© Korchenko O., Loginov I., Skvortsov S. Stationary systems of cyberattacks detection and prevention for cyberprotection and cyber-counterintelligence (by example USA) // Ukrainian Scientific Journal of Information Security, 2019, vol. 25, issue 1, pp. 5-12.

DOI: 10.18372/2225-5036.25.13664

СТАЦІОНАРНІ СИСТЕМИ ВИЯВЛЕННЯ І ПОПЕРЕДЖЕННЯ КІБЕРАТАК В ІНТЕРЕСАХ КІБЕРЗАХИСТУ ТА КІБЕРКОНТРРОЗВІДКИ (НА ПРИКЛАДІ США)

Олександр Корченко[1], Ігор Логінов[2], Сергій Скворцов[1]

[1]Національний авіаційний університет, Україна
[2]Служба безпеки України

КОРЧЕНКО Олександр Григорович, д.т.н.

Рік і місце народження: 1961, Київ, Україна.
Освіта: Київський інститут інженерів цивільної авіації (з 2000 року Національний авіаційний університет), 1983 рік.
Посада: завідувач кафедри безпеки інформаційних технологій з 2004 року.
Наукові інтереси: інформаційна і авіаційна безпека.
Публікації: більше 300 наукових публікацій, серед яких монографії, словники , навчальні посібники, підручники, наукові статті та патенти на винаходи.
E-mail: icaocentre@nau.edu.ua.
Orcid ID: 0000-0003-3376-0631.

ЛОГІНОВ Ігор Вадимович, к.ю.н., старший науковий співробітник

Рік і місце народження: 1966 р., м. Горький (нині Нижній Новгород, РФ)
Освіта: Київське вище інженерне радіотехнічне училище Військ протиповітряної оборони країни ім. Маршала авіації Покришкіна О. І., 1989 р.; Національна академія Служби безпеки України, 2001 р.
Посада: провідний фахівець Ситуаційного центру забезпечення кібербезпеки Служби безпеки України з 2015 року.
Наукові інтереси: кібербезпека
Публікації: понад 60 наукових праць, серед яких монографії, курси лекцій, навчальні посібники, навчально-методичні комплекси дисциплін, наукові статті
E-mail: logiv1966@i.ua.
Orcid ID: 0000-0001-9317-7304.

СКВОРЦОВ Сергій Олександрович, к.т.н

Рік та місце народження: 1961 рік, м. Ташкент, Узбекистан.
Освіта: Київський інститут інженерів цивільної авіації, 1983 рік.
Посада: доцент кафедри безпеки інформаційних технологій.
Наукові інтереси: інформаційна безпека, технології програмування, експертні системи, штучний інтелект.
Публікації: більше 30 наукових публікацій, серед яких наукові статті, матеріали і тези доповідей на конференціях, авторські свідоцтва.
E-mail: ssamailer@gmail.com.
Orcid ID: 0000-0001-9318-3667.

Аннотація. *У забезпеченні національної кібербезпеки задіяно декілька силових відомств нашої країни. Кожне з них вирішує власне коло завдань щодо захисту критичної інформаційної інфраструктури від кібератак і кіберінцидентів. Так, Державна служба спеціального зв'язку та захисту інформації (Держспецзв'язку) України, підрозділи технічного захисту інформації відповідають за кіберзахист інформаційних ресурсів та інфраструктури їх оброблення незалежно від характеру кібератак, що на них здійснюються. Служба безпеки України убезпечує критичну інформаційну інфраструктуру від кібератак розвідувально-підривного характеру, а Національна поліція захищає інтереси суспільства і громадян від кіберзлочинів. Але, для виконання поставлених перед ними завдань Служба безпеки і Держспецзв'язку України однаково потребують засобів виявлення і попередження кібератак. Проте, на характеристиках і функціональних можливостях цих засобів відбиватиметься специфіка завдань, вирішуваних обома відомствами. З огляду на це, у статті викладено результати вивчення зарубіжного досвіду побудови систем виявлення і попередження кібератак в інтересах кіберзахисту і кіберконтррозвідки, визначено їх сутнісні характеристики, які доцільно врахувати у практичній діяльності з розбудови національної системи забезпечення кібербезпеки.*

Ключові слова: *кібербезпека, кіберзахист, кібератака, критична інформаційна інфраструктура, кіберконтррозвідка, Intrusion Detection System, Intrusion Prevention System, Intrusion Detection and Prevention System, Deep Packet Inspection.*

