УДК 004.056-004.832

І.П. Сініцин, П.П. Ігнатенко, О.О. Слабоспицька, О.В. Артеменко

КОМПЛЕКСНИЙ ПІДХІД ДО ПОБУДОВИ СИСТЕМИ КІБЕРЗАХИСТУ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ

Надано комплексний підхід до вирішення проблем забезпечення кіберзахисту об'єктів критичної інформаційної інфраструктури держави з урахуванням кращих світових і вітчизняних практик та апробованих програмно-апаратних і програмних засобів кібернетичного захисту. Для ефективної реалізації підходу запропоновано інтелектуальну інформаційну технологію керівництва кібербезпекою. Вона поєднує доробок авторів з підтримки прийняття організаційних рішень (експертно-аналітичних і ділових) з новітніми підходами до управління вигодами від належної кібербезпеки та ризиками її порушення. Застосування підходу сприятиме підвищенню кіберзахисту критичної інформаційної інфраструктури держави.

Ключові слова: кіберпростір, кібератака, кібербезпека, комплексна система захисту інформації, кіберзахист, інтелектуальна інформаційна технологія, організаційне рішення.

Джерело та опис проблеми

Проблеми забезпечення кібербезпеки виникли у зв'язку з бурхливим розвитком мереж Інтернет. Запроваджений як дослідницький інструментарій для науковців, Інтернет поступово перетворився на головну інфраструктуру світової інформаційної спільноти. Уряди застосовують всесвітню мережу для інформування громадян і надання їм послуг у всьому світі. Компанії цілодобово обмінюються інформацією із своїми підрозділами, постачальниками, партнерами та клієнтами для підвищення ефективності своєї діяльності. Дослідницькі та навчальні заклади застосовують Інтернет насамперед як платформу співпраці та засіб дистанційного навчання і лише потім – як інструмент швидкого обміну результатами досліджень.

На жаль, з розвитком мережі Інтернет кількість зловмисних атак також почала швидко зростати. Згідно з даними CERT (Computer Emergency Response Team), центру експертизи безпеки Інтернет, розташованому в Сполучених Штатах, кількість задокументованих випадків порушення безпеки стрімко зросло в 1994 році з 2241 до 137539 у 2003 році. Починаючи з 2004 року CERT відмовився від підрахунку загальної кількості вторгнень і перейшов до практики детальних звітів із статистикою та аналізом за окремими типами атак.

Останнім часом усе частіше вживають термін «кібернетичний тероризм», що означає організовану діяльність, спрямовану проти Інтернет-інфраструктури певної держави (як приклад, можна навести атаки на сайти державних установ Естонії в 2007 р.). На сьогоднішній день доводиться констатувати, що надійного комплексного засобу протидії цим атакам немає. Досить згадати вірусні атаки 2017 року *Wanna Cry* та *Petya.A*, що завдали великих збитків державам в усьому світі, а від останньої вірусної атаки особливо постраждала Україна.

Таким чином, надійність і захищеність мережі Інтернет – це питання навіть не стільки втрати прибутків від бізнесу (хоча й це дуже важливо), скільки національної безпеки держави.

Отже, проблема, пов'язана із дослідженням кібератак у мережі Інтернет, розробкою методів їх виявлення та протиборства їм, побудовою систем захисту критичних та інших інфраструктур суспільства та держави в кіберпросторі є нині особливо важливою та актуальною [1–4].

Слід зазначити, що організація атак на відмову давно займає значне місце серед зловмисної діяльності в мережі Інтернет. Деяке спадання (точніше, незростання) кількості атак на відмову в 2006 році, що було пов'язане з бурхливим розвитком

інших видів діяльності, таких як спам і фітинг, схоже, закінчився. Початок 2007 року був ознаменований потужною атакою на кореневі сервери. Згідно з дослідженнями, спам і DoS-атаки – одні з основних тем новин інформаційної безпеки 2007 року. Починаючи з жовтня 2006 року, коли черв'як Warezov почав створювати гігантські зомбі-мережі в мережі Інтернет, почався новий етап розвитку спама. Ці події взаємопов'язані і вказують на взаємозв'язок цих двох явищ: Warezov збирав бази адрес і відправляв їх зловмисникам. Крім того, він встановлював на заражені комп'ютери модулі для організації спам-розсилок. Цим же займались і два інших активних поштових черв'яка – Zhelatin і Bagle.

Взагалі кажучи, можна виділити чотири категорії захисту від атак на відмову:

1) попередження атаки;
2) виявлення атаки;
3) ідентифікація джерела атаки;
4) протидія атаці.

Задача попередження атаки полягає у протидії атаці на підступах до жертви. Задача виявлення атаки полягає у детектуванні атаки на відмову в разі її появи. Виявлення атаки – це важливий етап, від якого залежать усі подальші дії. Ідентифікація джерела атаки призначена для виявлення істинного місця здійснення атаки, незалежно від того, звідки прийшов трафік. Це має велике значення для зменшення потужності атаки, крім того, ризик виявлення стримує потенційних нападників. Протидія атаці призначена для знешкодження атаки. Це заключна частина захисту, і тому визначає загальну характеристику усього механізму. Основна проблема протидії атаці полягає у наступному: як відфільтрувати трафік атаки і не вплинути на трафік звичайних користувачів.

Таким чином, атаки на відмову використовують певні особливості побудови мережі Інтернет і поставили перед дослідниками суттєву проблему, яка повністю не розв'язана і сьогодні. До головних причин такого стану справ можна віднести велику кількість різнотипних атак, кожна з яких використовує окрему особливість або слабкість програмного забезпечення, протоколу взаємодії або архітектури мережі. Більш того, бурхливий розвиток інформаційних технологій приводить до появи нових типів атак, що вимагає постійної адаптації механізмів захисту. Інша об'єктивна причина полягає у розміщенні системи захисту від атак. Ефективність системи виявлення і протидії, наприклад, фальшування IP адрес (одної з фундаментальних проблем мережі Інтернет) залежить від широти її запровадження. Однак, оскільки всесвітня мережа є децентралізованою і фактично складається з автономних систем, це практично неможливо. Тому системи захисту, як правило, є рішеннями для кінцевого користувача мережі. Такі механізми можуть забезпечувати захист користувача від експлойтних та спрямованих атак, але поглинаючі атаки залишаються загрозою. Це пов'язано з тим, що, при поглинаючій атаці трафік, який потрапляє до комп'ютера жертви, містить пакети атаки і пакети звичайних користувачів. Ефективних механізмів, які б дозволили розрізнити ці пакети, немає.

Ще один недолік існуючих систем захисту полягає у застосуванні при побудові певних припущень про природу трафіка або характеристик функціонування мереж, на яких базується весь механізм захисту (наприклад, про стійкість статистичних характеристик нормального трафіка або про невелику кількість нових IP адрес). Якщо ж ці припущення виявляються неправильними (при появі, скажімо, нового типу атак) то система перестає забезпечувати захист.

Протягом останніх років комп'ютерні системи та мережі постійно розвивались, при цьому кількість користувачів збільшувалась, а сервіси, що їх обслуговують, ускладнювались. Збільшення складності систем підвищило їх вразливість до різного роду вторгнень, зокрема, і до атак на відмову. Поточний розвиток дозволяє припустити, що наступним напрямком буде створення мереж з інтелектуальними компонентами, поведінка яких буде містити елементи автономності й адаптивності. Задачею системи захисту

буде тоді взаємодія з цими компонентами, оцінка загроз і вибір ефективних методів виявлення.

Розвиток алгоритмів виявлення відбувався у відповідь на існуючі загрози. Спочатку це були прості індикатори, що фіксували, наприклад, кількість байт в секунду або кількість відкритих з'єднань. З появою більш складних типів атак відповідно ускладнювались механізми захисту. При цьому відбувалось залучення математичних моделей з області статистики, нейронних мереж та інших. Сучасні системи виявлення атак – це системи прийняття рішення в умовах невизначеності інформації, динамічних змін середовища та можливих загроз. Для визначення аномальних явищ в таких системах використовують складні математичні алгоритми та спеціально побудовані бази знань.

Причини зростання складності пов'язані з різними аспектами. Одна з суттєвих причин – зростання мобільності користувачів. Дійсно, доступність ресурсів мережі для користувачів, що можуть підключатися з різних точок, комп'ютерів робить їх поведінку досить непередбачуваною, оскільки змінюється конфігурація мережі і всі попередньо виміряні характеристики можуть виявитися недостовірними. З іншого боку, поява нових уразливостей і нових типів атак також впливає на зростання складності.

Існуючі системи виявлення використовують, як правило, експертні моделі, статистичні методи або нейронні мережі. При побудові таких систем вважалось, що мережа зафіксована, а її властивості досліджені, і не змінюються протягом роботи системи. Фактично структура моделей для виявлення атак є попередньо визначеною і може змінюватися лише в межах певних параметрів. Однак при появі нових типів атак або аномалій майже завжди моделі потрібно перебудовувати структурно, що вимагає переробки системи захисту.

