ЖИТОМИРСЬКИЙ ВІЙСЬКОВИЙ ІНСТИТУТУ ІМЕНІ С.П.КОРОЛЬОВА

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ІНЖЕНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА

здобувача вищої освіти ступеня «бакалавр» заочної форми навчання
за спеціальністю «Кібербезпека»

Тема: «МЕТОД ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ КІБЕРАТАКАМ У КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ КОМУНІКАЦІЙНИХ СИСТЕМАХ»

Виконавець: Віталій МИРОНЯК

м. Житомир

2026

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АС	–	автоматизована система
ГРУ	–	Головне розвідувальне управління Генерального штабу Збройних Сил російської федерації
ЗЗІ	–	засіб захисту інформації
ЗС	–	Збройні Сили
ІКС	–	інформаційно-комунікаційна система
ІС	–	інформаційна система
ІТ	–	інформаційна технологія
КСЗІ	–	комплексна система захисту інформації
МГ	–	метрична група
ОКІ		об’єкт критичної інфраструктури
ОР	–	оцінка (оцінювання) ризиків
ОС	–	операційна система
ОУ	–	об’єкт управління
ОУВ	–	оперативне угрупування військ
ПЗ	–	програмне забезпечення
рф	–	російська федерація
СМІБ	–	системи менеджменту інформаційної безпеки
COBRA	–	Consultative Objective and BiFunctional Risk Analysis (методика аналізу і управління інформаційними ризиками)
CRAMM	–	CCTA Risk Analysis and Management Method (метод аналізу та управління ризиками)
CSSAs	–	cybersecurity situation assessment (оцінка кібербезпеки)
CSSAw	–	cybersecurity situation awareness (інформування кібербезпеки)
CSSE	–	cybersecurity situation evaluation (ситуаційний аналіз кібербезпеки)
CSSF	–	cybersecurity situation forecast (прогнозування кібербезпеки)
CSSV	–	cybersecurity situation value (загальна оцінка кібербезпеки)

ENISA – European Union Agency for Network and Information Security (Агентство Європейського Союзу з питань мережевої та інформаційної безпеки)

IEC – International Electrotechnical Commission (Міжнародна електротехнічна комісія)

$IRAM_2$ – Information Risk Assessment $Methodology_2$ (Методологія аналізу та управління ризиками)

ISO – International Organization for Standardization (Міжнародна організація зі стандартизації)

NIST – National Institute of Standards and Technology (Національний інститут стандартів і технології)

ВСТУП

В умовах ресурсних обмежень економічне зростання країни та забезпечення її конкурентоспроможності на світових ринках не може бути вирішеним без підвищення ефективності інформаційно-комунікаційних технологій, що використовуються в процесі здійснення саме управлінської діяльності. Глобальні зміни, які відбулися останнім часом у світовій економіці внаслідок інтенсивного розвитку інформаційно-комунікаційних технологій та систем, призвели до трансформації бізнес-середовища, прискорили індустріального до інформаційного суспільства. процес переходу від індустріального до інформаційного суспільства.

Аналогічні процеси і проявляються у військовій сфері, зокрема із початком повномасштабного вторгнення російської федерації (рф). Інтенсивність кібератак та кіберінцидентів суттєво зросла, зокрема у національному кіберпросторі зі сторони “мілітаризованих кібервійськ” рф. Протягом першого півріччя 2024 року команда CERT-UA у співпраці з підрозділами Сил Оборони зафіксувала суттєву еволюцію в застосуванні кібератак. У 2022 році ворог здійснював акцент на операціях знищення ІТ-інфраструктур організацій сектору критичної інфраструктури, а також отримання баз даних, списків. Проводилися кампанії проти медіа та комерційних організацій, які все ж не призводили до паніки серед цивільного населення та не створювали ефекту на полі бою. Інформаційні приводи для ворожих “кіберперемог” не давали бажаного довготривалого ефекту, а українські ІТ-системи швидко відновлювалися. У 2023 році їх стратегія поступово змістилася зі знищення інфраструктур організацій, провайдерів послуг Інтернету, міністерств і органів державної влади до закріплення і прихованого отримання інформації та використання кіберкомпоненту для отримання зворотного зв’язку про результати їхніх кінетичних уражень.

Саме тому розроблення методу виявлення та запобігання кібератакам у корпоративних інформаційних комунікаційних системах є актуальним та своєчасним завданням.

РОЗДІЛ 1. ОБҐРУНТУВАННЯ НЕОБХІДНОСТІ РОЗРОБЛЕННЯ МЕТОДУ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ КІБЕРАТАКАМ У КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ КОМУНІКАЦІЙНИХ СИСТЕМАХ

1.1. Поняття та структура корпоративних інформаційно-комунікаційних систем

Терміни та поняття інфокомунікаційних технологій та систем на сьогодні чітко формалізовані та визначені у нормативно-законодавчих актах держави. Такими фундаментальними документами є Закон України “Про Національну програму інформатизації” та “Про публічні електронні реєстри”, які у 2021–2022 роках внесли зміни (редагування) до інших законів: “Про основні засади забезпечення кібербезпеки України”, “Про Національну програму інформатизації”, “Про захист інформації в інформаційно-комунікаційних системах” тощо. Розглянемо деякі з основних визначень та понять у сфері інформаційно-комунікаційних систем.

ІТ – цілеспрямована організована сукупність інформаційних процесів із використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування.

ІКС – сукупність інформаційних та електронних комунікаційних систем, які в процесі обробки інформації діють як єдине ціле.

У популярній науково-технічній літературі використовуються й інші формулювання інфокомунікаційних технологій.

Основними складовими інфокомунікаційних технологій (рис. 1.1) є:

- *Hardware* (*HW*) – апаратне забезпечення, а також все обладнання системи або мережі (стійки, блоки тощо);

- *Microelectronics* (*ME*) – мікроелектроніка (напівпровідникові прилади, інтегральні мікросхеми);

- *Software* (*SW*) – математичне, алгоритмічне та програмне забезпечення (ПЗ), яке визначає математичну базу, алгоритми та програми роботи відповідного обладнання;

- *Computers and Processors* (*CP*) – комп'ютери та процесори, які об'єднують елементи комп'ютерної техніки;

- *Radio technologies* (*RT*) – радіотехнології, які забезпечують застосування радіохвиль для перенесення інформації;

- *Fiber Optics* (*FO*) – волоконно-оптичні лінії зв'язку, які використовують світловоди для передавання інформації на базі оптичного випромінювання;

- *Accumulators and Batteries* (*AB*) – системи електроживлення, які забезпечують якісне та надійне живлення електричних та електронних компонентів;

- *Projects and Design* (*PD*) – комплекси проєктування інформаційно-комунікаційних систем та мереж, які базуються на застосуванні ком-п'ютерної техніки та баз даних.

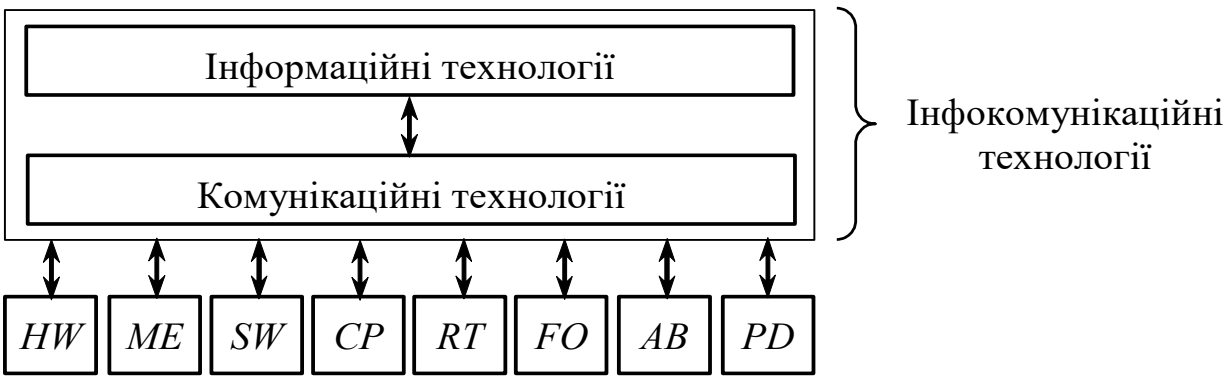


Рисунок 1.1. – Складові інформаційно-комунікаційних технологій

Інші терміни, визначені в законодавстві України, наведені нижче.

Електронна комунікація (телекомунікація) – передавання та/або приймання інформації незалежно від її типу або виду у вигляді електромагнітних сигналів за допомогою технічних засобів електронних комунікацій. Інформаційна (автоматизована) система – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів [1].

Електронна комунікаційна мережа – комплекс технічних засобів електронних комунікацій та споруд, призначених для надання електронних комунікаційних послуг.

1.2. Типи кібератак (кіберзагроз, кіберінцидентів) та аналіз кібератак рф в корпоративних інформаційно-комунікаційних системах

Під час російсько-української війни, яка розпочалась з анексії Криму в 2014 році, ІКС України ставали об'єктами атак з боку рф (табл. 1.1).