Актуальність проблеми дослідження

Із Закону "Про основні засади забезпечення кібербезпеки України" випливає, що кібербезпека держави забезпечується за напрямами кіберзахисту, кібероборони, протидії кіберзлочинності, протидії кібершпигунству і кібертероризму (далі – кіберконтррозвідки) тощо [1]. В Україні за кіберзахист відповідають органи та підрозділи технічного захисту інформації у сполучених з Інтернет та іншими глобальними мережами інформаційно-телекомунікаційних системах (далі – ІТС), за кіберконтррозвідку - спеціально створені підрозділи Служби безпеки України. Підрозділи кіберзахисту і кіберконтррозвідка спільно зацікавлені у виявленні кібератак: кіберзахист – щоб захистити інформацію в ІТС від загроз порушення цілісності, конфіденційності і доступності, кіберконтррозвідка – щоб запобігти акціям кібершпигунства і кібертероризма, які здійснюються у формі кібератак. Внаслідок цього суб'єкти кіберзахисту і кіберконтррозвідки однаково озброюються засобами виявлення кібератак. Але кіберзахист і кіберконтррозвідка – розбіжні функції, і тому ми припускаємо, що їх незбіг впливатиме на побудову та застосування їхніх засобів. Помилки у визначенні характерних рис засобів виявлення і попередження кібератак, призначених для кіберконтррозвідки і кіберзахисту, небезпечні виникненням дублювання функцій відповідних державних органів і підрозділів, що, на нашу думку, заважатиме ефективній міжвідомчій координації основних суб'єктів кібербезпеки, раціональному розподілу їх сил та засобів між законодавчо закріпленими напрямами її забезпечення. Для запобігання цьому актуальним вбачається вирішити наукове завдання з аналізу зарубіжного досвіду створення систем виявлення і попередження кібератак в інтересах кіберзахисту та кіберконтррозвідки з тим, щоб врахувати його результати у практичній діяльності з розбудови національної системи забезпечення кібербезпеки України.

Аналіз останніх досліджень і публікацій

Системи виявлення та попередження кібератак вивчались А. Астраховим, С. Клімовим, М. Сичовим, Д. Кузнєцовим, В. Бабошиним, В. Васильєвим, В. Голубевим, А. Лукацьким, Є. Веселкіним, К. Скарфоне, П. Меллом, М. Тіварі, А. Бхарті, Р. Кумарі та багатьма іншими вітчизняними і зарубіжними вченими. Однак, в їх публікаціях відображено результати дослідження систем виявлення і попередження кібератак в інтересах кіберзахисту. Результатів вивчення відповідних систем контррозвідувального призначення у відкритих джерелах не виявлено.

Наукова новизна цього дослідження обумовлена вперше проведеним порівняльним аналізом стаціонарних систем виявлення і припинення комп'ютерних атак, призначених як для кіберзахисту, так і для кіберконтррозвідки, що дало змогу визначити їх сутнісні характеристики.

Виклад основного матеріалу

Встановленню співвідношення між засобами кіберзахисту і кіберконтррозвідки заважає утаємничення інформації про системи контррозвідувального призначення. Однак, трапляються окремі випадки розсекречування такої інформації. Наприклад, матеріали щодо деяких засобів кіберконтррозвідки США виклав у загальний доступ Е. Сноуден. Цими матеріалами і скористаємось для вирішення поставленого наукового завдання. Проте, спочатку проаналізуємо відомості про стаціонарні системи кіберзахисту США.

1. Стаціонарні системи виявлення і припинення кібератак органів кіберзахисту США.

Донедавна головним виконавчим суб'єктом кіберзахисту США був створений у червні 2003 р. на базі Агенції національної безпеки (далі – АНБ, англ. National Security Agency, NSA), але підпорядкований Міністерству внутрішньої безпеки (далі – МВБ) Центр комп'ютерної безпеки (National Computer Security Center, NCSC). Нині його реорганізовано у Національний центр кібербезпеки та інтеграції зв'язку (National Cybersecurity and Communication Integration Center, NCCIC). До складу NCCIC входять Група екстреного реагування на комп'ютерні події в США (U.S. Computer Emergency Response Team, US-CERT), Група екстреного реагування на надзвичайні події у системах керування промисловістю (Industrial Control Systems Cyber Emergency Response Team, ICS-CERT), та Національний координаційний центр зв'язку (National Coordinating Center for Communications, NCC). US-CERT виявляє кібератаки на ІТС цивільних федеральних органів влади США, попереджає про них адміністраторів безпеки ІТС, та координує дії з відновлення федеральних ІТС після

кіберінцидентів [2]. Відповідно, ICS-CERT виявляє і попереджає кібератаки на ІТС критично-важливих об'єктів промисловості США [3]. 16 листопада 2018 р. указом президента США Д. Трампа NCCIC передано до нового Агенства з кібербезпеки та безпеки інфраструктури МВБ США [4].

За нашою оцінкою, NCCIC відіграє роль національного Центру операцій безпеки (Security Operations Center, SOC [5]) зі стандартними функціями. Останні реалізуються типовими засобами кіберзахисту, а саме, системами виявлення та/або попередження кібератак, які поділяються на: 1) системи виявлення кібератак (Intrusion Detection System, IDS); 2) системи попередження кібератак (Intrusion Prevention System, IPS); 3) системи виявлення та попередження кібератак (Intrusion Detection and Prevention System, IDPS) [6; 7].

Сучасні IDS/IPS/IDPS функціонують за принципом "глибокого аналізу пакетів даних" ("Deep Packet Inspection", DPI) [7; 8], внаслідок чого виконуються у вигляді "надбудови" над оперативно-розшуковими DPI-системами "законного перехоплення" ("lawful interception") інтернет-трафіка у правоохоронних цілях, або у вигляді спеціалізованих вузькопрофільних DPI-систем [7]. Від оперативно-розшукових DPI-систем IDS/IPS/IDPS відрізняються призначенням для пошуку за сигнатурами та блокування в інтернет-трафіку шкідливого програмного забезпечення, а не відбору приватного інтернет-контента.