Ще одним недоліком є архітектура системи, яка наділяє один модуль всією функціональністю щодо оброблення даних і пошуку атак. Такий підхід до побудови розподіленої системи виявлення атак має низку принципових недоліків:

– залежність від однієї точки, якщо комп'ютер з системою захисту всієї мережі буде атаковано або пошкоджено, це спричинить відключення загальної системи;

– обмежена масштабованість системи, оскільки весь аналіз відбувається на одному комп'ютері (це правильно не для всіх систем захисту);

– ускладнена адаптація системи до суттєвих змін середовища, яка зазвичай потребує оновлення бази даних і/або настроювання.

Вимоги до системи безпеки розвиваються відповідно до розвитку мереж. Через необхідність швидкої перебудови системи підвищується важливість гнучкості й адаптивності. Отже, система має задовольняти насамперед таким вимогам.

1. *Адаптивність*. Вимоги до безпеки в організаціях можуть бути різними або змінюватися з часом. Тому при зміні параметрів та настройок системи її функціональність має змінюватись відповідно.

2. *Гнучкість*. Мережа, за якою ведеться спостереження може змінюватися протягом часу. Це може бути спричинене появою додаткових можливостей або ресурсів. Отже, система захисту повинна мати можливість змінювати свою функціональність без перезапуску – в режимі онлайн. Агентні системи можуть забезпечити необхідну гнучкість шляхом встановлення цілей для кожного агента. При змінах відбувається зміна цілей, що не призводить до перезапуску.

3. *Придатність до навчання*. Фундаментальна характеристика, що дозволяє виявляти нові атаки. З огляду атак (розділ 4.) видно, що сценарії атак постійно змінюються, знаходять нові вразливості або схеми здійснення. Пропонується здійснювати навчання двома способами. Перший полягає в заданні адміністратором нових цілей для інтелектуальних агентів. Іншим способом є самонавчання агентів, та використання методів інтелектуальної обробки інформації (видобування знань, статистичних моделей, нейронних мереж тощо).

4. *Розподіленість*. Одною з властивостей мережі є взаємопов'язаність її компонентів. Для успішної роботи потрібна чітка взаємодія всіх складових елементів (роутерів, маршрутизаторів, файлових серверів, окремих комп'ютерів). Нападнику досить здійснити атаку проти однієї з цих ланок, щоб вся мережа або її частина стала враженою. Наприклад, він може затопити мережу фальшивими ICMP запитами від імені третіх осіб. Або спрямувати атаку проти провайдера, що надає Інтернет послуги. Тому система виявлення атаки, побудована на базі кінцевого комп'ютера може виявитись неефективною. Більшої результативності природно очікуваним від проведення розподіленого моніторингу з різних точок мережі.

5. *Автономність*. Для спрощення задачі виявлення атак необхідно виконати розподілення обчислювальних задач за різними вузлами. При цьому значно скоротиться час реагування, але потрібно також створити систему обміну інформацією, яка б дозволила доповнювати виміри вузла даними з інших місць. Інший аспект, пов'язаний з автономністю – це функція делегування. Динаміка процесів у комп'ютерних мережах часто вимагає у відповідь на початок атаки негайне застосування змін у настройках безпеки. Наприклад, чим раніше будуть увімкнені фільтри виявлених фальшованих адрес, тим меншою буде потужність атаки. Тому делегування елементам системи виявлення певних функцій адміністрування системи дозволить значно скоротити час реакції та загальну ефективність системи захисту.

Підсумовуючи все сказане, існує нагальна необхідність розробки системи виявлення і захисту, яка б задовольняла такі вимоги:

– ефективність функціонування: висока надійність виявлення, швидкість роботи, стійкість до фальшивих виявлень;

– масштабованість: розширення або зміна конфігурації системи мають автоматично враховуватися;

– адаптивність: поява нових видів атак або зміна характеристик роботи не має призводити до необхідності перепрограмування системи.

Базою для створення такої системи може бути технологія інтелектуальних агентів, що використовують методи статистичного аналізу та теорії ігор. Підхід інтелектуальних систем для розв'язання складних проблем, зокрема, в області керування комп'ютерними мережами описаний і обґрунтований у багатьох роботах. Багатоагентні системи є мобільнішими, крім того вони мають додаткові особливості, такі як, наприклад, розподіленість, можливість працювати за умов непередбачуваних змін як мережі, так і зловмисної діяльності, виявлення і документування значущих подій, навчання, аналіз зібраної інформації, планування дій, автономність, адаптивність.

Така система суттєво використовуватиме базу стратегій протидії, отриманих при аналітичному моделюванні взаємодії між нападниками та агентами захисту (це моделювання виконують для поглинаючих атак). Дослідження аналітичних моделей дозволяє вивчити ефективність протидії та можливі наслідки. Ігрова постановка тут випливає з самої природи конфліктної взаємодії нападника та системи захисту. Основна величина, на яку впливають гравці – завантаженість системи. Це може бути загальна завантаженість або завантаженість окремих, критичних для роботи системи, вузлів (процесора, оперативної пам'яті, каналів мережі). Позначимо p_i – завантаженість i-го вузла системи, $p = (p_1,..., p_n)$. При цьому будемо вважати, що $p_i \in [0,1]$, де 1 – позначає повну завантаженість, або відмову вузла. Мета команди нападника полягає у максимальному збільшенні хоча б одного з p_i, система захисту намагається, в свою чергу, утримати всі p_i в прийнятних межах і не допустити їх зростання. Оскільки функціонування системи протягом часу також впливає на $p(t)$, то в результаті маємо динамічну керовану систему:

$$p(t_{k+1}) = f(t_k, p(t_k), u(t_k), v(t_k)).$$

Складність описаної системи приводить до необхідності введення певних припущень й ідеалізацій динаміки руху та керувань конфліктуючих груп. Аналіз динаміки та визначення прийнятних стратегій захисту є складними науковими проблемами, вирішення яких створить передумови для забезпечення успішного функціонування системи.

Кібернетичний захист та інші види забезпечення інформаційної безпеки

Відповідно до загальновизнаних світових стандартів і рекомендацій у галузі інформаційної безпеки (зокрема, ITU-T X.1205 (резолюція 181) [5], ISO 27032 [6]), виконання будь-яких заходів у галузі інформаційної безпеки має на меті забезпечення трьох основних станів інформації, яку обробляють, зберігають і передають в інформаційних системах, а саме *цілісності, доступності* та *конфіденційності*.

Згідно з рекомендаціями ISO 27032 [6], кібербезпека займає у сфері інформаційної безпеки позицію, показану на рис. 1.

Рис. 1. Позиція кібербезпеки відносно інформаційної безпеки за ISO 27032

Таким чином, реалізація виключно заходів для забезпечення кібербезпеки не дозволить досягти основної мети – захисту активів від загроз конфіденційності, цілісності та доступності. Це призведе до вразливості інформації, сервісів та взагалі – функціонування кожної галузі, де застосовують інформаційні системи. Опосередкованими наслідками такої вразливості будуть, у свою чергу, значні фінансові та репутаційні збитки в комерційній сфері, зниження обороноздатності держави та збої у функціонуванні державних інституцій – у сфері державного управління.

У роботі зроблено спробу надати відповідь на актуальне питання: яким чином досягти бажаного стану захищеності інформаційних систем та знизити вказані ризики? Саме, запропоновано комплексний підхід, де кібербезпеку розглянуто як одну з невід'ємних складових загального процесу забезпечення інформаційної безпеки організаційних структур довільного рівня складності.

Безпека застосувань як складова кібербезпеки

Із розширенням мережі Інтернет, ростом потужностей обчислювальних систем та підвищенням рівня їхнього інтелекту, рівень кіберзагроз кожний рік підвищується. На даний момент часу ми бачимо багато прикладів реалізації кібератак по всьому світу, що несуть різний ступінь шкоди громадянам, організаціям, та суспільству в цілому.

Інформаційна безпека та кібербезпека багато в чому перетинаються (інформаційна спрямована в першу чергу на безпеку всіх ресурсів організації (в тому числі персоналу), кібер – на безпеку IT ресурсів, що взаємодіють з Інтернет.

В світі немає єдиного стандарту і визначень щодо кібербезпеки, але наприклад, міжнародний стандарт ISO/IEC 27032 вказує, що кібербезпека включає:

– мережний захист;

– захист кінцевих точок;

– захист від методів соціальної інженерії;

– безпеку застосунків.

Ми розуміємо, що основна ціль інформаційної безпеки – захист бізнес-процесів організації, у тому числі кіберресурсів, що працюють з Інтернет.