Таблиця 1.1

Перелік реалізованих кібератак на ОКІ у період з 2015–2017 років

Найменування кібератаки	Вражені ОКІ	Дата реалізації
BlackEnergy 3	АТ "Прикарпаттяобленерго"	23.12.2015
	ПАТ "Київобленерго"	23.12.2015
	АТ "Чернівціобленерго"	23.12.2015
вірус *Petya*	Аеропорти "Бориспіль", "Харків", "Київ"	27.06.2017
	НЕК "Укренерго", ПАТ "Київенерго", ДТЕК	27.06.2017
	ДСП "Чорнобильська АЕС"	27.06.2017
	КП "Київський метрополітен"	27.06.2017
	Засоби масової інформації	27.06.2017
	АТ "Укрзалізниця"	27.06.2017
	ПрАТ АК "Київводоконал"	27.06.2017
	ДП "Антонов"	27.06.2017
	Оператори мобільного зв'язку	27.06.2017

Так, наприклад 23 грудня 2015 року російським зловмисникам вдалось успішно атакувати комп'ютерні системи управління в диспетчерській "Прикарпаттяобленерго" та вимкнули близько 30 підстанцій, залишивши близько 230 тисяч мешканців без світла протягом однієї-шести годин. Ця атака стала першою у світі підтвердженою атакою, спрямованою на виведення з

ладу енергосистеми. Найбільшою за останні роки є атака на підприємства України вірусу *Petya* у 2017 році, внаслідок якої було призупинено роботу 1/3 українських банків, більш ніж 100 великих підприємств і організацій були вимушені призупинити свою роботу. Країни-члени організації розвідувального альянсу *FVEY*, покладають відповідальність за цю атаку на рф. Від початку повномасштабного воєнного вторгнення росії в Україну Урядова команда реагування на комп'ютерні надзвичайні події *CERT-UA* зареєструвала та дослідила понад 1500 кібератак. Більшість із них – з боку рф.

Серед головних цілей ворожих хакерів – шпіонаж (отримання розвідданих щодо логістики, озброєння, планів та операцій Сил безпеки та оборони), спроби виведення з ладу об'єктів критичної інформаційної інфраструктури, позбавлення доступу громадян до державних послуг та сервісів, банківського обслуговування тощо. А також – інформаційно-психологічні операції та дезінформаційні "вкиди" з метою підриву довіри до спроможностей органів державної влади, Сил безпеки та оборони, поширення панічних настроїв серед населення. Таким чином кіберзагрози, кіберінциденти та кібератаки мають негативне місце у забезпечення кібербезпеки та національної безпеки держави у тому числі [2].

1.3. Аналіз методів визначення ризиків кібербезпеки та запобігання кібератак на інформаційно-комунікаційні системи в національному кіберпросторі.

Відповідно Закону України "Про основні засади забезпечення кібербезпеки України" розглянемо та проаналізуємо ці поняття.

Законодавство України визначає кіберзагрозу як наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів.

Тобто, це будь-які обставини чи події, які можуть бути причиною порушення політики безпеки інформації (нанесення шкоди) автоматизованій системі (АС) або ІКС. Програмну та/або програмно-апаратну спробу реалізації кіберзагрози називають кібератакою.

Відповідно до цього Закону, кібератака – це спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об’єкти кіберзахисту.

Інцидент кібербезпеки (кіберінцидент) – подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактору) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів.

На теперішній час не існує єдиної уніфікованої класифікації кіберзагроз, атак та інцидентів. Однак, на основі аналізу існуючих науково-технічних джерел можна відокремити основні групи кібератак (рис. 1.2): розвідувальні, психологічні, атаки доступу та відмова в обслуговуванні.

Рисунок 1.2. – Класифікація кібератак

Розвідувальні атаки або мережна розвідка – це збір інформації про мережу за допомогою загальнодоступних даних, засобів і додатків. При підготовці будь-якої кібератаки на комп’ютерну мережу кіберзлочинець або інший актор, як правило, проводить мережну розвідку для отримання про неї інформацію (пошук відкритих портів, топологію та склад мережі, цільові *ip*-адреси жертв).

Мережна розвідка проводиться у формі запитів *DNS*, *ICMP*-тестування та сканування портів. Запити *DNS* допомагають зрозуміти, хто володіє тим чи іншим доменом і які адреси цьому домену належать. *ICMP*-тестування адрес, отриманих за допомогою *DNS*, дозволяє визначити, які вузли наявні у мережі. Отримавши список вузлів, кіберзлочинці використовують засоби сканування портів для формування повного списку сервісів, які підтримуються цими вузлами. У результаті отримується інформація, необхідна для іншої кібератаки.

Психологічні кібератаки. Вони націлені на емоційний та психологічний стан людини (страх, радість тощо). Найбільш поширеним видом психологічних кібератак є фішингові (рис. 1.3), які використовуються для отримання автентифікаційних даних доступу до приватних акаунтів (фармінг), електронних скриньок (фішинг), мобільних додатків або платіжних систем (смішинг) тощо. Вішинг – це фішингова атака з використанням голосу та телефонної системи.

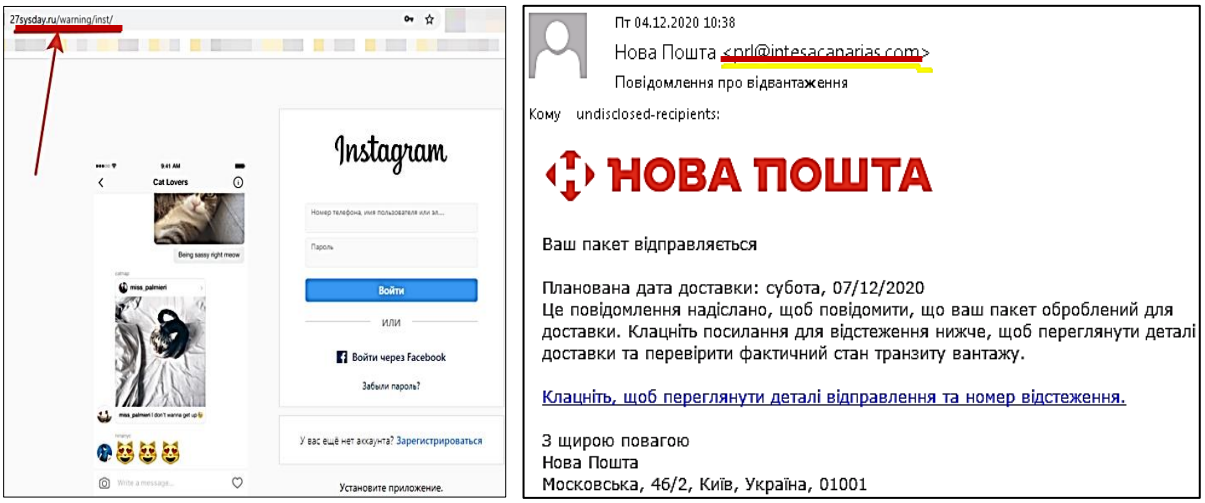


Рисунок 1.3. – Приклади фішингових атак

Третя група кібератак, виходячи вже із назви, націлені на отримання доступу до інформації, АС (або ІКС), кінцевих пристроїв систем тощо. Для отримання (підбору, злому) паролів існує велика кількість програмних засобів, зокрема атака повного перебору, грубої сили (*brute force*) тощо.

Серед кібератак цієї групи виділяють так звану атаку типу “людина в середині” *MITM* (“*Man-in-the-Middle*”). Це мережева атака, завданням якої є додавання стороннього користувача до вже наявного каналу зв’язку між двома системами й отримання доступу до інформації, що передається між ними з можливістю її підміни. Варто зазначити, що у багатьох випадках кібератак застосовуються комбіновано одна з одною.

Атака на відмову в обслуговуванні – кібератака на ІКС з метою зробити інформаційні або мережні ресурси недоступними користувачам, для яких система була призначена. Одним із найпоширеніших методів нападу є насичення атакованого ПК або мережного устаткування великою кількістю зовнішніх запитів (часто безглуздих або неправильно сформульованих) таким чином атаковане устаткування не може відповісти користувачам, або відповідає настільки повільно, що стає фактично недоступним. Якщо атака відбувається одночасно з великої кількості *IP*-адрес, її називають розподіленою *DDoS* (*distributed denial-of-service*). *DoS*-атаки поділяються на локальні та віддалені. До локальних відносяться різні експлойти: форк-бомби

та програми, які відкривають велику кількість файлів або запускають циклічний алгоритм. Віддалені *DoS*-атаки поділяються на два види: віддалена експлуатація помилок в ПЗ та *Flood* (*UDP*-флуд, *ICMP*-флуд, *MAC*-флуд тощо). Крім того існують основні види шкідливого ПЗ: віруси, троянські програми, Інтернет-хробаки, віруси-вимагачі (шантажисти, вимагачі тощо) та інше шкідливе ПЗ (шпигунське, рекламне, підроблене або фальшиве антивірусне ПЗ) та руткіти тощо.

За даними Державної служби спеціального зв'язку та захисту інформації України з початку військової агресії рф була зареєстрована критична кількість DDoS-атак за одну добу – 271. У березні-травні 2022 року кібератаки на енергетичну сферу, логістичну інфраструктуру, сайти українських онлайн-медіа та офіційні державні ресурси продовжувалися.

Варто відзначити, що у ІІ півріччі 2023 року ворожі кіберугруповання різко наростили використання такого інструменту, як розсилання шкідливого програмного забезпечення через електронну пошту. Кількість спроб компрометації таким способом зросла порівняно з першим півріччям 2023 року на 33% (рис. 1.4). Якщо на перше півріччя 2023 року [3] було зафіксовано 285 випадків з переважним використанням фішингових атак, то у другому півріччі було зафіксовано 380, значна кількість яких здійснювалась зі скомпрометованих скриньок, що стало можливим через відсутність двофакторної автентифікації.

Рисунок 1.4 – Аналітика російських кібероперацій за II півріччя 2023 року

Серед атак у другому півріччі 2023 року важливо відзначити численні спроби злому військових систем, зокрема національної військової системи ситуаційної обізнаності Delta, яку використовують Сили безпеки і оборони України. Атаки на мобільні пристрої та ланцюги постачання використовуються значно менше, хоча їх кількість у 2023 році суттєво зросла.

Особливо цікавим є інцидент, коли група хакерів Головного розвідувального управління Генерального штабу Збройних Сил (ЗС) рф (ГРУ) розробила мобільний додаток, який імітував додаток Delta для військових, та опублікувала в Google Play, офіційній платформі для операційної системи(ОС) Android (рис. 1.5).

