на витік даних. Аналіз, проведений у 2011 році та опублікований у березні 2012 року, повідомляє про середню вартість витоку даних на один запис (тобто загальну вартість, поділену на кількість зламаних записів) і середню загальну організаційну вартість витоку даних. Як показано на малюнку 6.19, середня вартість одного запису італійських організацій становить 78 євро. Ці витрати враховують низку бізнес-витрат: виявлення (26 євро), сповіщення (3 євро), реагування за фактом (22 євро) і втрачений бізнес (27 євро). Більшість загальної вартості (41 євро) пов'язана з непрямими витратами, тоді як решта частини (37 євро) пов'язана з прямими витратами.

На малюнку 6.20 показано середні загальні організаційні витрати на втечу даних (1 384 798 євро) та витрати, що входять до неї. Обидві цифри показують, що найбільші витрати спричинені втратою бізнесу. Ці витрати в основному пов'язані з ненормальною плинністю клієнтів (більша, ніж середня, втрата клієнтів для організації) і втратою репутації. Дійсно, клієнти часто залишають організацію після витоку даних. Аналіз також показав, що основною причиною витоку даних є недбалість (39%), потім системні збої (33%) і зловмисні або злочинні атаки (28%). Однак зловмисні атаки в середньому є найдорожчими.

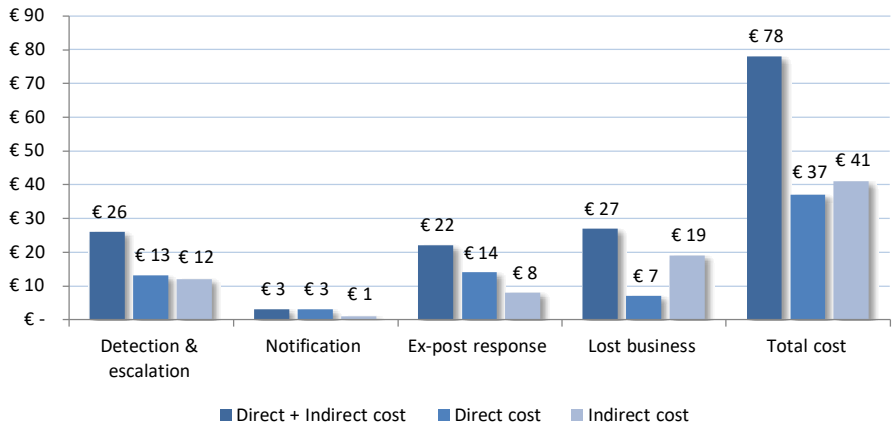
6.4 Готовність Італії до кібербезпеки

У 2013 році «Центр дослідження кіберрозвідки та інформаційної безпеки» при Римському університеті La Sapienza опублікував звіт про технічну зрілість основних акторів італійського ландшафту кібербезпеки [81]. Звіт включав дослідження, проведене шляхом інтерв'ю з кількома італійськими учасниками КІ, щоб оцінити рівень їх підготовки проти кібератак. Дослідження проводилося шляхом збору відповідей на розширену анкету, в якій досліджувалися кілька аспектів кібербезпеки, починаючи від організаційних аспектів і закінчуючи більш технічним питанням. Анкета була надіслана організаціям, які належать до групи критичної інфраструктури, зазначеної в розділі 1: ефективна кібератака на кожну з цих компаній може мати серйозні наслідки з економічної точки зору та/або з точки зору безпеки.

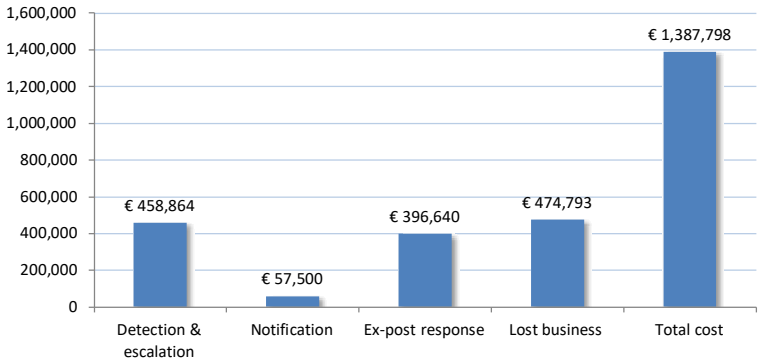
Один із найцікавіших результатів, про який повідомляється в цьому документі, представлений

індексом готовності до кібербезпеки, комплексним показником, заснованим на аналізі багатьох запитань, включених до анкети, який представили автори звіту. Він фіксує за допомогою однієї оцінки кілька взаємопов'язаних аспектів, які впливають на готовність CI проти кіберзагроз.

Індекс готовності до кібербезпеки є сукупним показником спроможності та готовності організації протистояти кіберзагрозам. Індекс охоплює чотири різні аспекти: обізнаність, захист, політика та зовнішня незалежність. Позитивною звичкою кібербезпеки для організації вважається та, яка здатна охопити найбільшу територію на радарній діаграмі з урахуванням чотирьох аспектів. Таким чином, індекс готовності до кібербезпеки відображає розмірність цієї сфери. Повна структура системи оцінок, яка обчислює індекс готовності до кібербезпеки на основі чотирьох індексів, представлена в [81].



Малюнок 6.19: Середня вартість витоку даних на один запис. Джерело: Ponemon Institute, 2011.



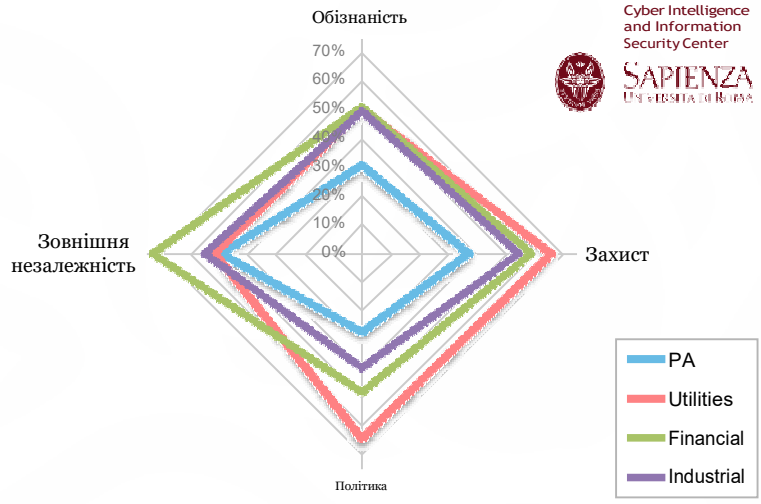
Малюнок 6.20: Середні загальні організаційні витрати на витік даних на запис. Джерело: Ponemon Institute, 2011.