При будь-якому найкращому захисті мережевому, антивірусному тощо, якщо немає адекватної існуючим загрозам безпеки рівня застосувань, то бізнес-процеси

не захищені, а значить, уся діяльність організації під загрозою.

Протягом останніх років ринок розробки програмних засобів констатує зростання уваги клієнтів до питань інформаційної безпеки, а також певні об'єктивні чинники, що сприяють такій увазі.

До таких чинників ми відносимо: різноманіття платформ розробки, зростання кількості веб-застосунків, постійне зростання мережі Інтернет та відповідних кіберзагроз.

Однією з причин можливих проблем, пов'язаних з ІБ при використанні ПЗ є недосконаліть застосувань в частині протидії сучасним кіберзагрозам, що можуть вести до відмов, неправильної роботи, витокам конфіденційної інформації.

Чому ми говоримо про використання софта саме Українського виробництва?

На діючий час ми маємо багато негативних прикладів використання зарубіжних виробів та систем, як програмних так і апаратних. В багатьох випадках у нас нема гарантій, що за допомогою таких засобів забезпечується надійний захист конфіденційної інформації, унеможливлюються її витоки тощо.

А багато реалізованих кібератак ми просто не бачимо, тому що вони добре масковані або ж у даний час відсутні засоби їх діагностики та протидії. Їх розвиток є складною науковою проблемою, яка розвивається з розвитком методів кібератак.

Практичним підходом у світі в цьому напрямку вже є рішення, що: для захисту державних ресурсів, особливо тих, де обробляється конфіденційна та секретна інформація, застосовувати засоби вітчизняних розробників. Такі засоби зазвичай мають відповідні експертні оцінки, зокрема щодо інформаційної безпеки.

Одним із міркувань, які треба враховувати при експертизі, є необхідність аналізу вихідного коду ПЗ для зниження загроз шпіонажу, витоків тощо.

Але отримання вихідного коду від зарубіжних виробників зазвичай становить дуже важку задачу. В протилежність вітчизняним.

Іншим аргументом у підтримку вітчизняного виробника є зазвичай вбудовані в продукти засоби підтримки криптографії, що відповідає Українським стандартам – ДСТУ.

При використанні імпортних засобів тут можуть виникнути істотні проблеми.

Яка ситуація в Україні? Існуюча законодавча та нормативна база із захисту інформації прямо вказує на викладений підхід. Так, згідно Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" Державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством.

Для створення комплексної системи захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, використовуються засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації.

В процесі державної експертизи, засоби оцінюються на відповідність встановленому профілю послуг безпеки із встановленим рівнем гарантій їх реалізації. Методики оцінки послуг на широко вживаний рівень гарантій Г-2 не використовують аналізу коду, але починаючи з рівня Г-3 такий аналіз проводиться.

Тому ми бачимо такі рекомендації при виборі ПЗ для використання в Україні:

– відомість на ринку, успішне використання у вітчизняних ІС різного рівня;

– наявність експертного висновку в сфері технічного захисту інформації з бажаним рівнем гарантій не нижче Г-3.

Комплексний підхід до забезпечення інформаційної безпеки державних і суспільних інфраструктур

Запропонований підхід є результатом подальшої систематизації й узагальнення практичного досвіду авторів із створення комплексної системи захисту інформації у національній грід-інфраструктурі [7] з урахуванням їх доробку в галузі підтримки прийняття організаційних рішень [8].

Підхід полягає в одночасному та взаємоузгодженому застосуванні:

а) кращих практик, рекомендацій і елементів досвіду з різних аспектів інформаційного захисту [9];

б) різнотипних і різнорівневих організаційних рішень, зокрема:

– кадрових рішень;

– рішень щодо критичних складників Інформаційної інфраструктури;

– рішень щодо сучасних програмних і програмно-апаратних засобів у галузі інформаційної безпеки;

– рішень щодо криптографічного та технічного захисту інформації;

– інженерних рішень;

– експлуатаційних рішень діючих систем;

в) сервісів підтримки прийняття й виконання організаційних рішень.

Сутність підходу показано на рис. 2. Далі стисло схарактеризовано його складники.

Кращі практики, рекомендації та різноаспектний досвід

Аспект інформаційного захисту. Використання рекомендацій профільних стандартів в усіх галузях інформаційної безпеки. Зокрема.

Безпека – це постійний процес. Неможливо «налаштувати інформаційну безпеку» один раз, необхідно працювати і модифікувати засоби, рішення, підходи забезпечення ІБ постійно, з урахуванням нових загроз та набутого досвіду.

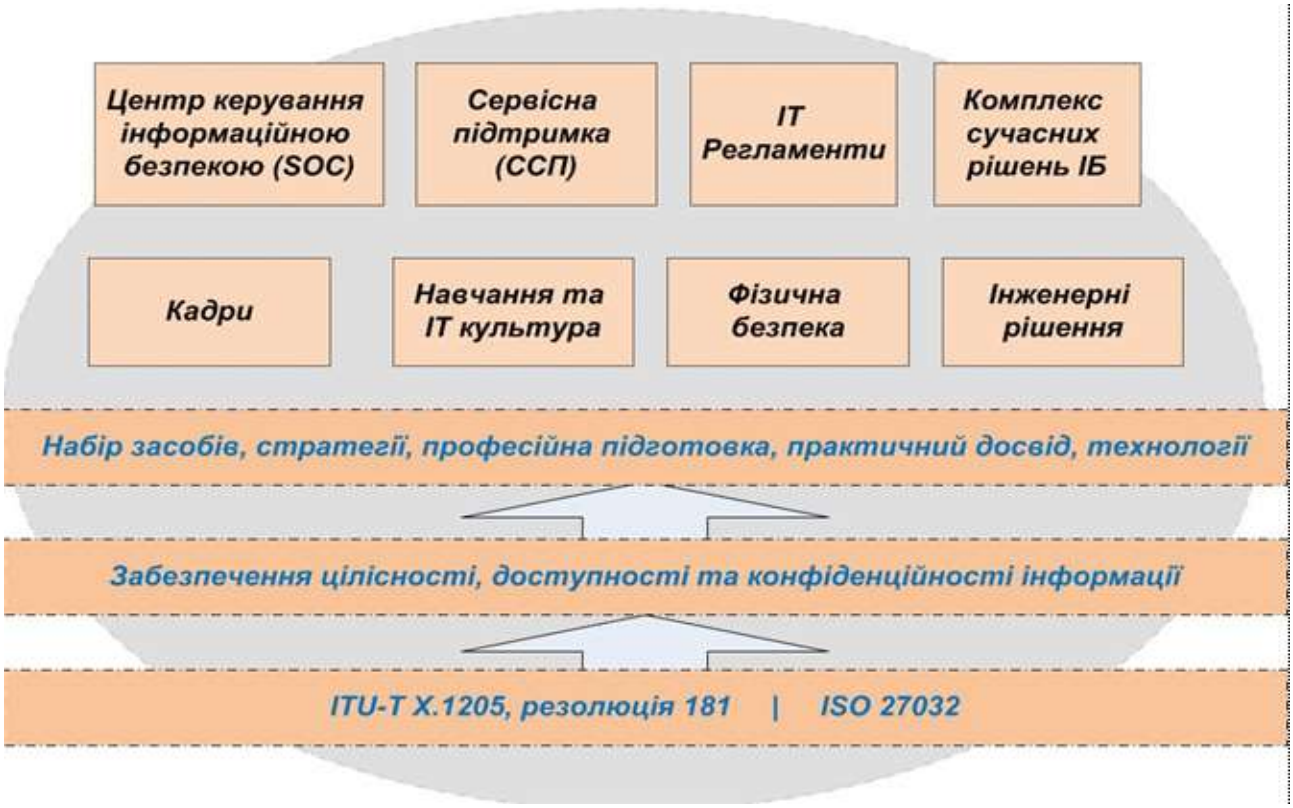

Рис. 2. Засади та складники комплексного підходу до забезпечення інформаційної безпеки (разом з Кібербезпекою) Інформаційної інфраструктури держави

Йде постійна боротьба між зломом (нападом, руйнуванням) і захистом. Засоби нападу і захисту постійно модифікуються і з'являються нові.

Наявність найсучасніших та найактуальніших засобів захисту не виключає необхідність використання інших, «застарілих» рішень і технологій.

Засоби захисту треба ешелонувати. Застосовують два типи ешелонування:

а) одне і те саме рішення на різних рівнях моделі OSI. Наприклад,

– антивірус – на транспортному (L4) і рівні додатків (L7) – на поштовому сервері і робочої станції користувача;

– на робочій станції одночасно встановлені антивірус та рішення класу End-Point-Protection, яке усуває «слабкі місця» та вразливості антивірусу;

б) різні виробники у послідовному з'єднанні. Наприклад,

– різні антивіруси у послідовному ланцюжку поштових серверів;

– послідовне з'єднання міжмережевих екранів від різних вендорів.