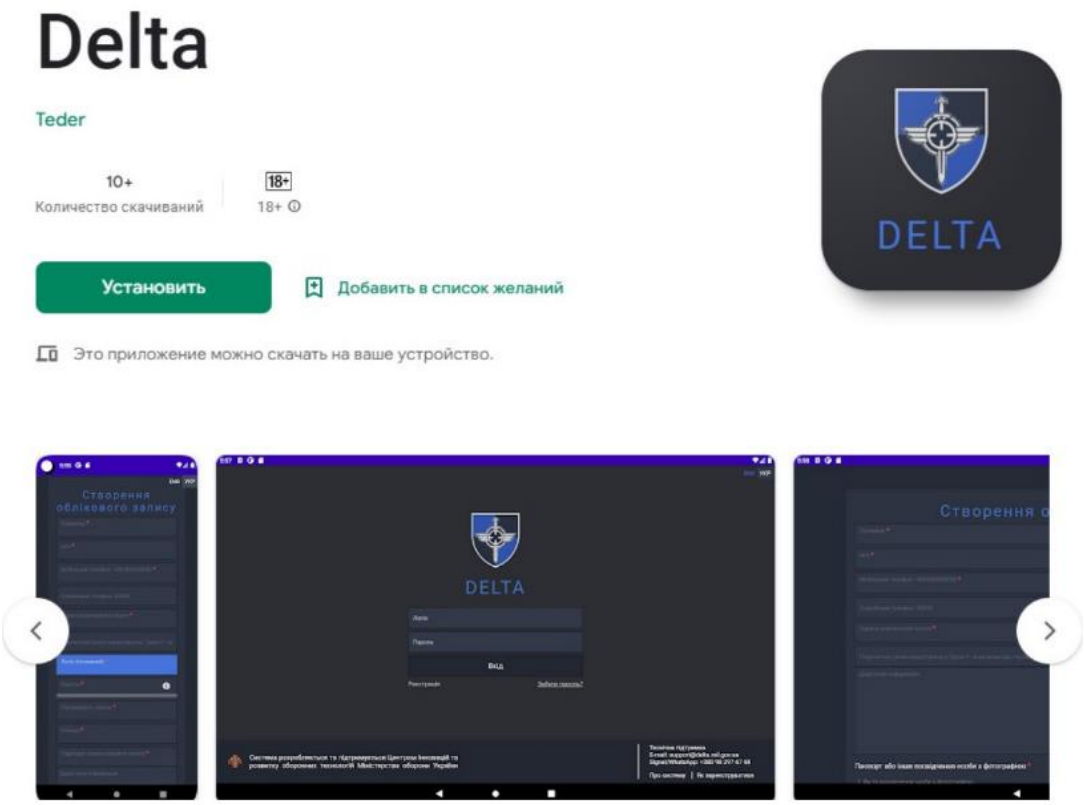


Рисунок 1.5 – Компрометація додатку Delta кібервійськами рф

При цьому хакери ГРУ навіть випередили публікацію справжнього мобільного додатку від розробників Міністерства оборони України. Російські хакери заохочували завантажувати додаток на телефони військовослужбовців та старших офіцерів. Для реалізації таких операцій військовим хакерам необхідно мати значний запас вільних ресурсів, які можна спрямувати на розроблення та розповсюдження мобільних додатків, та мати інформацію про плани військових щодо реалізації застосунка. Тож, очевидно, що ГРУ має суттєвий пул розробників та активно залучає їх для різних операцій імплантації та присутності.

Раніше спостерігалося розповсюдження електронною поштою повідомлення про необхідність оновити сертифікати в системі “DELTA”. Для цього використовували скомпрометовану електронну адресу одного зі співробітників оборонного відомства і месенджери. При цьому долучені до повідомлення PDF-документи, які містять посилання на шкідливий ZIP-архів, імітують легітимні дайджести підрозділу ISTAR оперативного угрупування військ (ОУВ) “Запоріжжя”, які містять посилання на шкідливий ZIP-архів.

Зловмисники використовують домени з довгими іменами і фішинг-сайти для того, щоб здійснити інфікування пристроїв військових, хоча посилання при наведенні на нього курсора виглядало легітимним.

Таким чином, аналіз свідчить, що в національному кіберпросторі спостерігається тенденція збільшення та гібридність кібератак з боку рф. У той же час, варто зазначити, що для протидії кібервикликам створено та активно функціонують відповідні органи.

1.4. Постановка завдання дослідження

Отже, для досягнення поставленої мети даної кваліфікаційної роботи необхідно:

1. Провести деталізований аналіз структури сучасних корпоративних інформаційно-комунікаційних систем, класифікації та типів кібератак (кіберзагроз, кіберінцидентів), а також систематизований та критичний аналіз кібератак рф в корпоративних інформаційно-комунікаційних системах, методів визначення ризиків кібербезпеки та запобігання кібератак на інформаційно-комунікаційні системи в національному кіберпросторі.

2. Розробити структуру методу виявлення та запобігання кібератакам у корпоративних інформаційно-комунікаційних системах із врахуванням:

- виявлення кібератак у корпоративних інформаційно-комунікаційних системах;
- запобігання кібератакам у корпоративних інформаційно-комунікаційних системах з використанням мережевих екранів та антивірусного забезпечення.

3. Провести апробацію розробленого методу виявлення та запобігання кібератакам у корпоративних інформаційно-комунікаційних системах та аналіз її результатів.

Висновки до першого розділу

У першому розділі було проведено аналіз структури сучасних корпоративних інформаційно-комунікаційних систем, класифікації та типів

кібератак (кіберзагроз, кіберінцидентів), а також систематизований та критичний аналіз кібератак рф в корпоративних інформаційно-комунікаційних системах, методів визначення ризиків кібербезпеки та запобігання кібератак на інформаційно-комунікаційні системи в національному кіберпросторі..

Встановлено, що тенденція, яка спостерігається з початку повномасштабного вторгнення, а саме збільшення загальної кількості кіберінцидентів при зменшенні інцидентів високого та критичного рівня, прослідковується і зараз. Одним із найважливіших етапів в забезпеченні кібербезпеки інформаційно-комунікаційної системи є процес виявлення кібератак та розроблення (застосування існуючого) необхідного інструментарію їх запобігання.

Розділ 2. СТРУКТУРА МЕТОДУ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ КІБЕРАТАКАМ У КОРПОРАТИВНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

2.1. Виявлення кібератак у корпоративних інформаційно-комунікаційних системах

Сучасні кібератаки (локальні або віддалені) – це комплекс спрямованих заходів (набір дій та операцій), виконання яких призводить до отримання бажаного кіберзлочинцем результату (злом паролів, отримання конфіденційної інформації тощо). Модель життєвого циклу кібератаки Cyber-Kill Chain описує всі етапи проведення кібератаки. Це класична модель кібербезпеки, розроблена командою реагування на кіберінциденти, які порушують кібербезпеку CSIRT (Computer Security Incident Response Team), яка розроблена компанією Lockheed Martin та опублікована в матеріалах доповіді [4] (рис. 1.6).

Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains

Eric M. Hutchins*, Michael J. Cloppert†, Rohan M. Amin, Ph.D.‡
Lockheed Martin Corporation

Abstract

Conventional network defense tools such as intrusion detection systems and anti-virus focus on the vulnerability component of risk, and traditional incident response methodology presupposes a successful intrusion. An evolution in the goals and sophistication of computer network intrusions has rendered these approaches insufficient for certain actors. A new class of threats, appropriately dubbed the "Advanced Persistent Threat" (APT), represents well-resourced and trained adversaries that conduct multi-year intrusion campaigns targeting highly sensitive economic, proprietary, or national security information. These adversaries accomplish their goals using advanced tools and techniques designed to defeat most conventional computer network defense mechanisms. Network defense techniques which leverage knowledge about these adversaries can create an intelligence feedback loop, enabling defenders to establish a state of information superiority which decreases the adversary's likelihood of success with each subsequent intrusion attempt. Using a kill chain model to describe phases of intrusions, mapping adversary kill chain indicators to defender courses of action, identifying patterns that link individual intrusions into broader campaigns, and understanding the iterative nature of intelligence gathering form the basis of intelligence-driven computer network defense (CND). Institutionalization of this approach reduces the likelihood of adversary success, informs network defense investment and resource prioritization, and yields relevant metrics of performance and effectiveness. The evolution of advanced persistent threats necessitates an intelligence-based model because in this model the defenders mitigate not just vulnerability, but the threat component of risk, too.

Рисунок 1.6. – Фрагмент доповіді Cyber-Kill Chain

Мета моделі полягає у деталізації етапів, через які повинна пройти кібератака для її проведення, та допомогти кіберфахівцям зупинити її на кожному з них.

Модель Cyber Kill Chain (рис. 1.7) складається із 7 етапів (кроків), які виконує зловмисник для успішної реалізації власної кібератаки:

- розвідка (Reconnaissance);
- озброєння (Weaponization);
- доставка (Delivery);
- експлуатація (зараження) (Exploitation);
- встановлення (Installation);
- управління та контроль (Command and Control);
- виконання дій (Actions on Objective).

Рисунок 1.7. – Життєвий цикл кібератак

Аналогічно *Cyber-Kill Chain* у спеціальній публікації *NIST* (*National Institute of Standard and Technology*) “Керівництво щодо оброблення інцидентів в області комп’ютерної безпеки” 800-61, редакція 2 (800-61*r*2), наводяться рекомендації щодо: оброблення інцидентів; аналізу даних, пов’язаних з інцидентом; визначення відповідної відповіді на кожен інцидент.