Індекс обізнаності - Це оцінює ситуаційну обізнаність, пов'язану з кіберризиками організації. Наприклад, організація, яка контролює рівень безпеки, гарантований її субпідрядниками, може мати вищий індекс обізнаності. Навпаки, компанія, яка часто стикається з ненормальною поведінкою у своїй IT-інфраструктурі, яка не аналізується належним чином, помітить зниження показника обізнаності.

Індекс оборони - Це оцінює здатність організації захистити себе від кібератак. Це розглядало оцінку захисних механізмів та інструментів, які використовує організація. Анкета містила добірку добре відомих стратегій, які використовують декілька організацій для захисту своїх активів. Цей індекс перевіряє, наскільки добре організація оснащена такими інструментами та чи достатньо вона навчена їх використовувати. Зауважте, що індекс захисту дещо корелює з індексом обізнаності. Деякі відповіді, які позитивно впливають на індекс захисту, також позитивно впливають на індекс обізнаності. Ця кореляція є цілком обґрунтованою, оскільки реалізація сильних захисних механізмів передбачає хороший рівень усвідомлення.

Індекс політики - Це оцінює реалізацію політики безпеки. Високий бал у цьому індексі свідчить про дотримання кількох політик безпеки та їх постійне оновлення. Що стосується індексу захисту, існує сильна кореляція індексу політики з індексом обізнаності, оскільки прийняття оновлених політик безпеки свідчить про підвищення обізнаності.

Індекс зовнішньої незалежності - Це оцінює кореляцію між внутрішніми системами та зовнішніми постачальниками. Низький бал за цим індексом вказує на негативну кореляцію внутрішніх механізмів організації із зовнішніми постачальниками, оскільки помилка зовнішнього постачальника може вплинути на його здатність постачати основний продукт його бізнесу. Високий бал за цим індексом означає, що організація мінімально покладається на зовнішні служби, які можуть вплинути на її безпеку. Зауважте, що такі високі бали означають більші операційні витрати, оскільки організація повинна залучати послуги програмного забезпечення без залучення третіх сторін.



Малюнок 6.21: Індекс готовності до кібербезпеки: індекси поінформованості, захисту, політики та зовнішніх залежностей на групу. Джерело: СНД, 2013 [81].

Аналіз проводився шляхом поділу організацій-респондентів на чотири групи: органи державного управління (ПА), комунальні підприємства (енергетика та телекомунікації), фінансові організації (наприклад, банки), промислові компанії. Радарна діаграма зображена на рисунку 6.21, де показано результати індексу готовності до кібербезпеки для кожної групи.

Група корисностей охоплює найбільшу площу в рейтингу. Вона має кращі результати, ніж інші групи, за двома осями, а саме оборона та політика. Він також має високу оцінку поінформованості. Тим не менш, він страждає від низької зовнішньої незалежності; цю проблему поділяють усі інші групи, за винятком фінансової групи, яка все ще не бажає покладатися на зовнішніх постачальників послуг.

Фінансова група також демонструє велику охоплену територію на радарній діаграмі, демонструючи високі значення індексів зовнішньої незалежності, захисту та поінформованості. Дивно, але він не отримав очікуваного результату за індексом політики. Однак слід зазначити, що деякі питання, які вплинули на індекс політики, стосувалися конкретної політики, встановленої директивою ЄС 2008/114/ЕС щодо європейських СІ, яку фінансові організації не зобов'язані дотримуватися.

Промислова група є третьою в рейтингу, показуючи високий рівень обізнаності та хороший індекс захисту, але відстаючи у прийнятті політики. Група РА демонструє низький ступінь готовності до кібербезпеки порівняно з іншими групами; дійсно, площа, охоплена радіолокаційним графіком, є найменшою серед усіх груп. Він має найнижчі індекси щодо політики, оборони та обізнаності.

Посилання

[1] Статистика повітряного транспорту - Statistics Explained (2013/12/10). Доступний на: http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=avia_paoc&lang=en.

[2] Базель II - Додаток 9. Доступно за адресою: http://www.bis.org/bcbs/cp3annex.pdf.

[3] Базель II – Стовп один. Доступний на: http://www.bis.org/bcbs/ cp3part2.pdf.

[4] Угода Базель II. Доступний на: http://www.bis.org/bcbs/ bcbscp3.htm.

[5] Веб-сайт Євроконтролю. http://www.eurocontrol.int/articles/what- air-traffic-management.

[6] Агентство ЄС з мережевої та інформаційної безпеки (enisa), список національних стратегій кібербезпеки, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in- the-world.

[7] PCI Security Standard Council, Payment Card Industries (PCI) Data Security Standard - Вимоги та процедури оцінки безпеки. доступні онлайн: https://www.pcisecuritystandards.org/ security_standards/download.html?id=pci_dss_v1-2.pdf.

[8] Президентська політична директива – Безпека та стійкість критичної інфраструктури | Білий дім.149

[9] Веб-сайт проекту SESAR.http://ec.europa.eu/transport/modes/ air/sesar/.

[10] Shamoon the Wiper – Copycats at Work – Публікація в блозі http://www.securelist.com/en/blog/208193786/Shamoon_the_Wiper_ Copycats_at_Work.

[11] Shodan website.http://www.shodanhq.com.

[12] Shamoon the Wiper – Copycats at Work – Публікація в блозі: http://www.eurocontrol.int/dossiers/single-european-sky.

[13] Комплексна національна ініціатива з кібербезпеки. Офіційний сайт Whitehouse. Доступний на: http://www.whitehouse.gov/sites/ default/files/cybersecurity.pdf.

[14] Вікіпедія - Alta velocità ferroviaria.

[15] Оцінка вразливості транспортної інфраструктури на основі глобальної системи позиціонування. Доступний на: http://www. navcen.uscg.gov/pdf/vulnerability_assess_2001.pdf. Національний центр транспортних систем Вольпе – Управління з досліджень транспорту та інноваційних технологій Департаменту США, Кембридж, Массачусетс, 2001.