Експлуатаційний аспект. Експлуатація – окремий етап життєвого циклу будь якої інформаційної системи, системи кіберзахисту, інформаційної безпеки тощо.

Недостатня увага до організації та забезпечення експлуатації створює загрози інформаційній безпеці.

Сервісна підтримка – одна з ключових складових експлуатації.

Організаційні рішення

На підприємстві, в державній установі або певній галузі народного господарства доцільно застосовувати та постійно оновлювати згідно зі зміною умов відповідні:

– політики,
– регламенти,
– стандарти,
– рекомендації

та інші нормативні правові документи довільних форматів, які дозволяють оформити, легалізувати та ввести в дію відповідні організаційні рішення.

Для спрощення викладу, далі буде застосовано узагальнені терміни: «регламент» і «підприємство».

Регламенти підприємства у галузі Інформаційних технологій та Інформаційної безпеки створюються з метою всебічного забезпечення надання користувачам Функціональних сервісів у першу чергу, а також Базових і Комунікаційних сервісів.

Сервіси усіх типів мають надаватися якісно, постійно, безперервно, надійно, безпечно, захищено. Якість надання сервісів має постійно зростати із плином часу.

Усі складові якості надання сервісів усіх типів мають на меті:

– забезпечення якісного прийняття ефективних управлінських рішень;

– сприяння якісному та результативному виконанню цих рішень на усіх рівнях організаційно-штатної структури підприємства.

Найактуальнішими з точки зору практичного впровадження ефективних систем безпеки Інформаційних інфраструктур, із урахуванням національної специфіки України, є такі організаційні рішення.

1. *Пошук кінцевого користувача сервісу. Цільове проектування*.

Інформаційна інфраструктура сама по собі не потрібна нікому. Важливість інформаційної інфраструктури визначається користувачами та інформаційними сервісами, які ці користувачі використовують.

Окреме важливе значення має інформація, яка обробляється, зберігається та передається в межах Інформаційної інфраструктури (ІІ) підприємства. При цьому вказана ІІ може бути:

– локалізована в межах будівлі;

– локалізована в межах групи будівель (кампусу);

– розподілена по території України;

– мати взаємозв'язки з іншими ІІ в межах України;

– мати взаємозв'язки з іншими ІІ за межами України.

Проектування ІІ та, відповідно, захисту ІІ в кіберпросторі має відбуватись виходячи з реальних потреб кінцевих користувачів відповідних інформаційних сервісів.

Це дозволить ефективно використовувати кошти, отримувати максимальну ефективність від використання ІІ (відповідно розраховувати або оцінювати повернення інвестицій (ROI)) та будувати ефективні системи кібернетичного захисту (оскільки захист буде відповідати реальній цінності ІІ).

2. *Формування ІТ культури персоналу та освіта в галузі ІТ.*

Цінність інформаційної інфраструктури визначається інформаційними сервісами, функціонування яких вона забезпечує.

Цінність інформаційних сервісів визначається цінністю продукції (товарів, послуг тощо), які виробляються підприємством.

Цінність товарів та послуг створюють люди, – персонал підприємства.

Таким чином, у разі відсутності масової ІТ культури персоналу підприємства, навіть найсучасніші та найефективніші ІІ та інформаційні сервіси будуть низько ефективними, а їх кіберзахист недоцільним.

Необхідно планувати та впроваджувати відповідні комплексні та системні заходи для підвищення рівня ІТ культури персоналу підприємства на усіх ланках.

Впровадження в експлуатацію ІІ та відповідних інформаційних сервісів необхідно узгоджувати з рівнем ІТ культури та ІТ освіти кінцевих користувачів ІІ та, відповідно, кінцевих споживачів інформаційних сервісів, які забезпечуються відповідною ІІ підприємства.

3. *Єдина термінологія.* Мета: уніфікувати та погодити термінологію, яка використовується різними підрозділами, організаціями тощо, задіяними у процесах створення, експлуатації, розвитку ІІ.

Проаналізувати та погодити термінологію, яка використовується:

– у різних документах підприємства стосовно ІІ;

– профільних стандартах країн – донорів, країн-партнерів;

– стандартах (українських та світових), хороших практиках, ІТ індустрії тощо.

Створити єдину базу даних термінів, їх визначень та організувати доступ до неї усіх зацікавлених осіб, підрозділів, організацій.

Створити політики, які визначають та зобов'язують профільні підрозділи, організації, співробітників тощо:

– приймати участь у погодженні термінології;

– приймати участь у постійній актуалізації термінології;

– використовувати затверджену та погоджену термінологію у повсякденній діяльності стосовно створення, експлуатації та розвитку ІІ.

4. *Регламент закупівель ІТ проектів.* Мета розроблення Регламенту – підвищення якості ІТ проектів, які створюються, економії бюджетних та інших коштів.

Проаналізувати чинники (пов'язані із: закупівлями ІТ обладнання, Програмного забезпечення, ІТ послуг та робіт), які негативно впливають на якість ІТ проектів.

Розробити організаційно-регламентні заходи для усунення негативного впливу цих чинників.

5. *Регламент гарантійної, післягарантійної й сервісної підтримки ІТ систем (ITIL / ITSM / Service Desk).* Розробити усі необхідні регламенти, політики, інструкції тощо відповідно до рекомендацій ITIL [10]:

– для кожного функціонального сервісу;

– для кожного базового та комунікаційного сервісу;

– для кожної системи, підсистеми, підрозділу, який цього потребує (наприклад, SOC, CERT).

6. *Регламент використання бездротових мереж (WiFi) у структурі підприємства. Порядок контролю виконання*

чинних політик. Завдання та вхідні дані для проектування ІТ регламенту мають включати:

− розробити правила, політики, порядки тощо, спрямовані на упорядкування використання бездротових мереж WiFi у структурі МОУ та ЗСУ;

− організувати постійно діючий та ефективний контроль стану виконання встановлених правил та політик;

− встановити відповідальність навмисних порушників встановлених порядків використання безпровідних мереж (WiFi).

7. *Регламент використання мобільних пристроїв (смартфон / планшет) у структурі підприємства. Порядок контролю виконання існуючих політик*. Завдання та вхідні дані для проектування регламенту.

Розробити правила, політики, порядки тощо, спрямовані на упорядкування використання мобільних пристроїв (смартфонів, планшетів тощо) у структурі підприємства.

Визначити порядки використання у службових цілях власних мобільних пристроїв, службових мобільних пристроїв.

Визначити підрозділи, групи користувачів тощо:

– яким дозволяється користуватися власними мобільними пристроями у службових цілях;

– які мають бути забезпечені службовими мобільними пристроями для виконання службових обов’язків.

Організувати постійно діючий та ефективний контроль стану виконання встановлених правил та політик.

Встановити відповідальність навмисних порушників встановлених порядків використання мобільних пристроїв.

8. *Підхід до побудови Інформаційної інфраструктури в розрізі виробників рішень*. Стратегія побудови Інформаційної інфраструктури у розрізі виробників рішень (у тому числі програмних, програмно-апаратних та апаратних комплексів) [11–13]:

– одновендорний підхід;

– багатовендорний підхід.

9. *Інші регламенти*. Вказаний перелік не є вичерпним. Крім цього, у кожному конкретному випадку необхідно враховувати специфіку підприємства та галузі його діяльності, стан інформатизації, кібербезпеки та багато інших чинників.

Приблизний перелік регламентів, які доцільно розробити, впровадити у діяльності підприємства та забезпечити постійну актуалізацію наведено далі.

Перевірка кіберзахищеності ІТ систем підприємства (Pentest, Penetration testing, Тестування на проникнення).

Реагування на інциденти комп'ютерної безпеки (CSIRT / CERT тощо).

Регламент антивірусного захисту ІТ систем підприємства (ЦАЗІ).

Підходи до побудови ешелонованого захисту інформації.

Резервування, резервне копіювання та відновлення (обладнання, ліній зв'язку, даних, додатків).

Використання АРМ користувача різних типів.

Використання ПЗ на робочих станціях користувачів.

Регламент організації фізичного і логічного доступу до обладнання. Заміна обладнання у рамках виконання гарантійних зобов’язань виробника або за умовами сервісних контрактів.

Регламенти планового технічного обслуговування обладнання.

Забезпечення функціонування системі фізичної безпеки, зокрема:

– організація фізичного доступу до обладнання;

– опечатування комунікаційних шаф, серверів, баз даних тощо;

– системи керування та контролю доступу (СККД);

– охоронна сигналізація;

– системи охоронного відеоспостереження (СВС) контрольованих територій, будівель, у яких розміщені серверні та комунікаційні приміщення, а також безпосередньо у серверних приміщеннях;

– пожежна тривога й пожежогасіння.

Регламент безпечного розміщення серверних і комунікаційних кімнат (фізична безпека та КТЗІ).

