УДК 004.236.13

В.В. Ліпінський, А.А. Кулько, Є.О. Толюпа

ВПЛИВ КІБЕРНЕТИЧНИХ АТАК НА ІНФОРМАЦІЙНУ СИСТЕМУ

У статті розглянуто засоби виявлення кібернетичних атак, що забезпечують одержання даних з мережі про зловмисну активність в зрозумілу інформацію, яка може бути використаний для усунення підтверджених порушень безпеки. Деталізовано можливості використання апаратних засобів віддзеркалення загроз, які дозволяють адміністраторам централізовано знаходити, визначати пріоритетність і відображати загрози за допомогою вже упроваджених в інфраструктуру мережевих пристроїв і пристроїв захисту.

Ключові слова: Запобігання кібератакам, сигнатурний метод, системи виявлення атак, забезпечення безпеки автоматизованих систем.

Вступ. Кібербезпека являє собою стратегічну комплексну проблему будь-якої держави, яка передусім стосується економіки країни, особливо електронної промисловості, в тому числі питань розвитку інфраструктури електронних комунікацій, технологій кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури, визначення заходів щодо боротьби з кіберзлочинністю та кібертероризмом тощо. Адже поняття кібербезпеки є багатоаспектним, і його можна розглядати з різних аспектів – політичного, філософського, технічного, економічного, правового, соціального.

Метою кіберзахисту залишається запобігання будь-яким кібератакам, які можуть бути як цілеспрямованими, так і абстрактними. До цільових кібератак можуть належати групові або окремі напади на об'єкти певної критичної інформаційної інфраструктури. Серед **хакерських атак на Україну 2017 року можна виділити** масштабну хакерську атаку, що відбувалась у декілька етапів. Розпочалась щонайменше 14 квітня 2017 року з компрометації системи оновлення програми M.E.Doc. Останній етап, з використанням різновиду вірусу Petya, відбувся 27 червня 2017 року, та спричинив порушення роботи українських державних підприємств, установ, банків, медіа тощо. Внаслідок атаки була заблокована діяльність таких підприємств, як аеропорт Бориспіль», ЧАЕС, Укртелеком, Укрпошта, Ощадбанк, Укрзалізниця та низки інших великих підприємств. Жертвою вірусу також стали телеканал «Інтер», медіахолдинг ТРК «Люкс», до складу якого входять «24 канал», «Радіо Люкс FM», «Радіо Максимум», різні інтернет-видання, а також сайти Львівської міської ради, Київської міської державної адміністрації. Трансляції передач припинили канали «Перший автомобільний» та ТРК «Київ».

28 червня 2017 року Кабінет Міністрів України повідомив, що атака на корпоративні мережі та мережі органів влади була зупинена.

Основна частина. Масштабна деструктивна атака різновидом вірусу Petya (також відомого як NotPetya, Eternal Petya, Petna, ExPetr, тощо) стала можливою завдяки компрометації системи оновлення програми M.E.Doc та встановлення прихованого бекдору. Таким чином, масштабною деструктивною атакою зловмисники закрили собі наявний в них завдяки бекдору доступ до комп'ютерів та комп'ютерних мереж у близько 80 % українських підприємств (в тому числі - представництв закордонних компаній). Є підстави вважати, що зловмисники пішли на такий крок оскільки або здобули надійніший доступ до інформаційних систем важливих для них жертв, або ж вважають, що зможуть доволі просто відновити його.

Кібератаки можуть здійснюватися автоматично, при цьому може бути атаковано велику кількість жертв, а дедалі більш тісний зв'язок між інформаційними системами через Інтернет та інші інфраструктури створює умови для зниження ефективності каналів телекомунікації та інших важливих стратегічних об'єктів. Слід зазначити, що завдяки виявленим кіберінцидентам світова спільнота стала обізнаною щодо необхідності підвищення спроможностей забезпечення безпеки автоматизованих систем управління технічними та виробничими процесами.