Безпосереднім експлуатантом IDPS у структурі NCCIC є Національна команда реагування на комп'ютерні інциденти US-CERT. Для виявлення і припинення кібератак вона застосовує IDS/IDPS Einstein трьох поколінь (Einstein-I, Einstein-II та Einstein-III), що відрізняються архітектурою і функціональними можливостями.

Так, створена у 2003 р. система Einstein-I складається з підключених до SOC NCCIC каналами телекомунікацій віддалених датчиків кіберінцидентів, встановлених на інтернет-шлюзах ІТС цивільних органів федеральної влади США. Датчики відбирають з інтернет-трафіку мета-дані та транслюють їх до US-CERT, де вони аналізуються на предмет виявлення аномалій. Мета-дані охоплюють адреси IP, номери портів, індекси протоколів, що використовуються, кількість пакетів і переданих байтів, час початку і закінчення з'єднання, назву датчика тощо.

Недоліками системи Einstein-I фахівці називали:

1) добровільність встановлення датчиків в органах влади. Так, у 2005 р. тільки три федеральних органи влади підключилися до системи, у грудні 2008 – вісім з декількох сотень;

2) обмеження призначення системи пасивним збором і аналізом мета-даних, що дає змогу виявляти кібератаки, але не забезпечує виявлення шкідливого програмного забезпечення у трафіку даних та попередження кібератак;

3) неможливість аналізу мета-даних в режимі реального часу;

4) ізольованість системи від схожих засобів кібероборони, кіберрозвідки і кіберконтррозвідки [8].

З урахуванням цього в листопаді 2007 р. під егідою Офісу з менеджменту і бюджету США та МВБ розпочато реалізацію програми Довірчих Інтернет-з'єднань (Trusted Internet Connections, TIC). У рамках програми планувалось охопити кіберзахистом близько 5 тис. ІТС органів і підрозділів федеральної влади. Їхні ІТС мали підключатись до 50 інтернет-шлюзів (по 100 ІТС на шлюз), які через датчики кіберзахисту контролювались US-CERT [там же].

Додатковий імпульс програмі TIC надано започаткуванням Комплексної національної ініціативи з кібербезпеки (Comprehensive National Cybersecurity Initiative, CNCI), яку засновано на директиві президента США з питань національної безпеки № 54 "Кібербезпека і моніторинг", та пов'язано з президентською директивою з питань внутрішньої безпеки (Homeland Security) № 23 з тою ж назвою [9]. CNCI передбачається, що федеральні агентства можуть отримувати доступ до Інтернет чотирма способами: 1) через [фізичне. – авт.] підключення до інтернет-шлюзу TIC, який експлуатується довіреним постачальником послуги доступу до Інтернет (TICAP); 2) через [віртуальне. – авт.] підключення до іншого TICAP; 3) через довірену службу IP схваленого (атестованого чи сертифікованого) МВБ комерційного Інтернет-провайдера (MTIPS); 4) комбінацією вказаних вище способів.

Результатом реалізації програми TIC стало істотне скорочення чисельності Інтернет-шлюзів для органів федеральної влади США, кількості встановлених на них датчиків кіберзахисту, і, відповідно, спрощення і здешевлення системи Einstein-II з одночасним збільшенням кількості об'єктів, охоплених кіберзахистом. Але, для цього у TIC-шлюзах порівняно зі звичайними довелося істотно збільшити пропускну здатність та спроможність провайдерів до її швидкого нарощування. Крім того, довелося повністю змінити маршрутизацію трафіку ІТС цивільних федеральних органів влади [8].

На відміну від Einstein-I, в Einstein-II на предмет виявлення шкідливого програмного забезпечення моніториться телекомунікаційний трафік, а не мета-дані. Для цього створюється його тимчасова копія, у якій за сигнатурами вишукуються підозрілі пакети даних та аномалії. До Einstein-II також спрямовуються мета-дані від датчиків Einstein-I, які інкапсулюються в пакети Einstein-II.

Станом на вересень 2009 р. у системі Einstein-II функціонувало 15 TICAP і 4 MTIPS. Від підключення до системи було звільнено Міністерство оборони, органи розвідки і контррозвідки США, кіберзахист яких забезпечується засобами АНБ США [8].

Проте, недоліком Einstein-II залишилась успадкована від Einstein-I неспроможність попереджати кібератаки. Тому у 2010 р. МВБ вирішило посилити Einstein-II системою Einstein-III Accelerated (скор. E3A), з кращими можливостями виявлення шкідливого програмного забезпечення в інтернет-трафіку цивільних органів федеральної влади, а головне – з можливістю попередження кібератак. Датчики E3A встановлюються на майданчиках інтернет-провайдерів, які обслуговують цивільні федеральні органи влади [можливо, MTIPS. – авт.]. Ними фільтрується мережний трафік, пакети в якому відбираються за окремими переліками IP-адрес. Зазначені переліки надаються і регулярно корегуються кож-

ною федеральною агенцією, та перевіряються МВБ чи довіреними інтернет-провайдерами [можливо, MTIPS. – авт.], які обслуговують датчики ЕЗА.