NIST визначає наступні чотири етапи життєвого циклу процесу реагування на інциденти:


NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-61
Revision 2

Computer Security
Incident Handling Guide

Recommendations of the National Institute of Standards and Technology

Paul Cichonski
Tom Millar
Tim Grance
Karen Scarfone

http://dx.doi.org/10.6028/NIST.SP.800-61r2

Рисунок 1.8. – Публікація *NIST*

Підготовка, на якому створюється та навчається група виявлення та реагування на кіберінциденти, розгортаються інструменти та ресурси, які необхідні для дослідження інцидентів.

На етапі виявлення та аналіз проводиться безперервний моніторинг щодо виявлення, аналізу та перевірки кіберінцидент.

Ізоляція, ліквідація та відновлення. Група *CSIRT* реалізує процедури для ізоляції кіберзагрози та ліквідації впливу на ресурси організації, а також за допомогою резервних копій відновлює дані та ПЗ.

На останньому етапі (дії після інциденту) проводиться документування процесу оброблення інциденту, рекомендування змін для майбутнього реагування та уникнення повторного кіберінциденту.

Забезпечення кібербезпеки та реалізація кіберзахисту проводиться для трьох типів внутрішніх елементів ІКС:

файли, ресурси (рівень даних);

кінцеве обладнання (рівень хоста). Стандартні приклади хостів: ноутбуки, ПК, гаджети, принтери, сервери, IP-телефони тощо.

мережна інфраструктура (рівень мережі). Пристрої інфраструктури локальної мережі з'єднують кінцеві пристрої та, зазвичай, включають комутатори, безпроводові та пристрої IP-телефонії.

Захист на рівні хоста здійснюється з використанням:

антишкідливого або антивірусного ПЗ;

міжмережного екрану на рівні хоста. Персональні міжмережні екрани – це автономні програми, які контролюють вхідний та вихідний трафік на ПК: міжмережний екран Windows; Iptables ОС Linux.

Пакети безпеки на рівні хоста, які включають в себе антивірусні та антифішингові інструменти, засоби безпечного перегляду веб-сторінок, системи запобігання вторгненням на рівні хоста, можливості міжмережевого екрану та функцій ведення мережевих та системних журналів.

Міжмережний (мережний) екран – це комплекс програмних, апаратних (програмно-апаратних) засобів, який реалізовує захист локальних хостів (ПК, ноутбуків тощо) від НСД та атак із зовнішньої мережі, зокрема Інтернет. Встановлюються між зовнішньою та внутрішньою локальною мережами. У науково-технічній літературі зустрічаються інші назви цього терміну, зокрема Brandmauer (брандмауер) та Firewall (фаєрвол). Сам термін "брандмауер" запозичений з німецької мови є аналогом англійського слова "firewall". Обидва терміни означають міжмережний (мережний) екран.

Він призначений для контролю вхідного та вихідного трафіку на хості або в локальній мережі, дозволяє протидіяти практично усім видам мережевих атак, блокувати шкідливе рекламне забезпечення тощо.

Схематично функціонування міжмережного екрану подано на рис. 1.9.

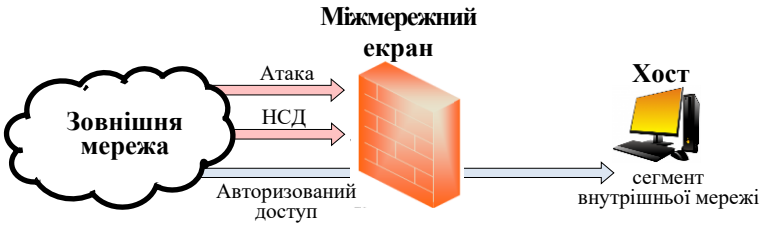


Рисунок 1.9. – Схема роботи міжмережного екрану

Його функціонування полягає в аналізі структури та вмісту інформаційних пакетів, які надходять із зовнішньої мережі, та в залежності від результатів аналізу пропускає їх у внутрішню мережу (сегмент мережі) або повністю їх відфільтровує.

Міжмережні екрани виконують такі функції:

фізичне відділення робочих станцій і серверів внутрішнього сегмента мережі від зовнішніх каналів зв'язку;

багатоетапна ідентифікація запитів, які надходять в мережу;

перевірку повноважень і прав доступу користувача до внутрішніх ресурсів мережі;

реєстрацію запитів до компонентів внутрішньої підмережі із зовнішньої;

контроль цілісності ПЗ і даних;

економію адресного простору мережі (при наявності технології *NAT*);

приховування (трансляція) мережних адрес хостів внутрішньої мережі.

Узагальнена класифікація міжмережних екранів подано на рис. 1.10.

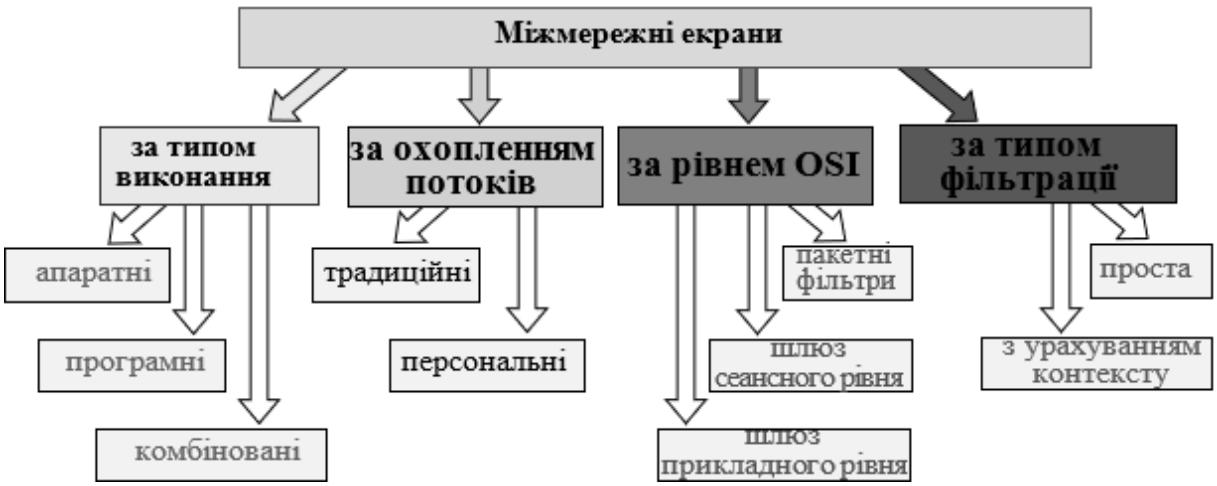


Рисунок 1.10. – Класифікація міжмережних екранів

1. За типом виконання розрізняють: апаратний і програмний. Апаратним міжмережним екраном є пристрій, який фізично підключається до мережі. Цей

пристрій відслідковує всі операції вхідного та вихідного обміну даними, а також перевіряє адреси джерела та призначення кожного повідомлення. Програмний виконує ті ж функції, але використовує не зовнішній пристрій, а програмний продукт, який завантажений на кінцевому хості або шлюзі.

Найбільшого розповсюдження отримав останній тип реалізації.

2. За охопленням контрольованих потоків даних міжмережні екрани поділяються на: традиційні та персональні.

Традиційний мережний екран – ПЗ (або системна складова ОС) на шлюзі (сервері) або апаратне рішення, який виконує контроль вхідних і вихідних потоків даних між підключеними мережами.

Персональний мережний екран – ПЗ, встановлена на хості користувача та призначена для захисту від НСД лише цього комп'ютера.

Популярними персональними мережними екранами є:

ОС Windows – Брандмауер для Захисника Windows (рис. 1.11);