Кадрові рішення

Кадрові рішення (система навчання, віддалене навчання – веб конференції, рішення з кадрового забезпечення високопрофесійними фахівцями).

Регламент кадрового забезпечення експлуатації ІТ систем, особливо в державній установі, має бути створений відповідно до завдань з проектування, описаних далі.

Проаналізувати та оцінити ризики, пов'язані із:

– вимогою – мати у штаті підприємства висококваліфікований персонал ІТ фахівців різної спеціалізації, з одного боку;

– рівень заробітної плати фахівця необхідної кваліфікації на державній службі та в комерції відрізняється на порядки (десятки разів), з другого боку.

Запропонувати організаційні заходи щодо:

– організації навчання у структурі підприємства та професійного зростання ІТ фахівців;

– залучення сторонніх висококваліфікованих фахівців до навчання, консультування, та вирішення поточних експлуатаційних завдань;

– системного вирішення питання звільнення ІТ фахівців, які бажають отримувати грошову компенсацію свого фахового рівня відповідно до ринкових умов;

– використання вкладених ресурсів у створення кваліфікованого фахівця, його досвіду, навичок, потенціалу після звільнення фахівця із структури державної установи;

– зменшення ризиків, пов'язаних із звільненням з структури державної установи висококваліфікованого ІТ-фахівця (фахівця з кіберзахисту/ІТ безпеки тощо), який не тільки має фахові навички, але й добре обізнаний з ІТ-рішеннями щодо кіберзахисту/ІТ безпеки, насамперед щодо структури, адресації, реалізованих технічних рішень та алгоритмів (зокрема, формування паролів), слабких місць тощо.

Критичні складові Інформаційної інфраструктури

Критичними складовими Інформаційної інфраструктури є:

– центр обробки даних;

– телекомунікаційна підсистема;

– кінцеві робочі точки (стаціонарні ПК, мобільні ПК, мобільні пристрої).

Перелік критичних складових ІІ підприємства суттєво залежить від галузі цільової діяльності підприємства та багатьох інших специфічних чинників.

Але, у будь-якому разі, для підвищення ефективності ІІ підприємства в цілому та кіберзахисту зокрема, доцільно аналізувати ІІ підприємства, виділяти критичні складові ІІ та планувати їх кібернетичний захист окремо, оскільки інформаційний захист (у тому числі кіберзахист) критичних складових ІІ має певну специфіку.

Комплекс сучасних рішень з інформаційної безпеки

Для реалізації ефективного інформаційного захисту (разом з кіберзахистом) ІІ підприємства необхідно застосовувати всі сучасні рішення (програмні, програмно-апаратні, апаратні) [14–16].

Перелік таких рішень наведено в табл. 1.

Наведений перелік не є вичерпним і може не враховувати певні специфічні особливості конкретного підприємства.

Проте в кожному конкретному випадку доцільно формулювати подібний перелік і визначати політику поетапних:

– аналізу конкурентних рішень, тестування, вибору;

– сайзінгу, бюджетування та поетапної закупівлі;

– інсталяції, впровадження в експлуатацію;

– організації експлуатації, у тому числі сервісної підтримки.

Таблиця 1

Основні сучасні рішення з інформаційної безпеки

Призначення	Склад
1	**2**
Програмне забезпечення пристроїв кінцевого користувача	Операційні системи
	Офісний пакет
	Захист кінцевих точок (End-Point-Protection)
	UTM (Антивірус, Антифішинг, Антиспам, Персональний фаєрвол)
	Стандартне ПЗ (Архіватор тощо)
Обчислювальні потужності та зберігання даних	Сервери
	СЗД
	Віртуалізація СЗД
	Комутація серверів
	Комутація СЗД
	VDI: тонкий / товстий / нульовий клієнт
	АРМ користувача (ПК, Ноутбук, планшет)
	Віртуалізація СЗД
Інформаційна безпека /Кібер-безпека / Безпека критичних інфраструктур	AAA
	WIPS / WLAN
	MDM (BYOD)
	SIEM
	UTM
	WAF
	Захист баз даних (DB)
	PAM
	NGFW
	APT
	DDoS
	DLP
	IDS/IPS Антивірус
	Захист кінцевих точок (End-Point-Protection)
Уніфіковані комунікації (UC)	IP телефонія
	Сервіси UC для підвищення ефективності комунікацій (Presence, click-to-call, довідники тощо)
	Відео- та конференц-зв'язок
Уніфіковані комунікації (UC)	Контакт центр
	Веб-конференції та дистанційне навчання
Телекомунікації	Лінії зв'язку: НСКЗ - для закритої підсистеми
Телекомунікації	Лінії зв'язку: свої волокна від Укртелекому
	Лінії зв'язку: оренда у комерційних українських операторів зв‘язку
	Магістральне обладнання
	Агрегація
	Доступ
	Оптичні модулі

Закінчення табл. 1

1	**2**
	WDM системи
	WAN оптимізація
	WLAN (WiFi)
	NMS (моніторинг, дистанційне керування, резервне копіювання і відновлення конфігурацій, інвентаризація тощо)
	Устаткування приміщення чергової зміни і адміністраторів
	Наскрізний моніторинг
	СКС (LAN / CAN)
	Інші
Фізична безпека ЦОД	СККД (включаючи регламенти доступу і реагування на інциденти фізичної безпеки)
	Відео-спостереження та відео-аналітика
	Охоронна сигналізація
	Пожежна сигналізація та пожежогасіння
	Інші

Реалізація вимог нормативно-правових документів України в галузі криптографічного та технічного захисту інформації має також бути здійснена, якщо діяльність підприємства підпадає під відповідні вимоги [17].

Інженерні рішення

Інженерна інфраструктура має вагомий вплив на стан інформаційної захищеності інформаційної інфраструктури підприємства.

Проте часто відповідному колу питань не приділяють належної уваги й необхідних ресурсів.

Неякісне прокладання та кріплення інформаційних кабелів, відсутність або непрацездатність джерел безперебійного живлення, розташування серверного або комунікаційного обладнання у приміщеннях, які можуть бути затоплені з високою ймовірністю – всі ці та багато інших чинників впливають на доступність інформації та інформаційних сервісів підприємства.

Базовий перелік інженерних рішень наведено в табл. 2.

Таблиця 2

Основні інженерні рішення

Призначення	Склад
Інженерія ЦОД	Комутаційна шафа / стійка
	Структурована Кабельна Система
	Фальшпол ЦОДу (комунікаційного приміщення)
	Кліматичні системи
	Безперебійне електроживлення
	Гарантоване електроживлення
	Безпечне розміщення Серверної / Комунікаційної кімнати (перекриття будівлі, близькість до магістралей водопостачання та відведення, тощо)
	Інші

Експлуатаційні рішення діючих систем та сервісна підтримка

Експлуатація складових систем/підсистем/комплексів інформаційної інфраструктури підприємства має бути визнана важливою частиною життєвого циклу [18, 19].

Вказане рішення має бути документально оформлено, затверджено та всебічно забезпечено.

Відсутність вказаних заходів призводить до збільшення вразливості ІІ підприємства до загроз цілісності, доступності та конфіденційності інформації та інформаційних сервісів, які експлуатуються на підприємстві.

Важливими чинниками якості функціональних сервісів є:

– сервісна підтримка користувачів;

– надійна робота обладнання та програмного забезпечення;

– оперативне відновлення працездатності сервісів у разі збоїв;

– оперативне виявлення проблем у роботі обладнання, програмного забезпечення, каналів зв'язку та інших складових ІТ інфраструктури, які задіяні в організації надання функціональних сервісів.

Забезпечення достатнього рівня якості вимагає відповідного фінансового забезпечення не тільки для закупівлі обладнання, програмного забезпечення, але також і закупівлі послуг підтримки різних типів. Обґрунтування ефективності відповідних витрат, а також візуалізація витрат (особливо на сервісні ІТ послуги) є досить складною та вкрай важливою задачею.

Усі вказані вище та багато інших не менш важливих викликів вже багато десятиліть є вкрай актуальними для багатьох великих компаній, державних установ на світовому рівні. І чим більше розвинена країна, тим складніше та актуальніше постають вказані виклики.

На сьогодні накоплений багатий досвід вирішення вказаних завдань, у тому числі автоматизації відповідних рішень.

Відповідна галузь знань називається «Керування ІТ послугами» (IT Service Management, ITSM).

Сучасний досвід та рекомендації «Гарних Практик» (Best Practice) ITSM викладено в:

– бібліотеці інфраструктури інформаційних технологій (ITIL) [10];

– міжнародних стандартах, які створені на базі (або із використанням) ITIL (наприклад, ISO/IEC 20000) [20];

– моделях та корпоративних стандартах, створених великими світовими компаніями на базі (або із використанням) ITIL (наприклад, MOF [21], рішення HPE IT Service Management [22]).