Україна досі залишається принципово уразливою у сфері використання сучасних ІТ, і не останню роль у цьому відіграє надмірно широке запровадження іноземних програмних

продуктів та використання матеріально-технічної бази іноземного виробництва. Саме тому актуальними є проблеми створення національної операційної системи, відновлення вітчизняних потужностей з виробництва матеріально-технічної телекомунікаційної бази (особливо для потреб закритих відомчих інформаційних систем), стимулювання з боку держави створення національного антивірусу.

За таких умов діяльність держави має бути спрямована, передусім, на розробку вітчизняної інноваційної продукції, що може бути використана з метою посилення кібербезпеки; запобігання правопорушенням та їх припинення у сфері державної безпеки у вітчизняному кіберпросторі; запобігання втручанню у внутрішні справи нашої держави і нейтралізації посягань на її інформаційні ресурси з боку інших держав та угруповань; розширення технічних і технологічних можливостей, наукового та людського потенціалу державних органів, які відповідно до покладених на них завдань безпосередньо виконують функції щодо забезпечення безпеки кіберпростору України; координацію заходів щодо забезпечення кібербезпеки її суб'єктами відповідно до їх призначення та повноважень.

Як показує практика заходів, які приймаються в сфері кіберзахисту держави, на сьогодні виявляється недостатньо. Випадки кібератак в Україні і далі продовжують рости. Причиною цього безумовно є те, що поряд з військовими діями на Сході, проти України ведеться повномасштабна кібервійна. Відповідно до експертних висновків, за більшістю кіберзлочинів в нашій державі стоять російські спецслужби, які намагаються всіляко нанести шкоду, та вивести з ладу найважливіші об'єкти інфраструктури України.

На жаль, на сьогодні доводиться констатувати, що правоохоронним органам рідко вдається передбачити кібератаки та попередити державні органи про можливі кіберзагрози. Їх діяльність більше нагадує «гасіння пожеж», аніж їх недопущення. Таку обставину можна пояснити відсутністю необхідної кількості кваліфікованих кадрів в правоохоронних органах, невеликим рівнем підготовки діючих спеціалістів в сфері кібербезпеки, неконкурентною оплатою їх праці в порівнянні з їх цивільними колегами.

Також є проблеми й в такому важливому процесі, як співробітництво спеціальних структур з приватним бізнесом, який має власний досвід і напрацювання протидії кіберзагрозам. Загалом, які б не створювалися умови для «чистого» використання інтернет-простору, та все ж основна боротьба з кібервикликами залежить від самих громадян, які часом легковажно відносяться до захисту персональної інформації. Дуже часто зазначені дані перехоплюються в публічних місцях із відкритим Wi-Fi доступом під час користування електронною поштою або соціальними мережами.

Для попередження таких випадків спеціалісти радять користуватися засобами захисту інформації, які пропонуються поштовими серверами або соціальними мережами. Проте найкращим захистом від викрадення персональних даних в Інтернеті є наявність в ньому мінімальної інформації про себе, або ж взагалі її відсутність. В свою чергу, користувачам платіжних карток слід дотримуватись елементарних засобів безпеки – не розголошувати PIN код стороннім особам та періодично змінювати його.

В свою чергу, на державному рівні питання кіберзахисту повинне набути системного характеру. Можна довго говорити про важливість і актуальність посилення регулювання на національному та міжнародному рівнях діяльності в кіберпросторі і зростання ролі в цьому приватного сектора; встановлення контролю над кіберзброєю, а також посиленням охорони критичної інфраструктури України; впровадження інновацій в сфері кібербезпеки та активізація дискусій щодо пошуку нових джерел фінансування засобів кібербезпеки; вдосконалення освітніх напрямів підготовки фахівців даної сфери діяльності; активізацію на національному та міждержавному рівнях обмін інформацією про кібератаки, тощо.