У ЕЗА застосовуються наступні методи попередження кібератак:

1) переспрямування підозрілих інтернет-з'єднань на так звані "безпечні сервери" (англ. "safe servers") або DNS-сервер-"пісочницю" (англ. "sinkhole"), розташовані в SOC NCCIC. При цьому, хоча інтернет-провайдер має доступ до DNS-сервера-"пісочниці", але може отримати з нього тільки відомості за DNS-запитом. Інформація, що стосується шкідливого або підозрілого програмного забезпечення, інтернет-провайдеру не надається;

2) фільтрація електронної пошти, що спрямовується на IP-адреси домену .gov. Пересилання листа електронної пошти адресату дозволяється тільки після його автоматизованого аналізу SOC NCCIC на наявність шкідливого програмного забезпечення. Підозрілі або інфіковані електронні листи відправляються на карантин або поглиблений аналіз.

У ЕЗА об'єднано методи виявлення шкідливого програмного забезпечення, відпрацьовані у системах Einstein-I та Einstein-II. Інформація, необхідна для формування сигнатур шкідливого програмного забезпечення, отримується NCCIC власноруч за результатами розслідування кібератак та кіберінцидентів, а також від партнерських комерційних служб кіберзахисту та Threat Intelligence (легальної комерційної "розвідки кіберзагроз") [10].

Викладене дає підстави виокремити наступні особливості стаціонарних систем виявлення і припинення кібератак органів кіберзахисту США:

1) призначення для кіберзахисту цивільних органів федеральної влади;

2) експлуатація підрозділом кіберзахисту, підпорядкованим МВБ США;

3) поступове усвідомлення нестачі аналізу мета-даних для вирішення завдань кіберзахисту (система Einstein-I) та доповнення його глибоким сигнатурним аналізом інтернет-пакетів (системи Einstein-II, Einstein-III);

4) поступове усвідомлення нестачі функції IDS для вирішення завдань кіберзахисту (системи Einstein-I, Einstein-II), та доповнення її функцією IPS (система Einstein-III);

5) розміщення датчиків IDS/IDPS Einstein-I, Einstein-II, Einstein-III у точках підключення цивільних федеральних органів влади до Інтернету (спочатку на відомчих інтернет-шлюзах, потім на інтернет-шлюзах TIC, і, нарешті, на майданчиках інтернет-провайдерів, які надають об'єктам захисту доступ до інтернету).

2. Стаціонарні системи виявлення і припинення кібератак органів кіберконтррозвідки США.

Згадувана вище Комплексна національна ініціатива з кібербезпеки (CNCI) містить перелік схвалених президентом США ініціатив із забезпечення національної кібербезпеки. Зокрема, ініціатива № 6 передбачає розробку та імплементацію урядового плану діяльності кіберконтррозвідки ("cyber counterintelligence (CI) plan"), що має узгоджуватися з Національною контррозвідувальною стратегією США [11]. У CNCI зазначається, що план необхідний для координації діяльності усіх федеральних агенцій з виявлення, визначення і зменшення загроз, створюваних іноземними кіберрозвідками інформаційним системам державного і приватного секторів США [9]. Обґрунтовано припустити, що координатором виконання цього плану мала б стати кіберконтррозвідка США.

У зв'язку з цим виникає питання: який орган або підрозділ США виконує функції національної кіберконтррозвідки, зокрема, здійснює контррозвідувальний захист ІТС від кібератак на національному рівні?

Традиційно у США контррозвідувальна діяльність вважається підвидом розвідувальної діяльності [12, с. 584; 13, с. 3]. Тому контррозвідувальні функції у США часто покладаються на розвідувальні органи. Наприклад, ЦРУ є органом зовнішньої розвідки і контррозвідки. Розвідувальні та контррозвідувальні заходи також проводять підрозділи Командування розвідки і безпеки Наземних військ США (INSCOM) [14, с.18-21]. З цієї причини обґрунтовано буде шукати підрозділ кіберконтррозвідки у структурі органу кіберрозвідки.

За даними Е. Сноудена, кіберрозвідка США представлена Директоратом розвідки сигналів АНБ (Signal Intelligence Directorate of NSA, SID NSA), а комп'ютерна розвідка – підрозділом TAO (Tailored Access Operations) цього Директорату [15]. За логікою, у структурі TAO або поряд має перебувати підрозділ, який відповідає за попередження, виявлення і припинення кібератак на ІТС США в рамках контррозвідувальної діяльності.

Дійсно, Д. Гольдман стверджує, що питаннями контррозвідувального захисту ІТС США від інспірованих іншими державами кібератак опікується підпорядкований TAO Департамент S31177, відомий під кодовою назвою "Transgression" [16]. Але, за даними Е. Сноудена, цим займається інший структурний підрозділ TAO з назвою Requirements & Targeting (R&T) [15].

Керівництво Requirements & Targeting складається з начальника підрозділу, його заступника, керівника цільової експлуатації ("target exploitation lead"), технічного директора з операцій у комп'ютерних мережах (Computer Network Operations, CNO), технічного директора з криптографічного аналізу та головуючого на засіданнях так званої "Ради чотирьох" ("Fourth Party Strategic/Lead").