[16] Захист критичної інфраструктури – ситуація в Італії. Президентство Ради міністрів - Департамент інновацій та технологій - Робоча група із захисту критичної інформаційної інфраструктури http://www.vigilfuoco.it/aspx/ReturnDocument.aspx?IdDocumento=2832, 2004.

[17] Директива ради щодо європейської програми захисту критичної інфраструктури. COM(2006) 786, Brussels., 2006.

[18] Директива Ради щодо ідентифікації та позначення європейської критичної інфраструктури та оцінки необхідності покращення їх захисту. COM(2006) 787, Brussels., 2006.

[19] Стратегія безпечного інформаційного суспільства – «діалог, партнерство та розширення можливостей». COM(2006) 251, Brussels., 2006.

[20] Директива Ради про ідентифікацію та позначення європейських критичних інфраструктур та оцінку необхідності покращення їх захисту. COUNCIL DIRECTIVE 2008/114/EC, 2008.

[21] Директива Європейського Союзу 2008/114/ec, 2008.

[22] Визначення критичних IT-інфраструктур національного інтересу. Указ Міністерства внутрішніх справ Італії G.U. 30 квітня 2008 р. № 101, 2008.

[23] ICS-CERT - Міністерство внутрішньої безпеки США - Сповіщення (ICS- ALERT-10-301-01) Система контролю доступу до Інтернету - http://ics-cert.us-cert.gov/alerts/ICS-ALERT-10-301-01, 2010.

[24] Пропозиція регламенту Європейського парламенту та Ради щодо Європейського агентства мережевої та інформаційної безпеки (enisa). COM(2010) 521, Brussels., 2010.

[25] Стратегія кібербезпеки Smart Grid, архітектура та вимоги високого рівня. Рекомендації NISTIR 7628 щодо кібербезпеки Smart Grid: Vol. 1,2010.

[26] UNISIG SUBSET-037, Euroradio FIS, версія 2.3.0. Європейське залізничне агентство. Доступний на: http://www.era.europa.eu/Document-Register/Pages/UNISIGSUBSET-037.aspx, 2010.

[27] Профіль безпеки для глобального моніторингу, захисту та контролю. версія 0.8. Проект розширеного прискорення безпеки (ASAP-SG), 2011.

[28] Майбутнє електричної мережі. Доступний онлайн: http://web.mit.edu/mitei/research/studies/the-electric-grid-2011.shtml. Массачусетський технологічний інститут (MIT), 2011.

[29] Збої в мережі Арізона-Південна Каліфорнія 8 вересня 2011 р. Звіт персоналу FERC/NERC про відключення електроенергії 8 вересня 2011 р., 2012 р.

[30] *Conto Nazionale delle Infrastrutture e dei Trasporti. Anni 2010 - 2011. Istituto Poligrafico e Zecca dello Stato S.p.A. - Рим, 2012.*

[31] Список безпеки Kaspersky. http://www.securelist.com/en/analysis/204792244/The_geography_of_cybercrime_Western_Europe_and_North_America, 2012.

[32] Мережа передового досвіду (NESoS) Результати: Вибір і документація двох основних практичних прикладів. Springer Lecture Notes in Computer Science, 2012.

[33] Звіт про кіберзлочинність Norton 2012 – Італія. http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/NCR-Country_Fact_Sheet-Italy.pdf, 2012.

[34] Стратегія кібербезпеки Європейського Союзу: відкритий, безпечний і надійний кіберпростір. Європейська Комісія, Брюссель, JOIN(2013) 1 фінал, 2013.

[35] *Ми, Італія. 100 статистичних даних, щоб зрозуміти, в якій країні ми живемо*. ISTAT, 2013.

[36] *Звіт Clusit 2013 про безпеку ІКТ в Італії. Cardi Editore San Babila gallery 4 20122 Milan, 2013*.

[37] Річний звіт про стан послуг. Технічний звіт, Управління електроенергетики та газу, 2013.

[38] М. Афзаал, К. Ді Сарно, Л. Копполіно, С. Д'Антоніо та Л. Романо. Відмовостійка архітектура для криміналістичного зберігання подій у критичних інфраструктурах. У High-Asurance Systems Engineering (HASE), 14-й міжнародний симпозіум IEEE, сторінки 48–55, 2012 р.

[39] М. Афзаал, К. Ді Сарно, С. Дантоніо та Л. Романо. Зловмисне та відмовостійке сховище для системи SIEM. На Восьмій міжнародній конференції з технології зображення сигналу та систем на основі Інтернету (SITIS), сторінки 579–586, 2012 р.

[40] ALARP - Автоматична система попередження про залізничну колію на основі розподілених персональних мобільних терміналів - Проектний контракт FP7-SST-2010- 234088, http://www.alarp.eu.

[41] M. Albanese, S. Jajodia, A. Pugliese та V. S. Subrahmanian. Масштабований аналіз сценаріїв атак. В ESORICS, сторінки 416–433, 2011.

[42] М. Альбанезе, А. Пульєзе та В. С. Субрахманян. Швидке виявлення активності: індексування для часових стохастичних автоматних моделей активності. IEEE Transactions on Knowledge and Data Engineering, 25(2):360–373, 2013.

[43] Л. Аллоді та Ф. Массаччі. Попередній аналіз балів уразливості для атак у дикій природі. У матеріалах семінару ACM CCS 2012 року зі створення наборів даних аналізу та збору результатів досвіду для безпеки, 2012.

[44] Л. Аллоді та Ф. Массаччі. Як CVSS використовує вашу політику виправлення DOS (і витрачає ваші гроші). Чорний капелюх США, 2013.

[45] П. Амманн, Д. Вієсекера та С. Каушік. Масштабований аналіз вразливості мережі на основі графіків. На конференції ACM з комп'ютерної та комунікаційної безпеки, сторінки 217–224, 2002 р.

[46] Г. Андерссон, П. Доналек, Р. Фармер, Н. Хаціаргіріу, І. Камва, П. Кундур, Н. Мартінс, Дж. Пасерба, П. Пурбейк, Дж. Санчес-Гаска, Р. Шульц, А. Станковіч, К. Тейлор і В. Віттал. Причини великих відключень мережі в 2003 році в Північній Америці та Європі та рекомендовані способи покращення динамічної продуктивності системи. IEEE Transactions on Power Systems, 20(4):1922–1928, 2005.