Джерелами кібернетичних загроз можуть бути міжнародні злочинні групи хакерів, окремі підготовлені у сфері інформаційних технологій злочинці, іноземні державні органи, терористичні та екстремістські угруповання, транснаціональні корпорації та фінансово-промислові групи тощо. Зростає загроза використання кібернетичних засобів як з середини держави, так і з-за меж її кордонів. Такою ж реальною є загроза використання інформаційної

інфраструктури держави як транзитного майданчика для приховування атаки на інформаційну інфраструктуру третьої сторони [3].

Україна послідовно виходить з того, що кібернетичний простір є відкритим простором, відкритим до інновацій, вільного розповсюдження ідей, інформації та обміну думками. Заходи із забезпечення кібернетичної безпеки жодним чином не можуть суперечити принципу гарантування прав та свобод українських громадян, в тому числі права на недоторканність приватного життя та свободи спілкування.

Системи виявлення мережевих вторгнень і виявлення ознак кібератак на інформаційні системи вже давно застосовуються як один з необхідних рубежів оборони інформаційних систем. Розробниками систем захисту інформації та консультантами в цій галузі активно застосовуються такі поняття (перенесені з напрямку забезпечення фізичної та промислової безпеки), як захист по периметру, стаціонарна і динамічний захист, стали з'являтися власні терміни, наприклад, проактивні засоби захисту.

На сьогодні системи виявлення вторгнень і кібератак зазвичай являють собою програмні або апаратно-програмні рішення, які автоматизують процес контролю подій, що відбуваються в інформаційній системі або мережі, а також самостійно аналізують ці події в пошуках ознак проблем кібербезпеки. Оскільки кількість різних типів і способів організації несанкціонованих проникнень в чужі мережі за останні роки значно збільшилася, системи виявлення кібератак (СВКбА) стали необхідним компонентом інфраструктури безпеки більшості організацій.

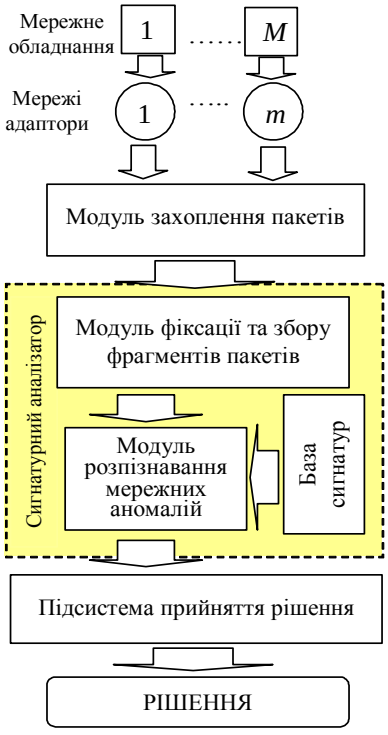

Рис. 1. Структура сигнатурного аналізатора

Взагалі кажучи, сучасні системи виявлення вторгнень і кібератак ще далекі від ергономічних і ефективних, з точки зору безпеки рішень. Підвищення ефективності ж слід ввести не тільки в області виявлення зловмисних дій на інфраструктуру захищених об'єктів інформатизації, але і з точки зору повсякденної експлуатації цих засобів, а також економії обчислювальних та інформаційних ресурсів власника даної системи захисту.

Якщо говорити безпосередньо про модулі обробки даних, то, кожна сигнатура кібератаки в системі обробки інформації про кібератаку є базовим елементом для розпізнавання більш загальних дій - розпізнавання фази кібератаки (етапи її реалізації). Саме поняття сигнатури узагальнюється до деякого вирішального правила. А кожна кібератака навпаки розбивається на набір етапів її проведення. Чим простіше кібератака, тим простіше її виявити і більше з'являється можливостей щодо її аналізу.