Основна мета створення та функціонування Служби сервісної підтримки (СС) підприємства – використання передового світового досвіду в галузі ITSM для забезпечення:

– максимально ефективного надання функціональних сервісів користувачам за рахунок забезпечення високого рівня сервісної підтримки на усіх рівнях ІТ інфраструктури підприємства;

– надання можливості керівництву об'єктивно оцінювати ефективність вкладених коштів у розвиток ІТ інфраструктури підприємства.

ССП підприємства складається з:

– регламентів сервісної підтримки;

– засобів автоматизації, рішення класу Service Desk.

Додатковими суміжними системами, які підвищують ефективність роботи ССП є:

– система централізованого моніторингу та керування;

– система проактивного виявлення і локалізації несправностей.

Інтелектуальна інформаційна технологія керівництва кібербезпекою

Як описано вище, організаційним рішенням щодо кіберзахисту властиві змістовна різнорідність, складність взаємозв'язків, слабка передбачуваність наслідків, повторюваність за змінних умов. Разом ці особливості рішень знижують

результативність й економічну ефективність процесів їх вироблення й виконання та керування ними. Тому для опрацювання зазначених особливостей доцільно розподілити описані вище організаційні рішення з одинадцяти рамкових областях [23] і запровадити уніфікований процес їх прийняття й виконання. Для цього запропоновано спеціальний формат реалізації вищеописаного комплексного підходу – інтелектуальну інформаційну технологію всеохоплюючого керівництва кібербезпекою держави (ІІТ ВК).

Призначенням ІІТ ВК є надання автоматизованої підтримки ведення й координації організаційних рішень на етапах високорівневого рамкового циклу виконання програми забезпечення кібербезпеки, показаного на рис. 3.

Рис. 3. Рамковий цикл виконання програми забезпечення кібербезпеки

Згідно з рис. 3, об'єднання показаних етапів у цикл стає можливим завдяки особливостям їх виконання суб'єктами забезпечення кібербезпеки держави [1, 2].

1. Етап *керування ризиками* охоплює їх кількісне й описове оцінювання, огляд інформаційних систем, яких торкаються ці ризики, та створення за результатами оцінювання й огляду потенціалу опрацювання ризиків і розгортання відповідних заходів.

2. Етап *оцінювання безпеки* охоплює кількісне оцінювання її досягнутого рівня, щоб описово схарактеризувати його результативність і повноту порівняно з загальновизнаними потребами цільової діяльності.

3. Етап *удосконалень* охоплює планування вдосконалень кібербезпеки (на відповідному організаційному рівні) за допомогою запровадження нових і підвищення ефективності наявних технологій і процесів.

4. На етапі *створення потенціалу* безпеки визначають і реалізують сервіси й ресурси, які будуть надані технологіями й процесами забезпечення кібербезпеки, уможливлюючи досягнення цілей кібербезпеки в ролі її потенціалу.

5. На етапі *керуючих впливів* застосовують складники створеного потенціалу для опрацювання конкретних проявів неочікуваної поведінки відстежуваних об'єктів інфраструктури, забезпечуючи їх запобігання, виявлення, експертизи або аудитування.

6. Етап *реалізації кібербезпеки* охоплює приведення в дію технологій, процесів, складників потенціалу та керуючих впливів, щоб надати кібербезпеку відповідній організаційній структурі.

7. Етап *описового оцінювання* операцій охоплює вимірювання продуктивності кібербезпеки, щоб усвідомити, які загрози кібербезпеки виникають і наскільки задовільно протидіють їм засоби захисту.

8. Етап *звіту про стан справ* охоплює звітування кібербезпеки, як внутрішнє, відповідно до прийнятих в організаційній структурі каркасів і стандартів, так і зовнішнє для регулюючих органів, органів страхування та інших зацікавлених сторін.

В ІІТ ВК додатково передбачено вдосконалення восьми наведених кроків згідно з новітніми підходами Керування вигодами [24] (кроки 2–8) і Всеохоплюючого керування ризиками [25] (кроки 1, 3, 6–8). Ці підходи поєднано за допомогою Інженерії корпоративних рішень, розробленої за участю авторів [26]. Завдяки цьому забезпечено координацію рішень різних рівнів і типів з реалізації кроків 1–8 (насамперед, регламентних, опціонально повторюваних і ситуативних).

Пропонована ІІТ ВК ґрунтується на таких принципах.

$П_1$. У кожному циклі стратегічного планування визначено/актуалізовано, типізовано й подано:

– об'єкти, заходи, ресурси та агентів діяльності державної системи забезпечення кібербезпеки – у форматі відповідної Онтології діяльності (ОА);

– інформаційні взаємодії агентів – у форматі відповідної Онтології інформації (OI);

– систему регламентних, опціонально повторюваних та інноваційних рішень – в Онтології рішень (OD);

– систему ризиків порушення кібербезпеки – в Онтології ризиків (OR);

– відображення узгодження між концептами різних онтологій для одного класу об'єктів (*MP*).

$П_2$. Початкова типізація концептів онтологій ґрунтується на виокремленні одинадцяти рамкових функціональних областей кібербезпеки [23]:

- адміністрування систем;
- мережна безпека;
- безпека застосунків;
- безпека серверів та пристроїв;
- тотожність, автентифікація та керу-вання доступом;
- захист даних і криптографія;
- моніторинг, уразливості та керування оновленнями;
- постійна доступність, аварійне відновлення та фізичний захист;
- реагування на інциденти;
- керування активами та ланцюги поставок;
- політики, аудит, on-line виявлення тенденцій, тренування.

$П_3$. В онтології *OA* мають бути зафіксовані:

- зацікавлені сторони національної системи кібербезпеки [1, 2] та їх вигоди як концепти відповідних категорій. Вигода – подія, що вірогідний інцидент не відбувся завдяки запобіжним заходам або його наслідки усунуто в мірі, прийнятній для зацікавлених сторін;
- дерево цілей регламентних та опціонально повторюваних рішень, необхідних для досягнення встановлених вигод, з додатковими відношеннями опціонального підпорядкування, вимушення, одночасного досягнення й одночасного недосягнення;
- моделі загроз (*MT*) і порушника кібербезпеки (*MA*);
- систему пріоритетів стосовно об'єктів захисту разом з моделлю цінності інформаційних об'єктів для досягнення цілей організаційної структури (*MP*).

$П_4$. Декомпозицію цілей продовжують, поки кожній з цілей поточного рівня, які стають термінальними, не можна буде зіставити термінальне ділове (програмоване) рішення [27] або, за його усвідомленої недостатності, термінальне експертно-аналітичне (непрограмоване) рішення [28] щодо певного термінального об'єкта в *OA*, причому різні рішення не впливають одне на одне. Ділові й експертно-аналітичні рішення подано їх описами в нотаціях Decision model and Notation (DMN) [27] і Business Process Model and Notation (BPMN) [28] відповідно.

$П_5$. Довільне нетермінальне рішення з реалізації підграфу цілей, не пов'язаних відношенням одночасного невиконання, подано автоматично формованим BPMN-описом спеціального вигляду, завданнями якого є BPMN і DMN-описи термінальних рішень, відповідних термінальним цілям цього підграфу. Процес забезпечення кіберзахисту являє собою систему багаторазово виконуваних у середовищі онтологій *OA*, *OI*, *OD*, *OR*:

– ділових рішень (за допомогою відповідних сервісів);

– експертно-аналітичних рішень (за допомогою сервісів автоматизованої підт-римки етапів їх прийняття й виконання);

– етапів допоміжних процесів керу-вання діловими та експертно-аналітичними рішеннями;

– етапів вкладеного допоміжного процесу експертно-аналітичного оцінювання рівня кібербезпеки, ризиків її порушення та якості формованих рішень.

$П_6$. Кожне експертно-аналітичне рішення приймається з урахуванням його позиції у поточному полі рішень – системі виконаних, виконуваних, формованих і наразі не формованих рішень (ділових та експертно-аналітичних), взаємопов'язаних згідно з онтологією *OD*.

$П_7$. Відповідно до підходу Всеохоплюючого керівництва ризиками [25, 29]

виокремлено чотири типи ризиків порушення інформаційної безпеки. Визначено чотири дедалі складніші режими керування ними, а також основні категорії зацікавлених сторін, яких необхідно залучати до їх опрацювання згідно з рис. 4.

Як показано на рис. 4, визначальною характеристикою типу ризику є:

1) простота – повнота знань про події ризику, вигоди й збитки від наслідків;

2) складність – неповнота знання про чинники й прояви ризику;

3) невизначеність – висока невизначеність другого порядку, усвідомлені межі знання;

4) нечіткість – відсутність усвідомлених меж знання.