[47] М. Ангел, К. Верлі та А. Моттер. Стохастична модель динаміки електромереж. На 40-й щорічній Гавайській міжнародній конференції системних наук (HICSS), сторінки 113–113, 2007 р.

[48] Asis International. Загальні рекомендації щодо оцінки ризиків безпеки. Доступно за адресою: http://www.asisonline.org/guidelines/guidelinesgsra.pdf, 2008.

[49] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr. Основні концепції та таксономія надійних і безпечних обчислень. Надійні та безпечні обчислення, IEEE Transactions on, 1(1):11–33, 2004.

[50] В. Бейкер, М. Говард, А. Хаттон і К. Д. Хайлендер. Звіт про розслідування витоку даних за 2012 рік. Технічний звіт, Verizon, 2012.

[51] Дж. Бальдіні, І. Н. Фовіно, М. Масера, М. Луїзе, В. Пеллегріні, Е. Багальї, Дж. Рубіно, Р. Малангоне, М. Стефано, Ф. Сенезі. Система раннього попередження для виявлення бездротових перешкод GSM-R в інфраструктурі високошвидкісної залізниці. Міжнародний журнал захисту критичної інфраструктури, 3(3–4):140 – 156, 2010.

[52] Р. Бальдоні, Г. Лоді, Л. Монтанарі, Г. Маріотта, М. Ріцуто. Онлайн-прогнозування несправностей чорної скриньки для критично важливих розподілених систем. У SAFECOMP, сторінки 185–197, 2012 р.

[53] М. Беккуті, С. К'ярадонна, Ф. Ді Джандоменіко, С. Донателлі, Дж. Дондоссола, Г. Франческініс. Кількісна оцінка залежностей між електричною та інформаційною інфраструктурами. Міжнародний журнал захисту критичної інфраструктури, 5(1):14–27, 2012 р.

[54] М. Беккуті, С. К'ярадонна, Ф. Д. Джандоменіко, С. Донателлі, Дж. Дондоссола, Г. Франческініс. Кількісна оцінка залежностей між електричною та інформаційною інфраструктурами. Міжнародний журнал захисту критичної інфраструктури, 5(1):14 – 27, 2012.

[55] Д. Белл і Л. Дж. Л. Падула. Захищені комп'ютерні системи: уніфікована експозиція та багатофункціональна інтерпретація. Технічний звіт, MITER Corp., Бедфорд, Массачусетс, Тех. Відповідь ESD-TR-75-306,, 1975.

[56] К. Беннетт і С. Вікер. Зменшення часу затримки та рекомендації щодо підвищення безпеки для мереж інтелектуальних лічильників AMI. Innovative Smart Grid Technologies (ISGT), 2010.

[57] Р. Бертьє і В. Х. Сандерс. Виявлення вторгнень на основі специфікацій для розширеної інфраструктури вимірювання. У матеріалах 2011 IEEE 17th Pacific Rim International Symposium on Dependable Computing, PRDC '11, сторінки 184–193, Вашингтон, округ Колумбія, США, 2011. IEEE Computer Society.

[58] Р. Блумфілд, Р. Блумфілд, І. Гаші, Р. Страуд. Наскільки безпечна ERTMS? У комп'ютерній безпеці, надійності та безпеці, том 7613 конспектів лекцій з інформатики, сторінки 247–258. Springer Berlin Heidelberg, 2012.

[59] Р. Блумфілд, Н. Чозос і П. Ноблс. Аналіз взаємозалежності інфраструктури: вимоги, можливості та стратегія. Технічний звіт, доступний онлайн http://www.csr.city.ac.uk/projects/ cetifs/d418v13_public.pdf, 2009.

[60] Дж. Бродер. Аналіз ризиків та дослідження безпеки. Баттерворт-Хайнеманн, 2006.

[61] С. Бучеггер і Дж.-Й. Ле Будек. Аналіз продуктивності впевненого протоколу. У матеріалах 3-го міжнародного симпозіуму ACM з мобільних спеціальних мереж і обчислень, MobiHoc '02, сторінки 226–236, Нью-Йорк, Нью-Йорк, США, 2002. ACM.

[62] Л. Буттян, Д. Гесснер, А. Гесслер, П. Лангендоерфер. Застосування бездротових сенсорних мереж у захисті критичної інфраструктури: проблеми та варіанти проектування. Бездротовий зв'язок, IEEE, 17(5):44–49, 2010.

[63] G. S. Capra та U. Center. Захист критично важливої з алізничної інфраструктури. Центр протидії розповсюдженню ВПС США, Повітряний університет, 2006.

[64] А. А. Карденас, Т. Руста, С. Састрі. Переосмислення властивостей безпеки, моделей загроз і простору проектування в сенсорних мережах: тематичне дослідження в системах SCADA. Ad Hoc Netw., 7(8):1434–1447, 2009.

[65] Е. Казалікіо, Е. Галлі та С. Туччі. Федеративне моделювання та імітаційний підхід на основі агентів для вивчення взаємозалежностей у критичних інфраструктурах. У розподіленому моделюванні та програмах реального часу, 2007. DS-RT 2007. 11-й міжнародний симпозіум IEEE, сторінки 182–189, 2007.

[66] М. Кашіаро. Моделювання та аналіз безпеки в системі автоматичного захисту робочого місця. Магістерська робота, Університет Флоренції, 2013.

[67] А. Чеккареллі, А. Бондаваллі, Ж. Фігейраса, Б. Маліновського, Я. Вакули, Ф. Бранкаті, К. Дамбри, А. Семінаторе. Розробка та реалізація переносних пристроїв у режимі реального часу для критично важливої д ля безпеки системи попередження про трек. У HASE, сторінки 147–154, 2012.

[68] А. Чеккареллі, І. Майзік, Д. Йовіно, Ф. Канескі, Г. Пінтер, А. Бондаваллі. Надійний SIL 2 інтерфейс машинобудування для систем керування поїздами. У DepCoS-RELCOMEX, сторінки 365–374, 2008 р.

[69] CENELEC. Залізничні програми – Системи зв'язку, сигналізації та обробки – Електронні системи сигналізації, пов'язані з безпекою. EN 50129, 1999.

[70] CENELEC. Залізничне застосування – специфікація та демонстрація надійності, доступності, ремонтопридатності та безпеки (RAMS). EN 50126, 1999.