Розглянемо один з ефективних методів виявлення вторгнень та кібератак, який основується на сигнатурному підході (рис. 1). Сигнатурні методи дозволяють описати кібератаку набором правил або за допомогою формальної моделі, в якості якої може застосовуватися символьний рядок, семантичне вираження на спеціальній мові й т.п. Суть даного методу полягає в використанні спеціалізованої бази даних шаблонів (сигнатур) кібератак для пошуку дій, що підпадають під визначення "кібератака".

Сигнатурний метод може захистити від вірусної або хакерської кібератаки, коли вже відома її сигнатура (наприклад, незмінний фрагмент тіла вірусу) і вона внесена в базу даних СВКбА. Тобто, коли мережа переживає перший напад ззовні, перше зараження ще невідомим вірусом і в базі просто відсутня сигнатура для його пошуку, сигнатурної СВКбА не зможе сигналізувати про небезпеку, оскільки вважатиме атакуючу діяльність легітимною.

Більшість існуючих програмних продуктів, які заявляють про використання сигнатурного методу, на самому ділі реалізують якраз найбільш примітивний спосіб сигнатурного розпізнавання. Багато систем позиціонуються як призначені для виявлення кібератак в інформаційних системах на основі інтелектуального аналізу мережевих пакетів. Насправді ж сигнатурний метод реалізований як алгоритм, який досліджує лише динаміку розвитку кібератаки, заснований на автоматі станів для оцінки сценарію розвитку атаки. За задумом такий підхід повинен дозволити відстежити динаміку розвитку кібератаки відповідно до дій зловмисника, при цьому в якості модуля збору даних можуть використовуватися навіть самі системи виявлення кібератак.

Таким чином, ефективність роботи сигнатурної СВКбА визначають три основні чинники: оперативність поповнення сигнутарної бази, її повнота з точка зору визначення сигнатур кібератаки, а також наявність інтелектуальних алгоритмів зведення дій атакуючої сторони до деяких базових кроків, в рамках яких відбувається порівняння з сигнатурами.

Системи виявлення атак, як і більшість сучасних програмних продуктів, повинні задовольняти ряду вимог. Це і сучасні технології розробки, і орієнтування на особливості сучасних інформаційних мереж і сумісність з іншими програмами. Щоб зрозуміти, як правильно використовувати СВКбА, потрібно чітко представляти, як вони працюють і які їх вразливі місця.

Якщо не враховувати різні несуттєві інновації в області виявлення комп'ютерних атак, то можна сміливо стверджувати, що існують дві основні технології побудови СВКбА. Суть їх полягає в тому, що СВКбА володіють певним набором знань про методи вторгнень, або про нормальному поведінці спостережуваного об'єкта.

Системи виявлення аномального поведінки засновані на тому, що СВКбА відомі деякі ознаки, що характеризують правильне чи допустиме поведінку об'єкта спостереження. Під нормальним або правильним поведінкою розуміються дії, виконувані об'єктом і не суперечать політиці безпеки.

Традиційно СВКбА класифікуються відповідно до двох характеристик: методу виявлення й рівня системи на якому здійснюється захист. І не дивлячись на те, що ці дві класифікаційні ознаки є найважливішими при виборі систем виявлення атак, все ж існують й інші характеристики які відіграють не менш важливу роль у проектуванні СВКбА. Адже найбезпечніше рішення не може бути досягнуто при розгляді одного чи двох аспектів таксономії. Всі розробники систем виявлення атак і організації, які використовують СВКбА повинні розуміти і вивчати їх класифікацію, щоб вибрати кращі рішення для систем захисту інформації. При дослідженні різних аспектів таксономії і застосуванні різних варіантів ми зможемо досягти більш високого рівня безпеки інформаційних систем.