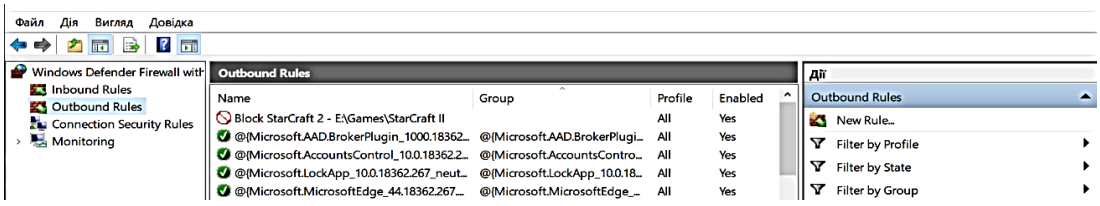


Рисунок 1.11. – Вікно Брандмауера Windows

ОС Linux – Netfilter з утилітою командного рядка iptables.

```
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  lo     any     anywhere             anywhere
    0     0 ACCEPT     tcp  --  any    any     192.168.1.0/24       anywhere             tcp dpt:ssh
    0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:http
   36  3504 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:https
   17  2249 DROP       all  --  any    any     anywhere             anywhere

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 25 packets, 4484 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

Рисунок 1.12. – Правила iptables

Окремим випадком є використання традиційного мережного екрану сервером для обмеження доступу до власних ресурсів.

3. За рівнем моделі OSI, на якому функціонує міжмережний екран, вони поділяються на (рис. 1.13):

на мережному – пакетні фільтри (packet filter);

на прикладному – шлюз прикладного рівня (application gateways);

на сеансному – шлюз рівня з'єднання або сеансного (circuit gateways).

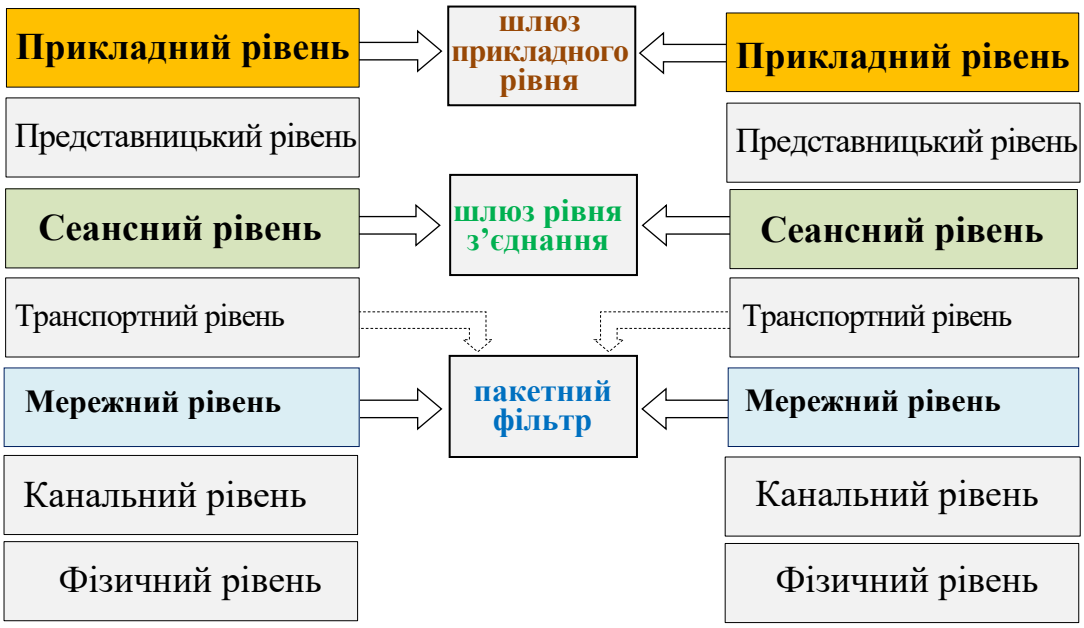


Рисунок 1.13. – Класифікація міжмережних екранів за рівнем моделі OSI

Міжмережні екрани з пакетними фільтрами приймають рішення про те чи пропускати пакет, чи відкинути, аналізуючи IP-адреси, прапорці або номери TCP-портів у заголовку цього пакета.

IP-адреса та номер порту – це інформація мережевого та транспортного рівнів. Водночас, пакетні фільтри використовують також інформацію прикладного, тобто всі стандартні сервіси в TCP/IP асоціюються з певним номером порту.

Міжмережні екрани прикладного рівня використовують сервера конкретних сервісів – TELNET, FTP тощо. Proxy-server, що відносяться до даного сервісу, запускаються на екрані та пропускають через себе весь трафік. Таким чином, між клієнтом і сервером утворюються два з'єднання: від клієнта до міжмережного екрана та від нього до місця призначення.

Використання серверів прикладного рівня дозволяє вирішити важливе завдання – приховати від зовнішніх користувачів структуру локальної мережі, включаючи інформацію в заголовках поштових пакетів або служби доменних імен DNS (Domain Name System).

Сервер рівня з'єднання схожий на міжмережний екран прикладного рівня тим, що вони обидва є серверами-посередниками. Користувач утворює з'єднання з певним портом на екрані, після чого останній з'єднається з місцем призначення.

4. За типом фільтрації (відстеження активних з’єднань) поділяють на:

- stateless (проста фільтрація) – не відслідковують поточні з’єднання, лише фільтрують потік даних виключно на основі статичних правил;

- stateful, SPI (stateful packet inspection) (фільтрація з урахуванням контексту) – з відстеженням поточних з’єднань та пропуском таких пакетів, які задовольняють логіці та алгоритмам роботи відповідних протоколів і програм.

Антивірусне програмне забезпечення (антивірусне ПЗ) – спеціалізоване ПЗ, призначене для виявлення комп’ютерних вірусів, іншого шкідливого ПЗ, відновлення заражених (модифікованих) такими програмами файлів, а також для запобігання зараженню файлів та/або ОС шкідливим кодом.

Антивіруси, виходячи з реалізованого в них підходу щодо виявлення та нейтралізації шкідливого ПЗ, прийнято поділяти на групи (рис. 1.14): детектори (полідетектори), фаги (поліфаги), вакцини, щеплення, ревізори та монітори.

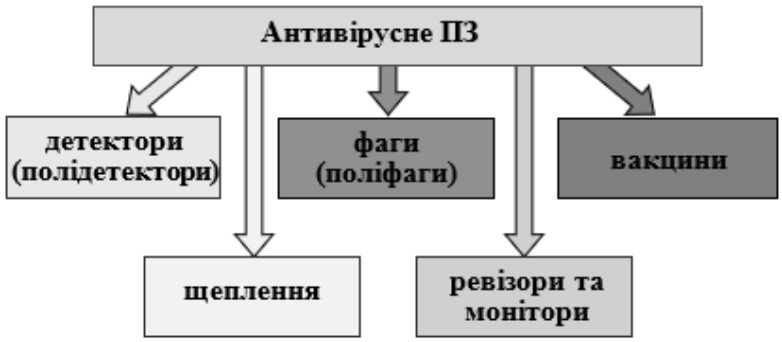


Рисунок 1.14. – Класифікація антивірусного ПЗ

Детектори забезпечують виявлення шкідливого ПЗ за допомогою перегляду виконуваних файлів і пошуку сигнатур (стійких послідовностей байтів, наявних в тілах відомих вірусів). Наявність сигнатури в будь-якому файлі свідчить про його зараження відповідним вірусом. Антивірусне ПЗ, яке забезпечує можливість пошуку різних сигнатур, називають полідетектором.

Фаги виконують функції, властиві детекторам, однак при цьому здатні “виліковувати” інфіковані програми шляхом видалення вірусних сигнатур з їхніх тіл. Аналогічно полідетекторами, фаги, орієнтовані на нейтралізацію різних вірусів, називаються поліфагами.

На відміну від детекторів і фагів, вакцини за своїм принципом дії подібні вірусам. Вакцина імплантується у ПЗ, яка захищається та запам'ятовує низку кількісних і структурних характеристик останньої. Характеристиками, які вакцини використовують, можуть бути довжина програми, її контрольна сума тощо. Принцип дії щеплень заснований на тому, що будь-який вірус позначає інфіковані програми певною ознакою для того, щоб не виконувати їх повторне зараження. В іншому випадку мало б місце багаторазове інфікування, супроводжуване істотним збільшенням обсягу заражених програм, який легко виявляється. Щеплення, не вносячи ніяких інших змін в текст програми, позначає її тією ж ознакою, що й вірус, який, таким чином, після активізації та перевірки наявності зазначеного ознаки, вважає її інфікованою та пропускає в аналізі. Ревізори забезпечують спостереження за станом файлової системи, використовуючи для цього підхід, аналогічно реалізованому в вакцинах. Програма-ревізор в процесі свого функціонування виконує порівняння поточних характеристик виконуваного файлу з аналогічними характеристиками, отриманими в ході попереднього перегляду файлів. Відмінність ревізорів від вакцин полягає в тому, що кожен перегляд виконуваних файлів ревізором вимагає його повторного запуску.

Монітор є резидентним ПЗ, яке забезпечує перехоплення потенційно небезпечних переривань, характерних для вірусів, і запитує у користувачів підтвердження на виконання операцій, наступних за перериванням. У разі заборони або відсутності підтвердження монітор блокує виконання користувацького ПЗ.

Технології (рис. 1.15), які використовуються в антивірусах, поділяються на:

технології сигнатурного аналізу;

технології ймовірнісного аналізу.

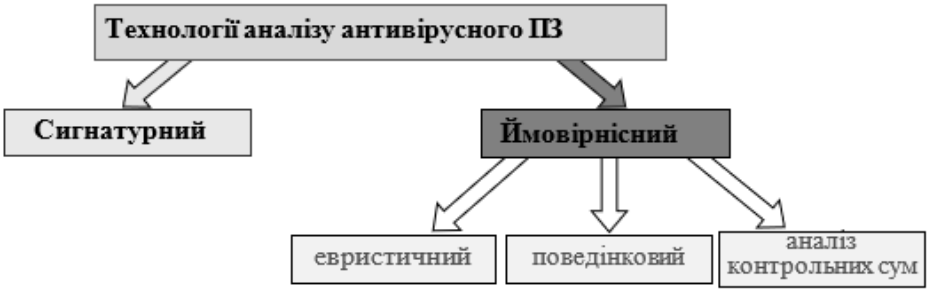


Рис. 1.15. Класифікація технологій антивірусного ПЗ

Сигнатурний аналіз – метод виявлення вірусів, який полягає у перевірці наявності в файлах сигнатур вірусів. Такий аналіз є найбільш відомим методом виявлення вірусів і використовується практично у всіх сучасних антивірусних ПЗ. Для проведення перевірки антивірусного ПЗ необхідний набір вірусних сигнатур, який зберігається в антивірусній базі.

Антивірусна база – база даних, в якій зберігаються сигнатури вірусів.

З огляду на те, що сигнатурний аналіз передбачає перевірку файлів на наявність сигнатур вірусів, антивірусна база потребує періодичного оновлення для підтримки актуальності антивірусного ПЗ. Сам принцип роботи аналізу також визначає межі його функціональності – можливість виявляти лише вже відомі віруси. З іншого боку, наявність сигнатур вірусів передбачає можливість лікування інфікованих файлів, виявлених за допомогою сигнатурного аналізу. Однак, лікування допустиме не для всіх вірусів (трояни та більшість хробаків не піддаються лікуванню за своїми конструктивними особливостями, оскільки є цілісними модулями, створеними для нанесення шкоди).