Проте, одним із структурних підрозділів R&T дійсно є згаданий Д. Гольдманом підрозділ "Transgression". За матеріалами Е. Сноудена, йому доручене "відстеження зовнішніх кібератак, спостереження за ними, їх аналіз та запозичення найкращих ідей зарубіжного кібершпигунства", "викриття, вивчення, оцінювання та застосування іноземних експлойтів, імплантів, систем управління ними, їх контролю та ексфільтрації, призначених для проведення комп'ютерних атак деструктивного (CNA) та шпигунського (CNE) характеру" [15; 16].

Поряд з "Transgression", R&T складається також з підрозділів "Persistent Threat" ("Постійних

загроз"), "Emergency Threat" ("Надзвичайних загроз"), та "Ради чотирьох" ("Fourth Party"), до якої входять уповноважені представники 4-х підрозділів АНБ, зацікавлених у взаємодії, а саме:

1) Ситуаційного центру кіберзахисту (NSA/ CSS Threat Operation Center, NTOC) Центральної служби безпеки (Central Security Service, CSS) АНБ, де CSS – провідний суб'єкт технічного і криптографічного захисту федеральної інформації (NTOC CSS NSA);

2) підрозділу SSG (SIGDEV Strategy and Governance), який розробляє стратегію та здійснює загальне керівництво Директоратом розвідки сигналів (SSG SID NSA);

3) підрозділу S2 (Analisys & Production), який аналізує добуту оперативну інформацію і готує вихідні документи Директорату розвідки сигналів (S2 SID NSA);

4) підрозділу S3 (Data Acquisition), який об'єднує добуваючі підрозділи GAO, SSO та TAO зі складу SID (S3 SID NSA) [17; 18].

На засіданнях "Ради чотирьох" вирішуються питання взаємодії між кіберрозвідкою (S3 SID NSA), підрозділом, відповідальним за попередження, виявлення і припинення кібератак іноземних кіберрозвідок в рамках контррозвідувальної діяльності (R&T TAO S3 SID NSA), та підрозділом кіберзахисту (NTOC CSS NSA), важливі для спільного забезпечення ними кібербезпеки США.

Підрозділ R&T TAO S3 SID NSA озброєно стаціонарною системою виявлення і попередження кібератак Tutelage (англ. "Піклування", "Опікунство") [19].

З матеріалів Е. Сноудена випливає, що вона займає проміжкову позицію між IDPS кіберзахисту і системами кіберрозвідки (Signal Intelligence, SIGINT), які пов'язує між собою в єдине ціле.

Згідно з цими матеріалами, до її впровадження підрозділ R&T TAO S3 SID NSA починав реагувати на кібератаку після фіксації її слідів у лог-файлах атакованої системи. При цьому від виявлення первинних ознак кібератаки до повідомлення про неї адміністрації атакованого об'єкта спливало кілька діб.

Впровадження системи Tutelage дало змогу організувати роботу на випередження кібератак, оскільки в ній акцент робиться на виявлення іноземної кіберзброї [20; 21; 22] на стадії її розробки і випробувань до початку атаки на національні ІТС США. Реалізовано цю ідею шляхом підключення до Tutelage систем SIGINT з перехоплення іноземного інтернет-трафіка. Нині виявлення і попередження кібератак іноземних розвідок на ІТС США здійснюється за етапами:

1) постійного пошуку в іноземному інтернет-трафіку неприятельської кіберзброї за окремими ознаками;

2) виявлення її на стадії випробувань, її аналізу та розробки комплексних демаскувальних ознак (сигнатур);

3) вироблення системи заходів запобігання її застосуванню;

4) цілеспрямованого пошуку і нейтралізації неприятельської кіберзброї за її сигнатурами на інтернет-шлюзах між національною системою телекомунікацій США і "зовнішнім" Інтернетом [імовірно, за допомогою датчиків кіберзахисту Einstein-III та NTOC CSS. – авт.];

5) виявлення і нейтралізації неприятельської кіберзброї за її сигнатурами на інтернет-шлюзах ІТС об'єктів захисту США [імовірно, за допомогою датчиків кіберзахисту Einstein-I, -II та комерційних IDS/IPS/IDPS. – авт.] [19].

Виявлені системою Tutelage кібератаки щодо об'єктів МО і ЗС США попереджаються підрозділами R&T TAO S3 SID та NTOC CSS NSA, щодо ІТС інших об'єктів захисту – підрозділами кіберзахисту інших відомств (зокрема, US-CERT, ICS-CERT). Такий розподіл компетенції у сфері кіберзахисту пояснюється тим, що військові об'єкти США убезпечуються в технічному плані військовою технічною контррозвідкою і військовими підрозділами інженерно-технічного захисту, які представлено підрозділами SID і CSS у складі АНБ, при чому останню формально підпорядковано МО США.

Зокрема, датчики кіберзахисту Tutelage встановлено на інтернет-шлюзи мережі NIPRNet ("Non-classified Internet Protocol Router Network") МО США, яка призначена для внутрішньовідомчого обміну нетаємним інтернет-трафіком між підрозділами МО і ЗС США. Ці датчики, імовірно, контролюються NTOC CSS NSA.

Для розробки сигнатур неприятельська кіберзброя досліджується в Tutelage інструментами CYBERQUEST, XKEYSCORE, GNOMEVISION, POPQUIZ тощо, де CYBERQUEST, імовірно, призначений для розпізнавання шкідливого програмного забезпечення у трафіку даних, XKEYSCORE – для високошвидкісної фільтрації трафіка даних, перехопленого засобами SIGINT, GNOMEVISION – деобфускації ("розплутування маршрутів") проходження пакетів даних зі шкідливим програмним забезпеченням, POPQUIZ – для аналізу поведінки підозрілого програмного забезпечення в режимі реального часу [19; 23; 24].