Датчики пристроїв кібервторгнень ідентифікують незвичайну поведінку, аномалії у функціонуванні окремого об'єкта - труднощі їх застосування на практиці пов'язані з нестабільністю самих об'єктів, що захищаються й взаємодіючих з ними зовнішніх об'єктів. Як об'єкт спостереження може виступати мережа в цілому, окремий комп'ютер, мережева служба, користувач і т.д. Датчики спрацьовують за умови, що вторгнення порушують нормальне функціонування інформаційної системи.

Заходи та методи, що традиційно використовуються у виявленні аномалії, включають в себе наступне:

- порогові значення: спостереження за об'єктом виражається у вигляді числових інтервалів. Вихід за межі цих інтервалів вважається аномальною поведінкою. Пороги можуть бути статичні й динамічні (тобто змінюватися, підлаштовуючись під конкретну систему);

- статистичні заходи: рішення про наявність кібератаки робиться по великій кількості зібраних даних шляхом їх статистичної предобработки;

- параметрична: для виявлення кібератаки будується спеціальний "профіль нормальної системи" на основі шаблонів (тобто деякій політиці, якої зазвичай повинен дотримуватися даний об'єкт);

- непараметричні: тут вже профіль будується на основі спостереження за об'єктом в період навчання;

- заходи на основі правил (сигнатур): вони дуже схожі на непараметричні статистичні заходи. В період навчання складається уявлення про нормальному поведінку об'єкта, яке записується у вигляді спеціальних "правил";

- інші заходи: нейронні мережі, генетичні алгоритми, що дозволяють класифікувати деякий набір відомих сенсор-датчику ознак. В сучасних СВКбА в основному використовують перші два методи. Слід зауважити, що існують дві крайності при використанні даної технології:

- виявлення аномальної поведінки, яке не є кібератакою, і віднесення його до класу атак (помилка другого роду);

- пропуск атаки, яка не підпадає під визначення аномального поведінки (помилка першого роду). Цей випадок набагато більш небезпечний, ніж помилкове зарахування аномальної поведінки до класу атак.

Аналіз останніх досліджень і публікацій дає змогу дійти висновку, що більшість існуючих класифікацій СВКбА дуже абстрактні, не є повними, і у них значні важливі характеристики (елементи) потребують доповнень та узагальнень.

Сьогодні методи виявлення аномалій являються пріоритетними у побудові систем виявлення кібератак. Найпопулярнішими серед них можна виділити чотири підгрупи, а саме: статичне виявлення аномалій, виявлення засноване на інтелектуальному аналізі даних, виявлення засноване на існуючих знаннях, виявлення на основі машинного навчання.

Також в більшості класифікацій відсутні гібридні методи, які стрімко досліджуються сьогодні і являють собою синтез сигнатурного методу і методу виявлення аномалій.

В залежності від архітектури СВКбА виділяють системи, на якій виконується програмне забезпечення (host) і системи, за якими спостерігають (target).

Раніше СВКбА, переважно, виконувалися на тих же системах, які вони захищали проте з появою робочих станцій і персональних комп’ютерів у більшості архітектур СВКбА передбачається виконання СВКбА на окремій системі, тим самим розділяючи системи host і target. Це поліпшує безпеку функціонування СВКбА.

Аналіз мережевих пакетів популярний для збору інформації про події, які надходять від мережі. Перехоплювачами можуть слугувати шлюзи прикладного рівня або фільтруючі маршрутизатори. Аналіз пакетів може бути виконаний досить швидко, якщо він проводиться на низькому рівні, виконавши, наприклад, зіставлення із зразком або використавши сигнатурний аналіз.

Використання сенсорів СВКбА є характерною рисою відносно нового покоління систем виявлення атак, що не виявляють атаки безпосередньо, але мають змогу корелювати інформацію, зібрану з декількох інструментів виявлення вторгнень (сканерів). Такий метод зберігає і зменшує кількість подій, які повинні бути оброблені. Це також вигідно, коли діяльність охоплює кілька користувачів, комп'ютерів або мереж.