Технології ймовірнісного аналізу поділяються на категорії: евристичний аналіз; поведінковий аналіз; аналіз контрольних сум.

Евристичний аналіз – технологія, заснована на ймовірнісних алгоритмах, результатом роботи яких є виявлення підозрілих об’єктів.

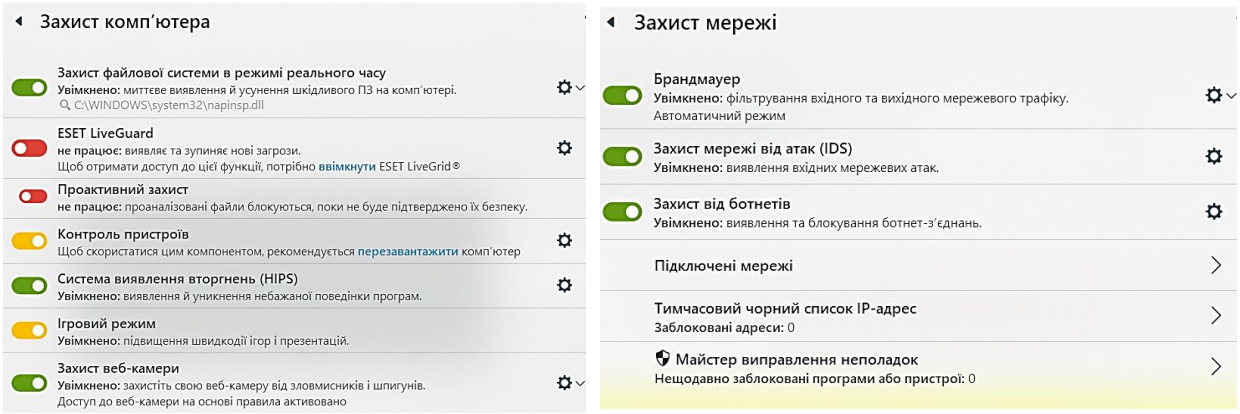
У процесі евристичного аналізу перевіряється структура файлу, його відповідність вірусним шаблонах. Найбільш популярною евристичної технологією є перевірка вмісту файлу на предмет наявності модифікацій уже відомих сигнатур вірусів та їх комбінацій. Це допомагає визначати гібриди та нові версії раніше відомих вірусів без додаткового оновлення антивірусної бази. Поведінковий аналіз – технологія, в якій рішення про характер об’єкта, який перевіряється приймається на основі аналізу виконуваних ним операцій.

Такий аналіз досить вузько застосовується на практиці, так як більшість дій, характерних для вірусів, можуть виконуватися звичайними програмами. Найбільшу популярність здобули поведінкові аналізатори скриптів і макросів, оскільки відповідні віруси практично завжди виконують ряд однотипних дій.

Поведінкові аналізатори не використовують для роботи додаткових об’єктів, подібних вірусним базам та, як наслідок, нездатні розрізняти відомі та невідомі віруси. Аналогічно евристичному аналізу не припускає лікування.

Аналіз контрольних сум – це спосіб відстеження змін в об’єктах. На основі аналізу характеру змін (одночасність, масовість, ідентичні зміни довжин файлів) можна робити висновок про зараження системи.

Аналізатори контрольних сум (“ревізори змін”) аналогічно поведінковим не використовують у роботі додаткові об’єкти. Окрім класичних задач, сучасні антивірусні ПЗ можуть містити модулі для захисту інших компонентів хоста та мережі. Так, наприклад, продукти *ESET*, зокрема версії *Smart Security*, у своєму складі містять функціонали, подані на рис. 1.16.



а) б)

Рис. 1.16. Функціонал ESET Smart Security для захисту:
а) хоста (комп’ютера); б) мережі

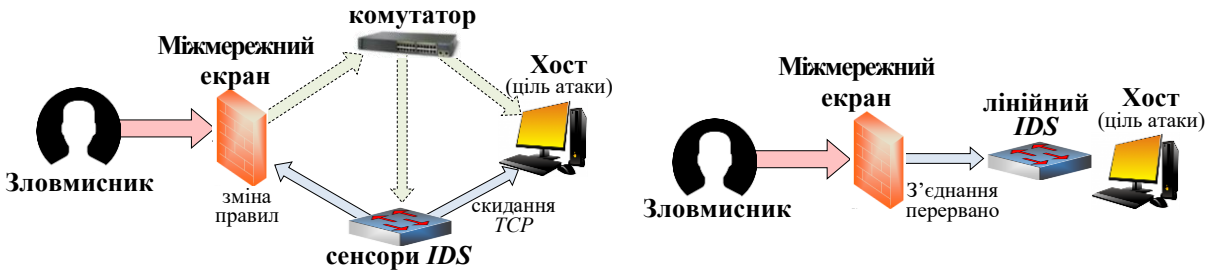
2.2. Запобігання кібератакам у корпоративних інформаційно-комунікаційних системах з використанням мережевих екранів та антивірусного забезпечення

Одним із таких нетипових функціоналів є система виявлення та протидії вторгненням – IDS (Intrusion Detection Systems) та IPS (Intrusion Protection Systems). Системи IPS можна розглядати як розширення систем IDS, так як завдання відстеження атак залишається однаковою. Однак, вони відрізняються в тому, що IPS повинна відслідковувати активність в реальному часі та швидко реалізовувати дії щодо запобігання атак.

Система IDS – програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу до комп'ютерної системи (мережі), або несанкціонованого управління такою системою.

Система IPS – програмна або апаратна система забезпечення безпеки, яка активно блокує вторгнення у випадку їх виявлення.

Архітектура IDS та IPS подана на рис. 1.17.



а) б)

Рисунок 1.17. – Архітектура систем: а) IDS; б) IPS

Системи виявлення вторгнень можна класифікувати:

1. За характером відповідної реакції:

пасивні – системи виявлення, в яких після виявлення та розпізнавання підозрілого трафіку, IDS тільки повідомляє користувача про загрозу;

активні – системи, які протидіють вторгненням, шляхом скидання з'єднання або зміни правил Firewall з метою блокування підозрілого трафіку;

гібридні, які здійснюють виявлення та протидіють вторгненням в автоматичному режимі.

2. За методиками аналізу:

статистичні IDS – системи, які використовують статистичний підхід.

сигнатурні IDS аналізують трафік у мережі або порівнюють пакети з базою даних сигнатур (відомих атрибутів атак). При такому підході основною проблемою є постійне "старіння" баз сигнатур.

гібридна IDS поєднує два та більше підходів для розробки IDS. Дані від агентів на хостах комбінуються з мережею інформацією для створення найбільш повного уявлення про безпеку мережі.

3. За рівнем виявленням атак:

NIDS (Network Intrusion Detection Systems). Система відстежує вторгнення, перевіряючи мережевий трафік і здійснює спостереження за декількома хостами. Мережна система виявлення вторгнень отримує доступ до мережевого трафіку, підключаючись до концентратору або комутатору, налаштованому на дублювання портів, або мережевий TAP-пристрій.

Перевагами NIDS є велике покриття для моніторингу та у зв'язку з цим централізоване управління, також NIDS не впливають на продуктивність і топологію мережі. До недоліків цих систем можна віднести: високе навантаження системи, NIDS потребує додаткового налаштування і функціональності мережевих пристроїв. Системи NIDS не можуть аналізувати зашифровану інформацію та розпізнавати результати атак.

GrIDS (Graph-Based Intrusion Detection System) є удосконаленою версією NIDS. У кожний сегмент локальної мережі встановлюється свій сніфер. Інформація від них збирається разом, аналізується та подається у вигляді схеми інформаційних потоків.

OIDS (Operational Intrusion Detection Systems). Система спеціалізується на внутрішніх атаках. Система порівнює дії конкретного користувача у даний момент часу з його звичайними діями, й у випадку великих розбіжностей видає повідомлення, тобто оцінюється типовість дій (операцій) кожного з користувачів, в той час коли NIDS оцінює типовість трафіку.

HIDS (Host-based Intrusion Detection System). Ця система працює з інформацією, зібраною всередині одного хоста. Таке розташування дозволяє HIDS аналізувати діяльність з великою ймовірністю та точністю, визначаючи тільки ті процеси та користувачів, які мають відношення до конкретної атаки в ОС. HIDS використовують інформаційні джерела двох типів: результати аудиту ОС і системних журналів подій. До недоліків цієї системи відноситься: високе навантаження системи хоста, мале покриття для моніторингу, не мають централізованого управління та вони можуть бути блокованими деякими DoS-атаками або навіть заборонені.

ERIDS (External Routing Intrusion Detection System). Приклад інноваційної та вузькоспеціалізованої системи. Необхідність її створення була обумовлена тим

фактом, що окрім простого та розподіленого способу збору даних про мережі існують менш тривіальні. Наприклад, зловмисник спочатку здійснює атаку на маршрутизатор, змінює його налаштування таким чином, що він направляє трафік через сегмент, який не контролюється та доступний атакуючому.

Існує 5 основних типів сенсорів HIDS:

аналізатори журналів;

сенсори ознак;

аналізатори системних викликів;