[71] CENELEC. *EN 50159-1 - Залізничне застосування - Системи зв'язку, сигналізації та обробки - Частина 1 - Зв'язок, пов'язаний з безпекою в закритих системах передачі, 2001*.

[72] CENELEC. *EN 50159-2 - Залізничне застосування - Системи зв'язку, сигналізації та обробки - Частина 2 - Зв'язок, пов'язаний з безпекою, у відкритих системах передачі, 2001*.

[73] Р. Чандіа, Дж. Гонсалес, Т. Кілпатрік, М. Папа та С. Шеной. Стратегії безпеки для мереж SCADA. У захисті критичної інфраструктури, том 253 Міжнародної федерації з обробки інформації IFIP, сторінки 117–131. Springer США, 2007.

[74] Ю. Чен, Б. В. Бем та Л. Шеппард. Моделювання загроз безпеці, орієнтоване на цінності, на основі аналізу шляху атаки. У HICSS, сторінка 280, 2007.

[75] С. Чунг, Б. Дутертре, М. Фонг, У. Ліндквіст, К. Скіннер і Вальдес. Використання моделі виявлення вторгнень для мереж SCADA. У матеріалах наукового симпозіуму безпеки SCADA, 2007.

[76] С. К'ярадонна, Ф. Д. Джандоменіко та П. Лолліні. Визначення, реалізація та застосування модельної основи для аналізу взаємозалежностей в електроенергетичних системах. Міжнародний журнал захисту критичної інфраструктури, 4(1):24–40, 2011.

[77] С. К'ярадонна, Ф. Д. Джандоменіко та П. Лолліні. Визначення, впровадження та застосування модельної основи для аналізу взаємозалежностей у захисті електроенергетичних систем. Міжнародний журнал критичної інфраструктури (IJCIP), Elsevier, 4(1):24–40, квітень 2011 р.

[78] Б. Конвей. Потреба Уолл-стріт у швидкості торгівлі: епоха наносекунд. Доступний на: http://blogs.wsj.com/marketbeat/2011/06/14/wall-streets-need-for-trading-speed-the-nanosecond-age/. *The Wall Street Journal*, 2011.

[79] А. Корсаро. CARDAMOM: проміжне програмне забезпечення нового покоління, яке має важливе значення для завдань і безпеки. На третьому семінарі IEEE з програмних технологій для майбутніх вбудованих і повсюдних систем (SEUS), сторінки 73–74, 2005 р.

[80] А. Костін і А. Франсильон. Ghost in the Air (Traffic): Про незахищеність протоколу ADS-B і практичні атаки на пристрої ADS-B. У Чорному Капелюсі, Лас-Вегас, Невада, США, 27 липня – 1 серпня 2012 р..

[81] Дослідницький центр кіберрозвідки та інформаційної безпеки Sapienza - Università di Roma. Італійський звіт про кібербезпеку за 2013 рік – готовність критичної інфраструктури та інших чутливих секторів. Casa Editrice Università La Sapienza, 2013.

[82] С. Деламаре, А. Діалло, К. Шоде. Високорівневе моделювання взаємозалежностей критичних інфраструктур. Міжнародний журнал критичних інфраструктур, 5(1/2), 2009.

[83] Г. Девараджан. Розгадування протоколів scada: використання Sulley fuzzer. На Def-Con 15 Hacking Conference, 2007.

[84] Г. Діні та М. Тілока. Міркування щодо безпеки в мережах zigbee. На IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC), сторінки 58–65, 2010 р.

[85] Д. Доберштейн. Основи GPS-приймачів: апаратний підхід. Springer New York, 2011.

[86] Д. В. Доллен. Доповідайте NIST про дорожню карту стандартів сумісності Smart Grid. Контракт EPRI № SB1341-09-CN-0031-Поставка 7, 2009.

[87] Д. Друїди. Смертельні випадки травм на залізниці. Доступно за адресою: http://www.pcsforum.org/library/files/1159904563-TSWG_INL_CIP_Tool_Survey_final.pdf. Технічний звіт Щомісячний огляд праці, 2007.

[88] Х. М. Ель-Бакрі та Н. Масторакіс. Дизайн анти-GPS з міркувань безпеки. У матеріалах міжнародної конференції з обчислювальної та інформаційної науки, СНД'09, сторінки 480–500, Стівенс-Пойнт, Вісконсін, США, 2009. Всесвітня наукова та інженерна академія та суспільство (WSEAS).

[89] Еніса. Аналіз аспектів кібербезпеки в морському секторі, 2011.

[90] Євроконтроль. Що таке організація повітряного руху? Будівництво skyways, управління

транспортними потоками та пропускною здатністю, обслуговування рейсів. Доступно в Інтернеті: http://www.eurocontrol.int/articles/what-air-traffic- management, 2011.

[91] Європейська комісія, Спільний дослідницький центр. JRC, проекти Smart Grid в Європі: отримані уроки та поточні розробки. Технічний звіт, Довідковий звіт Спільного дослідницького центру http://www.pcsforum.org/library/files/1159904563-TSWG_INL_CIP_Tool_Survey_final.pdf, 2011.

[92] Н. Фальєр, Л. О. Мурчу та Е. Чиен. W32. Досьє Stuxnet. Доступно онлайн http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier. pdf, 2011.

[93] Федеральне управління авіації. Вимоги до продуктивності автоматичного залежного спостереження (ADS-B) для підтримки служби управління повітряним рухом (ATC). Остаточне правило, 14 CFR, частина 91, Федеральний реєстр 75 (103), 2010 р.

[94] К. Фінке, Дж. Баттс, Р. Міллс і М. Грімайла. Підвищення безпеки спостереження за повітряним судном у системі управління повітряним рухом нового покоління. Міжнародний журнал захисту критичної інфраструктури, 6(1):стор. 3–11, 2013.

[95] Ф. Фламміні, А. Галіоне, Н. Маццокка, К. Прагліола. Кількісна оцінка ризиків безпеки та управління інфраструктурою залізничного транспорту. У безпеці критичної інформаційної інфраструктури, том 5508 конспектів лекцій з інформатики, сторінки 180–189. Springer Berlin Heidelberg, 2009.

[96]C.-B. G., C.-S. J., and S. L. *Вимірювання фінансового посередництва в Японії. Японія та світова економіка, 2008*.