При розгортанні СВКбА важливо знати, які технології використовуються в побудові інформаційної системи. Адже дротові мережі, порівняно з бездротовими, використовують різні і специфічні методи безпечної передачі, наприклад, шифрування. Тому фізична мережа передачі даних відіграє важливу роль у проектуванні систем виявлення кібератак.

Якщо система контролю трафіку (СКТ) реалізована на базі локальної або розподіленої інформаційної системи, то в ній можуть бути реалізований загрози безпеки інформації шляхом використовування протоколів міжмережевого взаємодії. При цьому може забезпечуватися НСД до контрольованого трафіку або реалізовуватися загроза відмови в обслуговування. Особливо небезпечні загрози, коли СКТ є розподіленою інформаційною системою підключеною до мереж загального користування і (або) мереж міжнародного інформаційного обміну.

Кібернетичні атаки на інформаційну систему реалізуються головним чином за рахунок даних кібератак: аналіз мережевого трафіку, сканування мережі, загроза виявлення пароля,

підміна довіреного об'єкту мережі і передача по каналах зв'язку повідомлень від його імені з привласненням його прав доступу, нав'язування помилкового маршруту мережі, несанкціоноване введення об'єкту мережі, відмова в обслуговуванні, видалений запуск додатків. Ці загрози можуть проявлятися у вигляді як навмисних, так і ненавмисних помилок, збоїв і відмов техніки і програмного забезпечення, шкідливого впливу зі сторони злочинних структур і кримінальних елементів.

Отже, засоби виявлення кібернетичних атак забезпечують одержання даних з мережі про зловмисну активність в зрозумілу інформацію, яка може бути використаний для усунення підтверджених порушень безпеки і забезпечення відповідності нормативним документам.

Висновки. Аналізуючи дані положення про здійснення кібернетичних атак, можна дійти висновку, що розглянуті вище можливості захисту даних не будуть у повній мірі ефективні якщо їх не використовувати у єдиному комплексі.

Засоби виявлення кібернетичних атак забезпечують одержання даних з мережі про зловмисну активність в зрозумілу інформацію, яка може бути використаний для усунення підтверджених порушень безпеки і забезпечення відповідності нормативним документам. Набір зручних у використанні апаратних засобів віддзеркалення загроз дозволяє адміністраторам централізовано знаходити, визначати пріоритетність і відображати загрози за допомогою вже упроваджених в інфраструктуру мережевих пристроїв і пристроїв захисту.

Список використаних джерел

1. Безрук В.М., Баранник В.В., Толюпа С.В. и др. Наукоемкие технологии в инфокоммуникациях: обработка информации, кибербезопасность, инфомационная боротьба. Коллективная монографія. Харьков – Компания СМИТ – 2017. – с. 620.

2. Бабенко Л.К. Разработка комплексной системы обнаружения атак / Л.К. Бабенко, О.Б. Макаревич, О.Ю. Пескова // Информационная безопасность: материалы V междунар. науч. - практ. конф. 2003. №4(33). С.235 - 239

3. Toliupa. S. V. , Nakonechny. V. S. , Brailovskyi. N. N. Building Cyber-Security Systems of Information Networks Based on Intellectual Technologies// Scientific & practical cyber security journal (SPCSJ) № 1.[Electronic journal]. URL: http://journal.scsa.ge/issues/2017/09/432

4. Самохвалов Ю.Я., Толюпа С.В., Сигнатурные методы обнаружения компьютерных кибератак в информационных системах. VII Міжнародна науково-технічна конференція «ITSEC», 16–18 травня 2017р. НАУ (м. Київ). с. 87-89.

5. Пархоменко І.І., Толюпа С.В. Засоби виявлення кібератак. Національна академія СБУ VIII Науково-практична конференція «Актуальні проблеми управління інформаційною безпекою держави». 2017р. С. 112-115.

Надійшла: 10.11.17 Рецензент: к.т.н., доц. Довбешко С.В.