аналізатори поведінки програм, служб;

контролери цілісності файлів.

Варто зазначити, що деякі розробники ПЗ пропонують нові функціональні можливості сенсорів HIDS.

Популярними системами з відкритим кодом є Snort, Suricata та OSSEC HIDS, з пропрієтарним – CATNET та McAfee IPS, Cisco Secure IDS, Dragon IDS.

Висновки до другого розділу

У другому розділі було наведено інструментарій необхідний для реалізації методу виявлення та запобігання кібератакам у корпоративних інформаційно-комунікаційних системах. Зокрема подано деталізації персональних мережних екранів та антивірусного ПЗ, а також системи виявлення та протидії вторгнення. Залежно від типу кібератаки, та наслідків їх можливої реалізації, необхідно здійснювати комбінацію їх використання. Забезпечення надійного захисту інформації інформаційно-комунікаційної системи є комплексним завданням, яке включає в себе сукупність задач. Для досягнення мети завдання запропоновано метод, який складається з:

постійний контроль стану мережевих вузлів та каналів зв’язку мережі;

фіксування фактів здійснення кібернетичних атак із детальним описом рівня небезпеки загроз;

постійний контроль доступу користувачів до мереж ІТС;

своєчасне виявлення НСД до мережі ІТС та кіберзагроз, а також оперативна протидія їм.

РОЗДІЛ 3. АПРОБАЦІЯ МЕТОДУ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ КІБЕРАТАКАМ У КОРПОРАТИВНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

3.1. Методика проведення апробації (експерименту)

Методика апробації методу виявлення та запобігання кібератакам у корпоративних інформаційно-комунікаційних системах базується на комплексному поєднанні моніторингу стану мережевих вузлів та активної протидії загрозам на рівні окремого хоста корпоративної системи. В основу методики покладено циклічну модель реагування на інциденти згідно з міжнародним стандартом NIST 800-61r2, яка включає етапи підготовки, виявлення, аналізу, ізоляції та відновлення систем.

Для деталізації процесу виявлення атак використовується модель Cyber-Kill Chain, що дозволяє відстежувати дії зловмисника на кожному з семи етапів: від розвідки до виконання кінцевих дій.

Експериментальне дослідження спрямоване на перевірку ефективності чотирьох ключових компонентів розробленого методу:

- Моніторинг (постійний контроль каналів зв’язку) (рис. 1.18).

Рисунок 1.18. – Етап моніторингу стану вузлів

Постійний контроль мережі передбачає безперервний моніторинг усіх вузлів (серверів, хостів, маршрутизаторів) та каналів зв’язку. Основні задачі, які вирішуються на цьому етапі полягають у перевірці доступності вузлів (ping, heartbeat), аналізі пропускної здатності каналів, контролю затримок (latency) та втрат пакетів, а також виявленні перевантажень мережі.

- детекція (фіксування фактів кібератак з оцінкою небезпеки) (рис. 1.19). Це процес документування всіх підозрілих або шкідливих подій. При цьому фіксується:

- тип атаки (DDoS, brute force, malware);

- джерело (IP-адреса);

- час події;

- рівень небезпеки (низький, середній, високий) тощо.

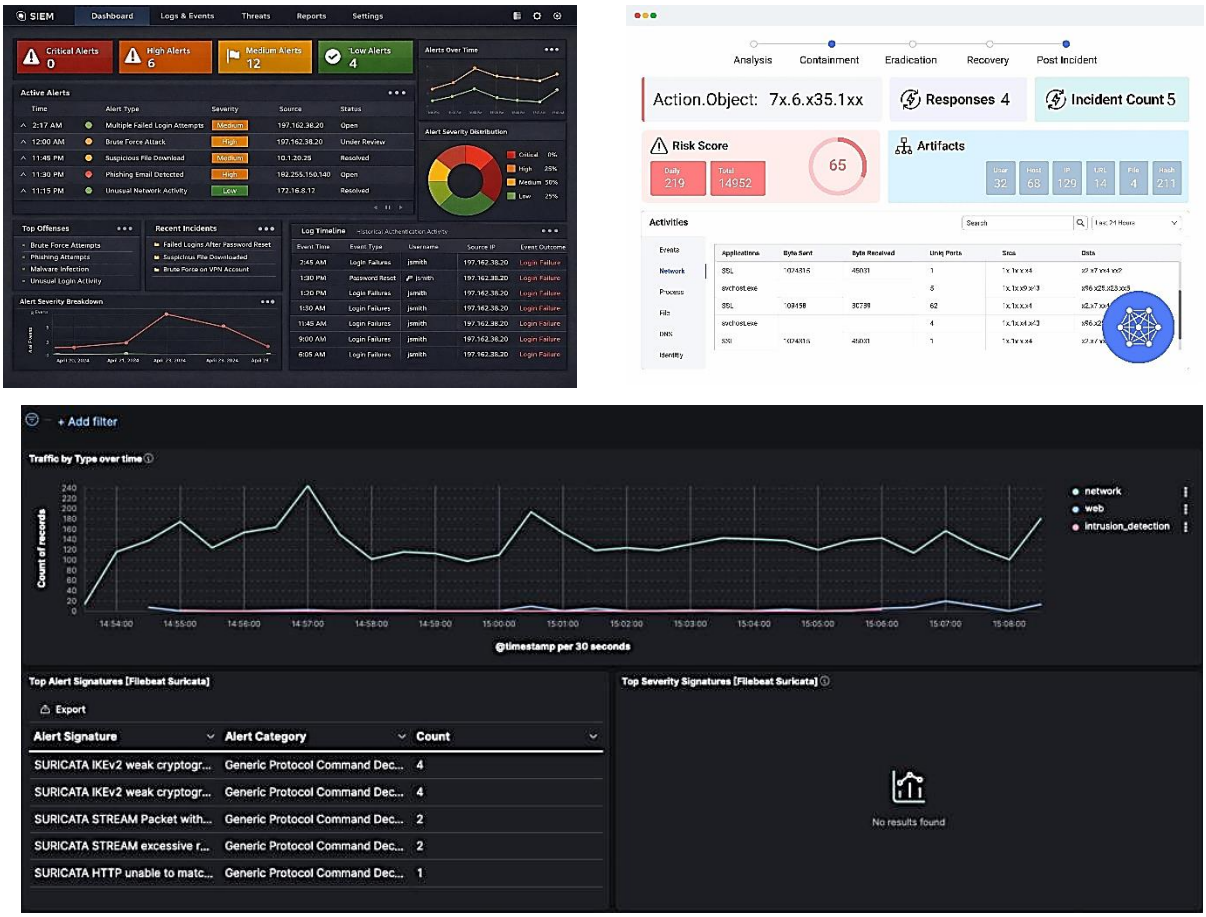


Рисунок 1.19. – Етап детекції кіберзагроз

- авторизація та аудит (контроль доступу користувачів) (рис. 1.20). Контроль доступу – це перевірка того, хто і як підключається до мережі.

Можливі варіанти реалізації:

- ESET HIPS контролює запуск програм, блокує несанкціоновані дії.

- мережеві засоби (мережеві екрани) фіксують входи в систему, аналізують підозрілі спроби входу тощо.

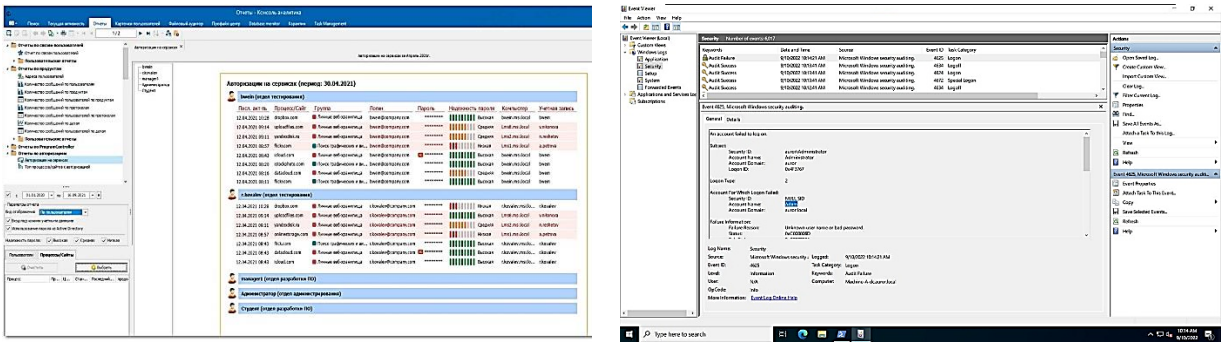


Рисунок 1.20. – Етап аудиту мережі (хоста)

- реагування (оперативна протидія НСД, кіберзагрозам) (рис. 1.21). Основні задачі на етапі є: виявлення вторгнень, аналіз поведінки користувачів та негайне блокування атак. Засоби необхідні для реалізації цих задач

- ESET Smart Security (HIPS) аналізує поведінку програм, блокує підозрілі дії (наприклад, доступ до реєстру).

- Wireshark фіксує підозрілий трафік, здійснює сканування портів, виявляє потенційно можливий витік даних.

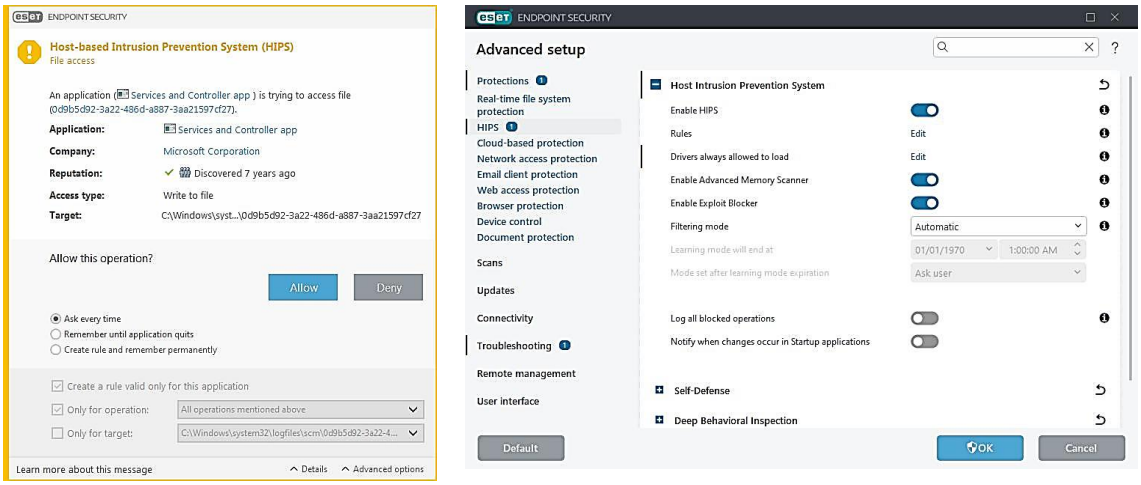


Рисунок 1.21. – Етап реагування на кіберзагрози

3.2. Початкові дані та умови проведення апробації (експерименту)

Об’єктом апробації виступає локальний хост (персональний комп’ютер), інтегрований у корпоративну мережу з виходом в глобальну Інтернет.

Склад системи (об’єкту дослідження):

-Апаратне забезпечення (Hardware): кінцеве обладнання (ПК/ноутбук) із мережевим адаптером;

- Програмне забезпечення (Software): Операційна система (Windows/Linux) із встановленим комплексом захисту ESET Smart Security;

Засоби захисту та аналізу (інструменти реалізації методу):

- система виявлення вторгнень на рівні хоста (HIPS), яка забезпечує моніторинг активності процесів та блокування небажаної поведінки програм;

- аналізатор мережевого трафіку Wireshark, що виконує роль сенсора для глибокого аналізу пакетів (Deep Packet Inspection) у реальному часі.

Умови експерименту передбачають моделювання типових кібератак (сканування портів, DDoS-атаки, спроби впровадження шкідливого ПЗ), що дозволяє перевірити роботу як сигнатурного, так і ймовірнісного (евристичного та поведінкового) аналізу антивірусного ПЗ та систем виявлення та протидії вторгненням.

.

3.3. Аналіз результатів апробації (експерименту)

Результати апробації аналізуються через призму чотирьох основних етапів методики.

1. Постійний контроль стану мережевих вузлів та каналів зв’язку мережі Під час експерименту за допомогою Wireshark здійснювався безперервний моніторинг вхідного та вихідного трафіку. Основна увага приділялася перевірці доступності вузлів (ping, heartbeat) та аналізу затримок. Використання технології SPI (Stateful Packet Inspection) дозволило фільтрувати пакети з урахуванням контексту з'єднання. Наприклад, система пропускала лише ті TCP-пакети, які відповідали логіці встановленої сесії, автоматично відсікаючи аномальні запити.

2. Фіксування фактів здійснення кібератак із детальним описом рівня небезпеки загроз Система захисту успішно документувала всі підозрілі події. Критеріями фіксації були: тип атаки (DDoS, brute force, malware), джерело (IP-адреса) та час події.

Низький рівень: Виявлення мережевої розвідки (сканування портів) через Wireshark. Середній рівень: Спроби доступу через атаку “людина в середині” (MITM). Високий рівень: Виявлення спроб модифікації системних файлів вірусами-вимагачами (типу Petya) за допомогою евристичного аналізу ESET.

3. Постійний контроль доступу користувачів до мереж ІКС На цьому етапі перевірялася робота персонального міжмережного екрана. Контроль доступу включав аутентифікацію та авторизацію запитів. Використання Proxy-server на прикладному рівні моделі OSI забезпечило приховування внутрішньої структури мережі та IP-адрес хостів від зовнішнього сканування. Система фіксувала невдалі спроби входу, класифікуючи їх як спроби атаки методом “грубої сили” (brute force).