[97] М. Гарсіа. Оцінка вразливості систем фізичного захисту. Баттерворт-Хайнеманн, 2005.

[98] А. Гарофало, К. Ді Сарно, Л. Копполіно, С. Д'Антоніо. Стійкий до підробки GPS WAMS для Smart Grid. У Dependable Computing, том 7869 конспектів лекцій з інформатики, сторінки 134–147. Springer Berlin Heidelberg, 2013.

[99] Л. Гепперт. Втрачений радіозв'язок залишає пілотів на самоті. Спектр, IEEE, 41(11):16–17, 2004.

[100] С. Гоф. Банки сказали виправити системи після збою RBS. Financial Times, липень 2012 р.

[101] Р. В. Голдсміт. Фінансова структура та розвиток. Yale University Press - New Haven, 1969.

[102] М. Говіндарасу, А. Хан, П. Зауер. Безпека кіберфізичних систем для Smart Grid. Серія вебінарів PSERC Future Grid Initiatives, лютий 2012 р.

[103] М. Хедлі, Дж. Макбрайд, Т. Едгар, Л. О'Ніл, Дж. Джонсон. Захист вимірювальних систем великої зони. Доступно за адресою:: http://energy.gov/ oe/downloads/securing-wide-area-measurement-systems. Управління постачання електроенергії та енергетичної надійності Міністерства енергетики США, 2007 р..

[104] Дж. Холл і Г. Рейнер. Збій комп'ютера RBS прирікає чоловіка проводити вихідні в камерах. Telegraph, червень 2012 р.

[105] М. Хентея. Покращення безпеки для систем управління SCADA. Міждисциплінарний журнал інформації, знань та управління, 3(1):73–86, 2008.

[106] Дж. Хонг, С.-С. Ву, А. Стефанов, А. Фшоша, К.-К. Лю, П. Гладишев, М. Говіндарасу. Випробувальний стенд протидії та захисту в середовищі кіберенергетичної системи. У Загальних зборах IEEE Power and Energy Society, сторінки 1–5, 2011 р.

[107] Інститут П. ім. Дослідження вартості витоку даних у 2011 році. http://www.ponemon.org.

[108] С. Р. Джонсон, М. Монтанарі та Р. Х. Кемпбелл. Автоматичне керування лісозаготівельною інфраструктурою. In *National Centers of Academic Excellence - Workshop on Insider Threat*, St Louis, MO, USA, 2010.

[109] Н. Джонсон, Г. Чжао, Е. Хунсадер, Х. Ці, Н. Джонсон, Дж. Мен і Тівнан. Раптовий розвиток нової машинної екології перевищує час реакції людини. Sci. Відп., 3, 09 2013.

[110] Лабораторія Касперського. Географія кіберзлочинності: Західна Європа та Північна Америка. Технічний звіт, 2012.

[111] Л. Кенні, Дж. Дітріх і Дж. Вудолл. Безпечне спостереження АТС для військових застосувань. На конференції IEEE Military Communications Conference, 2008. MILCOM, сторінки 1–6, 2008.

[112] С. Ларссон і Е. Ек. Знеструмлення в південній Швеції та східній Данії, 23 вересня 2003 р. На загальних зборах IEEE Power Engineering Society, сторінки 1668–1672, том 2, 2004 р.

[113] Y. W. Law, M. Palaniswami, G. Kounga та A. Lo. WAKE: схема керування ключами для систем глобального вимірювання в інтелектуальній мережі. Журнал IEEE Communications, 51(1):34–41, 2013.

[114] Е. Е. Лі, Дж. Е. Мітчелл і В. А. Уоллес. Оцінка вразливості запропонованих проектів для взаємозалежних інфраструктурних систем. На 7-й Гавайській міжнародній конференції з системних наук, 2004 р.

[115] Е. Лемей, М. Форд, К. Кіф, В. Сандерс і К. Мюрке. Показники безпеки на основі моделі з використанням оцінки безпеки ADversary View (ADVISE). На 8-й Міжнародній конференції з кількісної оцінки систем (QEST), сторінки 191–200, вересень 2011 р.

[116] Р. Леон, В. Віттал, Г. Манімаран. Застосування сенсорної мережі для безпечної електроенергетичної інфраструктури. IEEE Transactions on Power Delivery, 22(2):1021–1028, 2007.

[117] Т. Льюїс. Захист критичної інфраструктури у внутрішній безпеці: Захист мережевої нації. Джон Вайлі, 2006.

[118] J. Liu, Y. Xiao, S. Li, W. Liang і C. L. P. Chen. Проблеми кібербезпеки та конфіденційності в розумних мережах. Підручники з оглядів комунікацій, IEEE, 14(4):981–997, 2012 р..

[119]B. M. and S. E. M. *International CIIP Handbook 2008/2009*. Center for Security Studies, ETH Zurich, 2008.

[120]M. Mackenzie and A. Massoudi. NYSE cancels trades after algo glitch. Financial times. Available Online: http://www.ft.com/intl/cms/s/0/bd5f2af8-dbe7-11e1-8d78-

00144feab49a.html?siteedition=intl#axzz2f3Fy6h85, August2010.

[121] В. Мадані та Р. Кінга. Стратегії та дорожні карти для вирішення проблем електромережі щодо безпеки та надійності. У G. Anders і A. Vaccaro, редактори, Innovations in Power Systems Reliability, Springer Series in Reliability Engineering, сторінки 1–11. Springer London, 2011.

[122] Б. Маліновський, Г. Гронбек, Г. Швефель, А. Чеккареллі, А. Бондаваллі та Е. Нетт. Трансляція за часом через готову функцію розподіленої координації WLAN для важливих для безпеки систем. На Європейській конференції з надійних комп'ютерів (EDCC), сторінки 144–155, 2012 р.

[123] С. Марті, Т. Дж. Джулі, К. Лай і М. Бейкер. Пом'якшення неправильної маршрутизації в мобільних ad hoc мережах. У матеріалах 6-ї щорічної міжнародної конференції з мобільних комп'ютерів і мереж, Mobi-Com '00, сторінки 255–265, Нью-Йорк, Нью-Йорк, США, 2000. ACM.

[124] М. Масера. Підхід до розуміння взаємозалежностей. В енергетичних системах та інфраструктурах зв'язку майбутнього (CRIS). 2002 рік.