Згідно з принципами $П_1$–$П_7$, рамкова модель ІІТ ВК являє собою структурований кортеж:

$$MIC = \langle [\,AS\,];\ [\,Rq\,];\ (\,SM_i\,,\ i{=}1,\ldots,8);$$

$$\langle\, OA, OI, OR, OD\,\rangle;\ \langle\, MT, MA, MP\,\rangle;$$

$$\langle PS,\ MT,\ KPI\rangle;\ \ AT\,\rangle,$$

де AS – передумови її реалізації для деякої організаційної структури певного рівня;

Rq – спеціальні вимоги до виконання вищенаведених рамкових етапів 1–8;

SM_i – модель i-го етапу в об'єднаній нотації BPMN і DMN;

$PS \neq \varnothing$ – відкрита для поповнення множина постановок задач, необхідних для виконання етапів 1–8 за їх моделями SM_i;

$MT \neq \varnothing$ – відкрита для поповнення множина методів розв'язання задач із постановками з множини PS;

$KPI \neq \varnothing$ – відкрита для поповнення множина показників рівня кібербезпеки та ризику;

$AT \neq \varnothing$ – відкрита для поповнення множина інструментальних засобів підтримки виконання етапів 1–8 за їх моделями SM_i.

Для розроблення детальніших технологічних схем для цієї ІІТ може бути корисною портфельна модель процесу прийняття рішень, керованих вигодами, запропонована в [30].

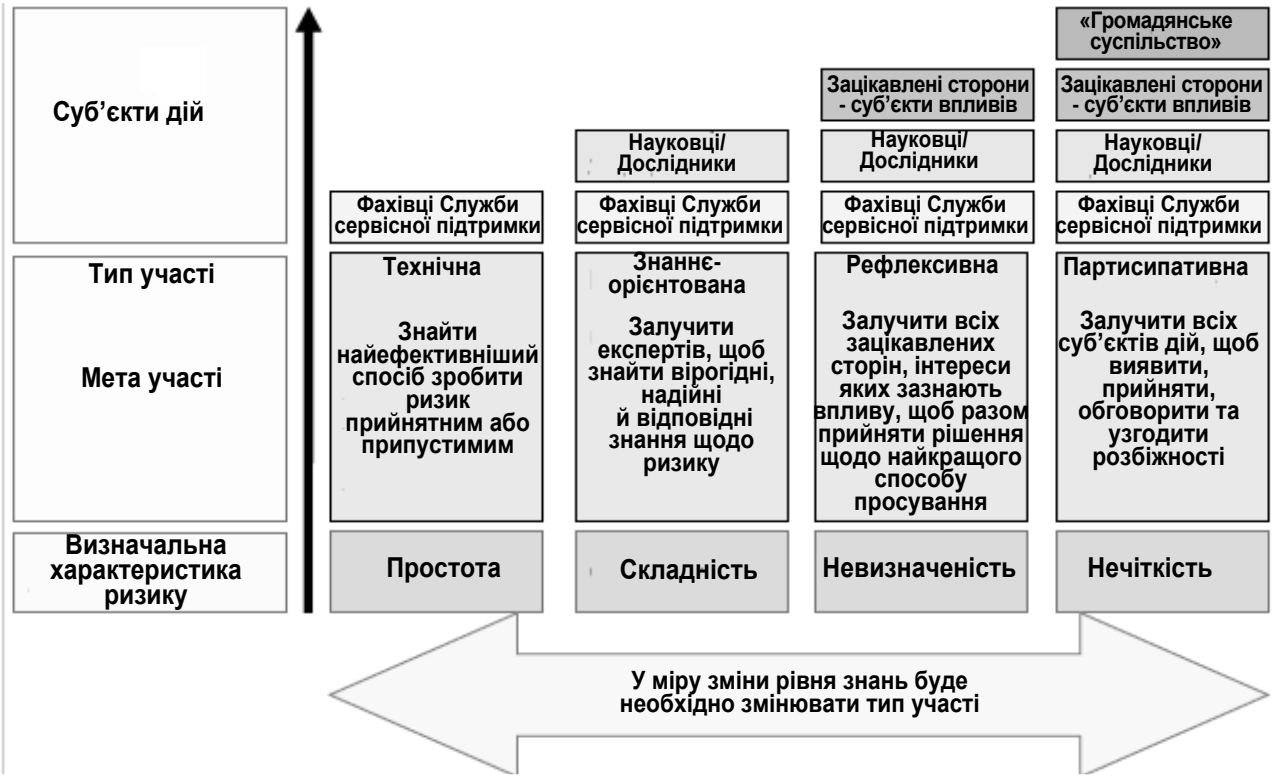

Рис. 4. Сутність залучення зацікавлених сторін в ІІТ ВК відповідно до рівня знань про ризики

Висновки

Проаналізовано поточні тенденції порушень кібербезпеки держави, зокрема зловмисних атак в Інтернет. Поставлено проблему побудови системи кіберзахисту критичної інформаційної інфраструктури держави. Обґрунтовано зростання актуальності цієї системи за поточних соціально-політичних умов. На підставі засадничого ISO 27032 визначено позицію кібербезпеки як базового складника інформаційної безпеки, що об'єднує елементи решти її складників (безпеки мереж, застосунків і роботи в Інтернет), пов'язані з інформаційними (автоматизованими), телекомунікаційними й інформаційно-телекомунікаційними системами.

Надано комплексний підхід до забезпечення інформаційної безпеки певної інфраструктури. Він передбачає взаємоузгоджене прийняття й виконання організаційних рішень з усіх аспектів безпеки та інтелектуальне керування системою цих рішень.

Запропоновано обмеження наданого підходу рішеннями щодо кіберзахисту об'єктів критичної інформаційної інфраструктури держави. Для реалізації обмеженого підходу розроблено Інтелектуальну інформаційну технологію керівництва кібербезпекою. Вона поєднує доробок авторів з автоматизованої підтримки прийняття рішень в організації з новітніми підходами керування вигодами (від належного кіберзахисту) та керівництва ризиками (порушення кібербезпеки).

Виділено основні наукові проблеми, які виникають при розробці та застосуванні розглядуваного комплексного підходу, вирішення яких створить передумови для забезпечення його успішного застосування, зокрема:

– розробка методів діагностики стану мережі з метою виявлення замаскованих кібератак;

– розробка методів аналізу динаміки мережі та стратегій її захисту:

– розробка методів підтримки прийняття рішень щодо застосування засобів кіберзахисту критичної інформаційної інфраструктури держави;

– розробка моделей і методів керівництва ризиками порушення кібербезпеки.

1. Стратегія кібербезпеки України. Затв. Указом Президента України від 15.03.2016 р. № 96/2016. [Електронний ресурс]. Режим доступу: http://www.president.gov.ua/documents/962016-19836.
2. Проект Закону про основні засади кібербезпеки України (реєстр. № 2126а від 14.04.2016 р.). [Електронний ресурс]. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55657.
3. Андон П.І., Ігнатенко О.П. Атаки на відмову в мережі Інтернет: опис проблеми та підходів щодо її вирішення. Препр. Ін-т програмних систем НАН України, 2008. 50 с.
4. Андон П.І., Ігнатенко О.П. Потокові моделі мережі Інтернет за умов атак на відмову. *Проблеми програмування*. 2012. № 2-3. С. 86–96.
5. Визначення та термінологія стосовно побудови довіри і безпеки в застосуванні інформаційно-комунікаційних технологій. Резолюція 181. Міжнародна спілка електрозв'язку. Сектор стандартизації електрозв'язку. Гвадалахара, 2010. 4 с.
6. ISO/IEC 27032:2012 Information technology. Security techniques – Guidelines for cybersecurity. [Електронний ресурс]. – Режим доступу: http://www.iso27001security.com/html/27032.html. 50 p.
7. Загородній А.Г., Боровська О.М., Свістунов С.Я., Сініцин І.П., Родін Є.С. Створення комплексної системи захисту інформаційних ресурсів у національній грід-інфраструктурі України. Вид. «Сталь», Київ. 2014. 374 с.
8. Ильина Е.П., Синицын И.П. Модели и методы поддержки аналитического сопровождения поля решений организации. *Проблеми програмування*. 2017. № 3. С. 93–107.