4. Своєчасне виявлення НСД до мережі ІТС та кіберзагроз, а також оперативна протидія їм Ключовим інструментом активного захисту виступила система HIPS. На відміну від пасивних систем (IDS), HIPS не лише повідомляла про загрозу, а й автоматично блокувала її.

Приклад дії: При спробі шкідливої програми внести зміни до реєстру Windows або відкрити несанкціоноване мережеве з’єднання, HIPS миттєво перехоплювала системний виклик і блокувала процес.

Ефективність: Поведінковий аналіз дозволив виявити загрози, що не мали сигнатур у базі, забезпечуючи захист від атак “нульового дня”.

Висновки до третього розділу

Апробація підтвердила, що поєднання Wireshark (як інструменту глибокого аналізу) та ESET HIPS (як системи активного захисту) забезпечує повний цикл безпеки: від моніторингу до оперативного блокування атак. Запропонований метод дозволяє мінімізувати ризики порушення конфіденційності та цілісності інформації в корпоративних системах навіть в умовах інтенсивних кібератак.

ВИСНОВКИ

У кваліфікаційній роботі розв’язано актуальне науково-практичне завдання щодо розроблення та апробації методу виявлення та запобігання кібератакам у корпоративних ІКС в умовах зростання інтенсивності загроз у національному кіберпросторі. На основі аналізу структури сучасних корпоративних ІКС встановлено, що забезпечення їхньої безпеки вимагає комплексного захисту на трьох рівнях: даних, хоста та мережевої інфраструктури. Досліджено еволюцію кіберзагроз з боку рф, яка змістилася від операцій зі знищення ІТ-інфраструктури до тривалого прихованого шпигунства та використання кіберкомпонентів для підтримки кінетичних операцій. Систематизовано класифікацію кібератак, виокремлено основні групи: розвідувальні, психологічні, атаки доступу та відмови в обслуговуванні (DoS/DDoS). Встановлено, що найбільш критичними для сучасних систем є атаки типу “людина в середині” (MITM), фішинг та впровадження складного шкідливого ПЗ. Обґрунтовано використання моделі Cyber-Kill Chain для деталізації етапів кібератаки, що дозволяє фахівцям з безпеки ефективно зупиняти зловмисника на кожному з кроків: від розвідки до виконання кінцевих дій. Також інтегровано рекомендації стандарту NIST 800-61r2 щодо циклічного процесу реагування на інциденти, який включає підготовку, виявлення, ізоляцію та відновлення систем.

Запропоновано структуру методу захисту, що базується на поєднанні засобів фільтрації трафіку (SPI-технології), сигнатурного та ймовірнісного (евристичного та поведінкового) аналізу. Основу методу складають чотири етапи: постійний моніторинг стану вузлів, документування фактів атак з оцінкою рівня небезпеки, контроль доступу користувачів та оперативна протидія несанкціонованому доступу (НСД).

Практична апробація методу на прикладі локального хоста із використанням ESET Smart Security (HIPS) та аналізатора трафіку Wireshark підтвердила його високу ефективність. Експериментально доведено, що використання системи HIPS дозволяє активно блокувати підозрілу активність програм у реальному часі, а поведінковий аналіз забезпечує виявлення загроз

“нульового дня”, які не мають сигнатур у базах. Поєднання глибокого аналізу пакетів та персональних міжмережних екранів дозволяє мінімізувати ризики порушення конфіденційності та цілісності інформації навіть в умовах інтенсивних кібератак.

Таким чином, мети кваліфікаційної роботи досягнуто, а запропонований метод може бути рекомендований для впровадження в корпоративні системи для підвищення загального рівня кіберзахисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кібербезпека інформаційно-комунікаційних систем. Частина 1. Комп'ютерні мережі : навчальний посібник / [І. В. Гуменюк, О. В. Самчишин, А. О. Жуков, І. Г. Кошева]. – Житомир : ЖВІ, 2022. – 180 с.

2. Державна служба спеціального зв'язку та захисту інформації України. Російські кібероперації: Аналітика за І півріччя 2024 року. URL: https://cip.gov.ua/ua/news/cyber-operations-rf-h1-2024-report.

3. Державна служба спеціального зв'язку та захисту інформації України. Російські кібероперації: Аналітика за ІІ півріччя 2023 року. URL: https://docs.google.com/viewer?url=https://cip.gov.ua/services/cm/api/attachment/download?id=64621&embedded=true&a=bi.

Risk management – Risk assessment techniques: IEC 31010:2019 [Чинний від 06.2019]. – Женева: [б.в.], 2019. – (Міжнародні стандарти ISO/IEC).

4. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII (редакція від 04.04.2024, підстава – 3549-IX): станом на 15 берез. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 15.03.2024).

5. Онищенко С. В., Глушко А. Д. Аналітичний вимір кібербезпеки України в умовах зростання викликів та загроз // Економіка і регіон № 1 (84), Полтава : Національний університет ім. Юрія Кондратюка, 2022. С. 13–20.

6. Onyshchenko, S., Yanko, A., Hlushko, A. and Sivitska, S. (2020), "Conceptual principles of providing the information security of the national economy of Ukraine in the conditions of digitalization", International Journal of Management (IJM). Volume 11, Issue 12. P. 1709–1726.

7. Microsoft Special Report: Ukraine. An overview of Russia's cyberattack activity in Ukraine. April 27, 2022.

8. Служба безпеки України. Результати СБУ з початку повномасштабного вторгнення рф. URL: http://ssu.gov.ua/zabezpechennia-informatsiinoi-bezpeky (дата звернення: 10.04.2024).

9.

10. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР (редакція від 04.04.2024, підстава – 3549-IX): станом на 15 квітн. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/80/94 (дата звернення: 15.04.2024).

11. О. Г. Корченко, С. В. Казмірчук, Б. Б. Ахметов, Прикладні системи оцінювання ризиків інформаційної безпеки. Монографія, Київ, ЦП "Компринт", 2017 – 435 с.

12. Савельєв Д. В. Методи оцінки ризиків кібербезпеки об'єктів критичної інформаційної інфраструктури // Моделювання та інформаційні технології. зб. наук. пр., Київ : ІПМЕ ім. Г. Є. Пухова НАН України, 89, 2019. С. 136–149.

13. Вілюха Ю. І. Кількісне оцінювання рівня небезпеки кібернетичних загроз інформаційно-телекомунікаційної системи // Сучасні інформаційні технології у сфері безпеки та оборони № 3(30), Київ : НУОУ ім. І. Черняховського, 2017. С. 9–13.

14. Common Vulnerability Scoring System version 4.0. User Guide. Document Version: 1.0. URL: https://www.first.org/cvss/v4-0/cvss-v40-user-guide.pdf (дата звернення: 06.05.2024).

15. Sorting algorithm. URL: https://en.wikipedia.org/wiki/Sorting_algorithm (дата звернення: 06.05.2024).

16. Рейтинг Ело. URL: https://uk.wikipedia.org/wiki/ Рейтинг_Ело (дата звернення: 22.05.2024).