[125] Б. Мастерс, Е. Мур, Дж. Пікард. Оновлення, яке призвело до падіння Королівського банку Шотландії. Financial Times. Доступно онлайн: червень 2012.

[126] Д. Маккеллі, Дж. Баттс і Р. Міллс. Аналіз безпеки впровадження ads-b у системі повітряного транспорту наступного покоління. Міжнародний журнал захисту критичної інфраструктури, 4(2):стор. 78–87, 2011.

[127] П. Мак-Деніел і С. Маклафлін. Проблеми безпеки та конфіденційності в Smart Grid. Безпека та конфіденційність IEEE, 7(3):стор. 75–77, травень 2009 р.

[128] Г. Макдональд, Л. О. Мурчу, С. Доерті та Е. Чиен. Stuxnet 0.5: Відсутня ланка – доступно в Інтернеті http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/stuxnet05themissinglink.pdf.

[129] Дж. Макдональд. Інженерія електропідстанцій. CRC Press, Бока-Ратон, Флорида, 2007.

[130] С. Маклафлін, Д. Подкуйко, П. Макденіел. Крадіжка енергії в передовій інфраструктурі вимірювання. Безпека критичних інформаційних інфраструктур, сторінки 176–187, 2010.

[131] П. Мелл, К. Скарфоне та С. Романоскі. Повний посібник із загальної системи оцінки вразливостей версії 2.0. Технічний звіт, FIRST, доступний на http://www.first.org/cvss, 2007.

[132] Дж. В. Мерітт. Метод кількісного аналізу ризику. Доступно в Інтернеті: http://csrc.nist.gov/nissc/1999/proceeding/papers/p28.pdf, 2008.

[133] Я. Момох. Smart Grid: основи проектування та аналізу. I E E Серія Енергетика. Wiley, 2012.

[134] Б. Морен, Л. Ме, Х. Дебар і М. Дюкассе. M2d2: формальна модель даних для кореляції сповіщень ідентифікаторів. У RAID, сторінки 115–127, 2002.

[135] Б. Т. Морріс і М. М. Тріведі. Навчання траєкторії для розуміння діяльності: неконтрольований, багаторівневий та довгостроковий адаптивний підхід. IEEE Transactions on Pattern Analysis and Machine Intelligence, 33(11):2287–2301, 2011.

[136] Т. Морріс, С. Пан і У. Адхікарі. Рекомендації з кібербезпеки для систем глобального моніторингу, захисту та контролю. У Power and Energy Society General Meeting, 2012 IEEE, сторінки

1–6, 2012.

[137] Дж. Мотефф. Управління ризиками та захист критичної інфраструктури: оцінка, інтеграція та управління загрозами, вразливими місцями та наслідками. Звіт CRS для Конгресу, Бібліотека Конгресу, 2004.

[138] Ж. М. Мойя, А. Араухо, З. Банкович, Ж.-М. Д. Гойенече, Х. К. Вальехо, П. Малагон, Д. Вільянуева, Д. Фрага, Е. Ромеро та Дж. Блеса. Покращення безпеки для сенсорних мереж SCADA за допомогою систем репутації та самоорганізованих карт. У датчиках. 9, сторінки 9380–9397, 2009.

[139] К. Манро. SCADA - Критична ситуація. Безпека мережі, (1):4 – 6, 2008.

[140] NDTV. Програма для телефону, яка загрожує безпеці. Press Trust of India, Нью-Делі, Індія, 4 жовтня 2010 р.

[141] Д. М. Нікол, В. Х. Сондерс і К. С. Тріведі. Оцінка на основі моделі: від надійності до безпеки. IEEE Transactions on Dependable and Secure Computing, 1(1):48–65, 2004.

[142] С. Ноель, Е. Робертсон і С. Джайодія. Співвідношення подій вторгнення та створення сценаріїв атак за допомогою відстаней на графіку атак. В ACSAC, сторінки 350–359, 2004.

[143] North American Electric Reliability Corporation. Стандарти захисту критичної інфраструктури 002-3 - 009-3, 2009.

[144] У. Д. енергетики. Звіт про систему Smart Grid. Технічний звіт, Міністерство енергетики США, лютий 2012 р. http://energy.gov/sites/prod/ files/2010%20Smart%20Grid%20System%20Report.pdf.

[145]OMG. Специфікації служби розповсюдження даних. http://www.omg.org/spec/DDS/, 2007.

[146] Ф. Д. Орал. Вплив стихійних лих на енергетичні системи: анатомія відключення електроенергії від землетрусу Мармара. Acta Polytechnica Hungarica, 7(2):107–118, 2010.

[147] М. А. Палфі. Ефективний захист критичної інфраструктури морського порту: перспектива управління проектами та критичного мислення. Синергія, 2:237–253, 2008.

[148]A. Pecchia, R. Pietrantuono, and S. Russo. Criticality-driven component integration in complex software systems. In *Computer Safety, Reliabil-ity, and Security*, pages 452–466. Springer, 2011.

[149]D. Peck and D. Peterson. Leveraging ethernet card vulnerabilities in field devices. In *Proceedings of SCADA Security Scientific Symposium,Miami, USA*, 2009.

[150]P. Pederson, D. Dudenhoeffer, S. Hartley, and M. Permann. Critical infrastructure interdependency modeling: A survey of U.S. and international research. Technical Report INL/EXT-06-11464, http://www.pcsforum.org/library/files/1159904563- TSWG_INL_CIP_Tool_Survey_final.pdf, August 2006.

[151]P. Pourbeik, P. S. Kundur, and C. W. Taylor. The anatomy of a power grid blackout. *IEEE Power and Energy Magazine*, pages 22–29,September-October 2006.

[152]J. Quirke. Security in the GSM system. *AusMobile, May*, pages 1–26,2004.

[153]B. R., S. K., W. D., C. N., and N. P. Infrastructure interdependency analysis: an introductory research review. In *Adelard document reference D/422/12101/4 available for download at http: // www. csr.city. ac. uk/projects/cetifs. html* , 2009.

[154]G. D. Rash. GPS Jamming in A Laboratory Environment. In *Proceed- ings of the 53rd Annual Meeting of The Institute of Navigation*, pagespp. 389–398., 1997.

[155]S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly. Identifying, Un- derstanding, and Analyzing Critical Infrastructure Interdependencies.*IEEE Control Systems Magazine*, pages 11–25, December 2001.