Розроблені після цього сигнатури передаються:

1) до засобів SIGINT для цілеспрямованого пошуку дослідженої кіберзброї в інтернет-трафіку, що заходить в США зовні;

2) у датчики кіберзахисту, встановлені на інтернет-шлюзах NIPRNet;

3) до партнерських організацій кіберзахисту (зокрема, NCCIC).

При цьому систему Tutelage оснащено інструментарієм для:

1) виявлення кібератаки і генерації сигналу тривоги пасивними датчиками кіберзахисту. Згенерований сигнал тривоги транслюється на засоби SIGINT, щоб співставити кібератаку перехопленим пакетам даних;

2) перехоплення шкідливого трафіка. Виявлені пакети даних зі шкідливим програмним забезпеченням вилучаються з трафіка, – тобто, на інтернет-шлюзи захищуваних ІТС трафік має надходити "очищеним";

3) підміну комп'ютера атакованого об'єкта "сплячим" ("sleep") комп'ютером, відповіді від якого

комп'ютер нападника не в змозі розшифрувати ("unable to decrypt");

4) переспрямування трафіка нападника з ІТС атакованого об'єкта на "безпечний сервер" ("safe server");

5) блокування трафіка нападника за портами або IP-адресами;

6) регульовану затримку реакції комп'ютера атакованого об'єкта на кібератаку ("latency/speed adjusted"), що дає змогу виграти у нападника час для реалізації інших можливостей Tutelage;

7) "переривання" ("reset") TCP-протоколу шляхом розриву з'єднання [18].

Станом на час публікації матеріалів Е. Сноудена, Tutelage задіювалась у протидії 28 основним видам кібератак (зокрема, Black Energy, Zeus, Byzantine) з використанням 794 операційних ефектів, створених вказаними вище інструментами [там же].

У перспективі передбачалось:

– переоснастити систему сенсорами з пропускною здатністю 10 гігабайт на секунду, що дало б змогу збільшити її продуктивність та ємність, реалізувати в ній правила Snort сесійного та багатоподійного ("multi-event") рівнів замість Snort пакетного рівня, налагодити з використанням протоколу Netflow аналіз мережевого трафіка інструментом GHOSTMACHINE, призначеним для дослідження Big Data за допомогою хмарних технологій;

– доповнити інструментарій Tutelage засобом "сайдлайнінгу" ("sidelining" – "витискування, обмеження"), який дасть змогу перенаправляти кібератаку на вторинний рівень втручання, де хости-посередники, призначені для прослуховування трафіку, карантину тощо забезпечуватимуть додаткові можливості маніпулювання шкідливим трафіком в інтересах нейтралізації комп'ютерної атаки;

– інтегрувати Tutelage з системою кіберзахисту МО США HBSS (Host-Based Security System);

– підключити Tutelage до системи TURBINE вірусної комп'ютерної розвідки [25, с.193]. Це дасть змогу проводити стосовно нападників кіберконтратаки з використанням арсеналу кіберзброї QUANTUM [19].

Серед прикладів успішного застосування Tutelage згадується відбиття NTOC за орієнтуваннями R&T:

– у 2009 р. кібератаки BYZANTINE HADES, проведене за допомогою комплексу заходів, розроблених на основі інформації, яку було отримано засобами SIGINT;

– у жовтні 2010 р. цілеспрямованої фішингової атаки на комп'ютери Голови Об'єднаного комітету начальників штабів США та керівника військово-морських операцій, коли шкідливе програмне забезпечення надсилалось pdf-документами;

– цілеспрямованої фішингової атаки AMULETSTELLAR на комп'ютери 10 генералів та старших офіцерів МО США на Різдвяні свята [рік у джерелі інформації не вказано. – авт.] [19].

Викладене дає підстави виокремити такі особливості, притаманні стаціонарним системам виявлення і припинення кібератак в інтересах кіберконтррозвідки США:

1) вони експлуатуються підрозділами кіберконтррозвідки, створеними у складі кіберрозвідки США;

2) ці системи пов'язують між собою в єдине ціле засоби кіберрозвідки (SIGINT) та кіберзахисту;

3) їх призначено для виявлення неприятельської кіберзброї у зовнішньому інтернет-трафіку на стадії її випробувань, що дає змогу завчасно сповіщати про неї підрозділи кіберзахисту для запобігання вторгнень;

4) для цього системи SIGINT дооснащено сенсорами кіберконтррозвідки, які фільтрують зарубіжний, у т.ч. вхідний у США інтернет-трафік за правилами Snort пакетного, сеансового та багатоподійного рівнів;

5) інтегрованими у кіберконтррозвідувальну систему Tutelage датчиками кіберзахисту облаштовуються інтернет-шлюзи між національним інтернет-сегментом США та "зовнішнім" Інтернетом (перший рубіж кіберзахисту), а також інтернет-шлюзи між відомчими ІТС та національним інтернет-сегментом США (другий рубіж кіберзахисту);

6) за встановлення та застосування датчиків кіберзахисту відповідають підрозділи кіберзахисту (зокрема, NTOC NSA);

7) діяльність кіберконтррозвідувальних підрозділів NSA, зокрема, зосереджено на:

– виявленні засобами SIGINT кіберзброї неприятеля у зарубіжному, у т.ч. вхідному у США інтернет-трафіку;

– її аналізі, розробці сигнатур та комплексу заходів протидії, їх повідомленні підрозділам кіберзахисту для відбиття кібератак на декількох рубежах кіберзахисту;

– нейтралізації кібератак наявними (див. вище) та перспективними (сайдлайнінг, кіберконтратаки) інструментами системи Tutelage.