9. Сторінка команди реагування на комп'ютерні надзвичайні події України. [Електронний ресурс]. – Режим доступу: http://cert.gov.ua/.
10. Сторінка ITIL. [Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/ITIL
11. Elliot B., Fernandez M.M. Single-Vendor or Multivendor UCC: Which Approach Is Best for You? /– Gartner Report ID: G00247556. – 2013, 7 березня. [Електронний ресурс]. – Режим доступу: https://www.gartner.com/doc/2363015/singlevendor-multivendor-ucc-approach-best.
12. [Електронний ресурс]. Режим доступу: http://www.information-age.com/how-internet-things-will-forever-change-data-centre-123458414/.
13. [Електронний ресурс]. Режим доступу: https://www.slideshare.net/SeanLeslie1/debunking-the-myth-of-the-singlevendor-network-gartner-white-paper-2-58388315.
14. Сторінка "Інформаційна_безпека_України". [Електронний ресурс]. Режим доступу: https://uk.wikipedia.org/wiki/Інформаційна_безпека_України.
15. [Електронний ресурс]. Режим доступу: https://www.anti-malware.ru/analytics/Technology_Analysis.
16. Шаньгин В.Ф. Информационная безопасность. М.: ДМК Пресс, 2014. 702 с.
17. [Електронний ресурс]. Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=89740&cat_id=89734.
18. [Електронний ресурс]. Режим доступу: http://libraryno.ru/ekspluataciya-informacionnyh-sistem-infmen/.
19. [Електронний ресурс]. Режим доступу: http://onlanta.ru/services/appmanagement/.
20. [Електронний ресурс]. Режим доступу: https://ru.wikipedia.org/wiki/ISO_20000.
21. [Електронний ресурс]. Режим доступу: https://technet.microsoft.com/en-us/library/cc543224.aspx.
22. [Електронний ресурс]. Режим доступу: https://saas.hpe.com/en-us/software/it-service-management-itsm.
23. Donaldson S.E., Siegel S., Williams C.K., Aslam A. Enterprise Cybersecurity. How to Build a Successful Cyberdefense Program Against Advanced Threats. Apress, 2015. 536 p.
24. Jenner S. Managing Benefits. The new Guidance and Certification Scheme from APMG-International. The Stationery Office, 2012. 297 p.
25. Renn O. Risk Governance: Coping with Uncertainty in a Complex World. Earthscan, 2008. 455 p.
26. Ильина Е.П., Синицын И.П., Слабоспицкая О.А. Создание инженерии корпоративных решений как концепции комплексного управления организацией. Зб. праць десятої міжнар. наук.-практ. конф. "*Математичне та імітаційне моделювання систем. МОДС '2016*". Чернігів, 2015. С. 248–262.
27. Decision Model and Notation (DMN). Version 1.1. Object Management Group, Inc, 2016. – 182 p. [Electronic resourse]. Mode of access: http://www.omg.org/spec/DMN/1.1.DMN 1.1
28. Business Process Model and Notation (BPMN). Version 2.0 Object Management Group, 2011. 538 p. [Electronic resourse]. Mode of access: http://www.omg.org/spec/BPMN/2.0/PDF.
29. Renn O. Coping with complexity, uncertainty and ambiguity:The risk governance approach NSF-DFG Joint Risk Meeting, Washington, D.C., Oct. 3–5, 2012. 33 p.
30. Слабоспицкая О.А. Портфельная модель процесса принятия решений по управлению изменениями в организации. Проблеми програмування. 2015. № 1. С. 72–80.

References

1. Cybersecurity strategy of Ukraine. Approved by Presidential Decree of Ukraine No. 96/2016 dated 15 March 2016. [Electronic resource]. Mode of access: http://www.president.gov.ua/documents/962016-19836.
2. On Basic Principles of Ensuring the Cybersecurity of Ukraine. Draft Law N2126a. [Electronic resource]. Mode of access: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55657.
3. Andon F.I., Ignatenko O.P. Denial of servise attacks on the Internet survey of problems and solutions. Draft Inst. of Softvare Systems of NASU. Kyiv, 2008. 50 p.

4. Andon F.I., Ignatenko O.P. Modeling conflict processes on the internet. Cybernetics and Systems Analysis. 2013. Vol. 49. N 4. P. 616–623.
5. Definitions and terminology relating to building confidence and security in the use of information and communication technologies. Resolution 181. Plenipotentiary Conf. of the Int. Telecom. Union. Guadalajara, 2010. 4 p.
6. ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity. [Electronic resource]. – Mode of access: http://www.iso27001security.com/html/27032.html.
7. Zagorodniy A.G., Borovskaya O.M., Svistunov S.Ya., Sinitsyn I.P., Rodin Ye.S. Complex System Creation for Information Resources Defense over National Grid Infrastructure of Ukraine. «Stal» ed. Kyiv. 2014. 374 p.
8. Ilina E.P., Sinitsyn I.P. Models and Methods for Automated Analytic Support of the organization decisions field. Problems of Programming. 2017. N 3. P. 93–107.
9. Page of Computer Emergency Response Team of Ukraine. [Electronic resource]. Mode of access: http://cert.gov.ua/.
10. Page of ITIL. [Electronic resource]. Mode of access: https://ru.wikipedia.org/wiki/ITIL
11. Elliot B., Fernandez M.M. Single-Vendor or Multivendor UCC: Which Approach Is Best for You? Gartner Report ID: G00247556. 2013, march 7. [Electronic resource]. Mode of access: https://www.gartner.com/doc/2363015/ sing-levendor-multivendor-ucc-approach-best.
12. [Electronic resource]. Mode of access: http://www.information-age.com/how-internet-things-will-forever-change-data-centre-123458414.
13. [Electronic resource]. Mode of access: https://www.slideshare.net/SeanLeslie1/debunking-the-myth-of-the-singlevendor-network-gartner-white-paper-2-58388315.
14. Page “Information Security of Ukraine”. [Electronic resource]. Mode of access: https://uk.wikipedia.org/wiki/Інформаційна_безпека_України.
15. [Electronic resource]. Mode of access: https://www.anti-malware.ru/analytics/Technology_Analysis.
16. Shangin V.F. Information Security. M.: DMK Press, 2014. 702 p.
17. [Electronic resource]. Mode of access: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=89740&cat_id=89734.
18. [Electronic resource]. Mode of access: http://libraryno.ru/ekspluataciya-informacionnyh-sistem-infmen/.
19. [Electronic resource]. Mode of access: http://onlanta.ru/services/appmanagement/.
20. [Electronic resource]. Mode of access: https://ru.wikipedia.org/wiki/ISO_20000.
21. [Electronic resource]. Mode of access: https://technet.microsoft.com/en-us/library/cc543224.aspx.
22. [Electronic resource]. Mode of access: https://saas.hpe.com/en-us/software/it-service-management-itsm.
23. Donaldson S.E., Siegel S., Williams C.K., Aslam A. Enterprise Cybersecurity. How to Build a Successful Cyberdefense Program Against Advanced Threats. Apress, 2015. 536 p.
24. Jenner S. Managing Benefits. The new Guidance and Certification Scheme from. APMG-International. The Stationery Office, 2012. 297 p.
25. Renn O. Risk Governance: Coping with Uncertainty in a Complex World.
26. Ilyina E.P., Sinitsyn I.P., Slabospitskaya O.A. Creating Corporate Decision Engineering as a Concept for Complex Organizational Management. Proc. Tenth Int. Sci.-Pr. Conf. MODS’2015. Chernigov, 2015. P. 248–262.
27. Decision Model and Notation (DMN). Version 1.1. Object Management Group, Inc, 2016. 182 p. [Electronic resourse]. Mode of access: http://www.omg.org/spec/DMN/1.1. DMN 1.1.
28. Business Process Model and Notation (BPMN). Version 2.0. Object Management Group, 2011. 538 p. [Electronic resourse]. Mode of access: http://www.omg.org/spec/BPMN/2.0/PDF.
29. Renn O. Coping with complexity, uncertainty and ambiguity:The risk governance approach NSF-DFG Joint Risk Meeting, Washington, D.C., Oct. 3-5, 2012. 33 p.
30. Slabospitskaya O.A. Portfolio model for decision process concerning organizational change management. Problems in Programming. 2015. N 1. P. 72–80.

Одержано 19.07.2017

Про авторів:

Сініцин Ігор Петрович,
доктор технічних наук,
старший науковий співробітник,
завідувач відділу.
Кількість наукових публікацій в
українських виданнях – понад 90.
Кількість наукових публікацій в
зарубіжних виданнях – 7.
http://orcid.org/0000-0002-4120-0784.

Ігнатенко Петро Петрович,
кандидат технічних наук,
старший науковий співробітник,
заступник завідувача відділу.
Кількість наукових публікацій в
українських виданнях – понад 50.
Кількість наукових публікацій в
зарубіжних виданнях – 2.
http://orcid.org/0000-0001-6546-0936.

Слабоспицька Ольга Олександрівна,
кандидат фізико-математичних наук,
старший науковий співробітник.
Кількість наукових публікацій в
українських виданнях – понад 50.
Кількість наукових публікацій в
зарубіжних виданнях – 5.
http://orcid.org/0000-0001-6556-0947.

Артеменко Олександр Володимирович,
головний конструктор.
Кількість наукових публікацій в
українських виданнях – 5.
http://orcid.org/0000-0002-9443-4154.

Місце роботи авторів:

Інститут програмних систем
НАН України,
03187, Київ-187,
проспект Академіка Глушкова, 40.
Тел.: +38(044) 526 4286.
E-mail: ips@nas.gov.ua,
olsips2017@gmail.com