[156]B. Robert, R. D. Calan, and L. Morabito. Modelling interdependencies among critical infrastructures. *IJCIS*, 4(4):392–408, 2008.

[157]L. Romano, S. D'Antonio, V. Formicola, and L. Coppolino. Protecting the wsn zones of a critical infrastructure via enhanced siem technology. In F. Ortmeier and P. Daniel, editors, *Computer Safety, Reliability, andSecurity*, volume 7613 of *Lecture Notes in Computer Science*, pages 222–
234. Springer Berlin Heidelberg, 2012.

[158]J. J. Romero. Blackouts illuminate India's power problems. *IEEE Spec-trum*, 49(10):11–12, 2012.

[159]V. Rosato, L. Issacharoff, F. Tiriticco, S. Meloni, S. D. Porcellinis, and
R. Setola. Modelling interdependent infrastructures using interacting dynamical models. *International Journal of Critical Infrastructures*, 4(1/2):63, 2008.

[160]J. Salmeron, K. Wood, and R. Baldick. Analysis of electric grid security under terrorist threat. *IEEE Transactions on Power Systems*, 19(2):905–912, 2004.

[161]W. H. Sanders and J. F. Meyer. Stochastic activity networks: formal definitions and concepts. In *Lectures on formal methods and performance analysis*, pages 315–343. Springer-Verlag New York, Inc., New York, NY,USA, 2002.

[162]R. Shapiro, S. Bratus, E. Rogers, and S. Smith. Identifying vulnera- bilities in SCADA systems via Fuzz-Testing. In *Critical Infrastructure Protection V*, volume 367 of *IFIP Advances in Information and Com-munication Technology*, pages 57–72. Springer Berlin Heidelberg, 2011.

[163]D. P. Shepard, T. E. Humphreys, and A. A. Fansler. Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks. *International Journal of Critical Infrastructure Protection*, 2012.

[164]A. Singh and S. Aasma. A Grid failure in Northern, Eastern and North-Eastern grid in 2012: Cause & its effect on economy of India And Re- view. *SAMRIDDHI-A Journal of Physical Sciences, Engineering andTechnology (S-JPSET)*, 3(2), 2012.

[165]I. Sommerville. *Software engineering*. Addison-Wesley, 2001.

[166]J. Tate and T. Overbye. Line outage detection using phasor angle mea-surements. *IEEE Transactions on Power Systems*, 23(4):1644–1652,2008.

[167]J. Tate and T. Overbye. Double line outage detection using phasor angle measurements. In *IEEE Power and Energy Society General Meeting 09*,pages 1–5, 2009.

[168]C.-W. Ten, G. Manimaran, and C.-C. Liu. Cybersecurity for critical in- frastructures: Attack and defense modeling. *IEEE Transactions on Sys-tems, Man and Cybernetics, Part A: Systems and Humans,*, 40(4):853–865, 2010.

[169]H. Teso. Aircraft hacking: Practical aero series. In *4th annual Hack in the Box Security Conference*, Amsterdam, The Netherlands, April 10–11 2013.

[170]The Power Grid. TCIPG: Trustworthy Cyber Infrastructure for the Power Grid website: http://tcipg.org.

[171]W. C. Thompson. Railroad infrastructure security, trb annual meeting,january 14 2002.

[172] UIC. *Subset 033 - rev. 2.0.0 - ERTMS-ETCS Class 1 - FIS for the Man-Machine Interface*, 2000.

[173] UIC. *Subset-026 - rev.2.2.2 - ERTMS-ETCS Class 1 - System require- ments specification*, 2002.

[174]V. Urias, B. Van Leeuwen, and B. Richardson. Supervisory Command and Data Acquisition (SCADA) system cyber security analysis using a live, virtual, and constructive (LVC) testbed. In *Military Communica-tions Conference (MILCOM)*, pages 1–8, 2012.

[175]U.S.-Canada Power System Outage Task Force. *Final report on the August 14, 2003 blackout in the United States and Canada: causes and recommendations.* U.S. Dept. of Energy, Washington, D.C, 2004.

[176]U.S. Commodity Futures Trading Commission and U.S. Securities & Exchange Commission. Findings regarding the market events of may 6, 2010 - Available online: http://www.sec.gov/news/studies/2010/
marketevents-report.pdf, September 2010.

[177]U.S. Department of Transportation. The Public Transportation Security & Emergency Preparedness Planning Guide. Federal Transit Adminis-tration, Final Report, 2003.

[178]G. Vigna. A Topological Characterization of TCP/IP Security. In *FME*,pages 914–939, 2003.

[179]G. Vigna and R. A. Kemmerer. NetSTAT: A Network-Based IntrusionDetection Approach. In *ACSAC*, pages 25–34, 1998.

[180]J. Wang, Z. Cheng, M. Zhang, Y. Zhou, and L. Jing. Design of a Situation-Aware System for Abnormal Activity Detection of Elderly Peo- ple. In *AMT*, pages 561–571, 2012.

[181]L. Wang, A. Liu, and S. Jajodia. An efficient and unified approach to correlating, hypothesizing, and predicting intrusion alerts. In *ESORICS*,pages 247–266, 2005.

[182]L. Wang, S. Noel, and S. Jajodia. Minimum-cost network hardening us- ing attack graphs. *Computer Communications*, 29(18):3812–3824, 2006.

[183]J. S. Warner and R. G. Johnston. GPS Spoofing Countermeasures.
Journal of Homeland Security, 2003.

[184]R. Watts. Maritime Critical Infrastructure Protection: Multi-Agency Command and Control in an Asymmetric Environment. Homeland Se-curity Affairs 1, issue 2, 2005.

[185]W. E. Wong, V. Debroy, A. Surampudi, H. Kim, and M. F. Siok. Recent Catastrophic Accidents: Investigating How Software Was Responsible. In *Fourth International Conference on Secure Software Integration andReliability Improvement (SSIRI)*, pages 14–22, 2010.

[186]A. Wood. After ADS-B launch, security concerns raised. Aviation In-ternational News, July 2006.

[187]D. Wu and C. Zhou. Fault-tolerant and scalable key management forsmart grid. *IEEE Transactions on Smart Grid*, 2(2):375–381, 2011.

[188]J. Xia and Y. Wang. Secure key distribution for the smart grid. *Smart Grid, IEEE Transactions on*, 3(3):1437–1443, 2012.