Висновки

Порівняння визначених нами особливостей систем виявлення і попередження кібератак в інтересах кіберзахисту і кіберконтррозвідки США дає підстави стверджувати наступне:

1. Якщо в найперших системах кіберзахисту (Einstein-I) кібератаки виявлялись шляхом аналізу мета-даних, то сучасні системи кіберзахисту (Einstein-II, Einstein-III) та кіберконтррозвідки (Tutelage) однаково засновані на принципі "глибокого аналізу пакетів даних" ("Deep Packet Inspection").

2. Крім виявлення, сучасні системи кіберзахисту і кіберконтррозвідки призначаються також для попередження кібератак.

3. Датчики систем кіберзахисту США утворюють два захисні рубежі: перший (зовнішній) з обладнаних ними інтернет-шлюзів між "зарубіжним" Інтернетом і його національним сегментом, другий (внутрішній) – між національним сегментом та відомчими ІТС об'єктів, що захищаються.

4. Датчики систем кіберконтррозвідки винесено у "зарубіжний" Інтернет з тим, щоб виявляти кіберзброю противника у зовнішньому інтернет-трафіку на етапі її розробки та випробувань, та потім здійснювати її цілеспрямований пошук в інтер-

нет-трафіку, що надходить до США зовні. Для цього датчики кіберконтррозвідки інтегруються в засоби SIGINT.

5. Відібрані датчиками кіберконтррозвідки та проаналізовані відомості, необхідні для виявлення і попередження кібератак, передаються у датчики систем кіберзахисту. Разом з тим, кіберконтррозвідка володіє власним інструментарієм попередження кібератак, який може застосовуватись за призначенням незалежно від систем кіберзахисту.

Література

[1]. Закон України "Про основні засади забезпечення кібербезпеки" № 2163-VIII від 05 жовтня 2017 р.

[2]. National Infrastructure Protection Plan – NIPP. [Електронний ресурс]. Режим доступу: https:// www.dhs.gov/national-infrastructure-protection-plan.

[3]. ICS-CERT. Industrial Control Systems Cyber Emergency Response Team. [Електронний ресурс]. Режим доступу: https://ics-cert.us-cert.gov.

[4]. Cybersecurity and Infrasructure Security Agency. [Електронний ресурс]. Режим доступу: https://www.dhs.gov/cybersecurity-and-infrasructure-security-agency.html.

[5]. Что такое SOC? [Електронний ресурс]. Режим доступу: https://rvision.pro/2-1-chto-takoe-soc-perevod-gajda-mitre/.

[6]. A. Tatsuhiko, Y. Yukiko, T. Yutaka, "Security Operations Center (SOC) and Security Monitoring Services to Fight Complexity and Spread of Cyber Threats" // *NEC Technical Journal. Special Issue on Cybersecurity*, Vol. 12, No. 2, pp. 34-37, 2018.

[7]. K. Scarfone, P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)", *Recommendations of the National Institute of Standards and Technology, Special Publication 800-94. Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg*, MD 20899-8930, February 2007.

[8]. M. Mueller, A. Kuehn, "Einstein on the Breach: Surveillance Technology", *Cybersecurity and Organizational Change.* [Електронний ресурс]. Режим доступу: https://www.econinfosec.org/archive/weis2013/papers/MuellerKuehnWEIS2013.pdf

[9]. Comprehensive National Cybersecurity Initiative. [Електронний ресурс]. Режим доступу: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-034.pdf.

[10]. Privacy Impact Assessment for EINSTEIN 3 - Accelerated (E3A) April 19, 2013 DHS/PIA/NPPD-027. [Електронний ресурс]. Режим доступу: https://www.dhs.gov/sites/default/files/publications/privacy/PIAs/PIA%20NPPD%20E3A%2020130419%20FINAL%20signed.pdf.

[11]. National Counterintelligence Strategy of the United States of America 2016 [Електронний ресурс]. Режим доступу: https:// www. dni. gov/ files/ NCSC/ documents/ Regulations/National_CI_Strategy_2016.pdf.

[12]. М. Дундуков, "Разведка как вид государственной деятельности в США", *Национальная безопасность*, № 4 (27), 2013.

[13]. В. Пилипчук, М. Будаков, В. Гірич, *Система організації управління і правового забезпечення діяльності спецслужб (досвід країн Європейського Союзу та Північної Америки): аналіт. доп.* К.: НІСД, 2012, 56 с.

[14]. R. Harfst, T. Stokowski, "Intelligence and Security Command Mission Command", *Military Intelligence Professional Bulletin*, July-September 2018.

[15]. J. Appelbaum, A. Gibson, *The Digital Arms Race. NSA Preps America for Future Battle.* [Електронний ресурс]. Режим доступу: http://www.spiegel.de/international/world/new-snowden-docs-indicate-scope-of-nsa-preparations-for-cyber-battle-a-1013409.html

[16]. D. Goldman, *Department S31177. Posturing for Digital Warfare* [Електронний ресурс]. Режим доступу: https:// intelligencebriefs.com/ tag/ department-s31177/

[17]. *Transgression overview for Pod58.* [Електронний ресурс]. Режим доступу: https://edward-snowden.com/ru/2015/01/18/transgression-overview-for-pod58/.

[18]. *NSA's organizational designations.* [Електронний ресурс]. Веб-сайт "Electrospaces.net". Режим доступу: https://electrospaces.blogspot.com/2014/01/nsas-organizational-designations.html.

[19]. *Tutelage.* [Електронний ресурс]. Веб-сайт "Snowden Archive". Режим доступу: https://snowden archive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH013b/995d9773.dir/doc.pdf.

[20]. В. Бабенко, "Основні групи кіберзброї та особливості її застосування", *Актуальні задачі та досягнення у галузі кібербезпеки. Матеріали Всеукраїнської науково-практичної конференції 23-25 листопада 2016 року, м. Кропивницький*, С. 23-24.

[21]. О. Запорожець, "Кібервійна: концептуальний вимір", *Actual problems of international relations. Release 121 (part I)*, pp. 80-84, 2014.

[22]. В. Каберник, "Проблемы классификации кибероружия", *Вестник МГИМО-Университета*, № 2(9), С. 72-78, 2013.

[23]. *NSA Nicknames and Codewords.* [Електронний ресурс]. Режим доступу: https://electrospaces.blogspot.com/p/nicknames-and-codewords.html.

[24]. *How to read the NSA Documents.* [Електронний ресурс]. Режим доступу: http://www.spiegel.de/international/world/glossary-of-nsa-abbreviations-a-975930.html.

[25]. І. Логінов, Ю. Аліфіров, *Системи та засоби основних видів технічних розвідок іноземних держав : навч. посіб*, Київ: Нац. акад. СБУ, 2016, 344 с.

УДК 004.032 : 004.056.57

Корченко А., Логинов И., Скворцов С. Стационарные системы обнаружения и предупреждения кибератак в интересах киберзащиты и киберконтрразведки (на примере США)

Аннотация: *В обеспечении национальной кибербезопасности Украины задействованы несколько государственных силовых ведомств. Каждое из них решает собственный круг задач по защите критической информационной инфраструктуры от кибератак и киберинцидентов. Так, Государственная служба специальной связи и защиты информации (Госспецсвязь) Украины отвечает за киберзащиту информационных ресурсов*

и инфраструктуры их обработки независимо от характера осуществляемых на них кибератак. Служба безопасности Украины обеспечивает безопасность критической информационной инфраструктуры от кибератак разведывательно-подрывного характера, а Национальная полиция защищает интересы общества и граждан от киберпреступлений. При этом, для выполнения поставленных перед ними задач Служба безопасности и Госспецсвязь Украины одинаково нуждаются в средствах обнаружения и предупреждение кибератак. В то же время, на характеристиках и функциональных возможностях таких средств должна отразиться специфика задач, решаемых обоими ведомствами. Учитывая это, в статье изложены результаты изучения зарубежного опыта построения систем обнаружения и предупреждения кибератак в интересах киберзащиты и киберконтрразведки, определены их сущностные характеристики, которые следует учесть в ходе построения национальной системы обеспечения кибербезопасности.
Ключевые слова: *кибербезопасность, киберзащита, кибератака, критическая информационная инфраструктура, киберконтрразведка, Intrusion Detection System, Intrusion Prevention System, Intrusion Detection and Prevention System, Deep Packet Inspection.*

Korchenko O., Loginov I., Skvortsov S. Stationary systems of cyberattacks detection and prevention for cyberprotection and cybercounterintelligence (by example USA)

Abstract. *Several state institutions deal with the providing of national cybersecurity. Each of them solvs its own number of tasks on critical information infrastructure protection from cyberattacks and cyberincidents. For example, the State Service of Special Communication and Information Protection, units of technical protection are responsible for cyberprotection of information resources and data processing infrastructure from cyberattacks of any origin. The Security Service of Ukraine defends national critical information infrastructure from cyberattacks of foreign intelligence services and cyberterrorists, and the National Police protects legal rights and interests of cityzens and society from cybercrimes. For solving their tasks, all of them use cyberattacks detection and prevention instruments. But these specific tasks, solved by both institutions, have to be affected on functional possibilities and characteristics of these means. Taking this into account, the article contains results of studying the foreign experience of creation the cyberattacks detection and prevention systems for cyberprotection and cybercounterintelligence, is determined key characteristics of the mentioned systems of different functions, which we need to conside in practical activity of building national cybersecurity system.*
Key words: *cybersecurity, cyberprotection, cybercounterintelligence, cyberattack, critical information infrastructure, cybercounterintelligence, Intrusion Detection System, Intrusion Prevention System, Intrusion Detection and Prevention System, Deep Packet Inspection.*

Отримано 3 *лютого 2019 року*, затверджено редколегією *30 березня 2019 року*