ЕКОНОМІКА ТА УПРАВЛІННЯ НАЦІОНАЛЬНИМ ГОСПОДАРСТВОМ

УДК 658.012.45-049.5

Сучасні напрями типологізації інформаційних загроз та тренди ринку інформаційної безпеки

Азєєв А.С.
аспірант кафедри менеджменту та математичного моделювання ринкових процесів
Одеського національного університету імені І.І. Мечникова

Чайковська М.П.
кандидат економічних наук,
доцент кафедри менеджменту та математичного моделювання ринкових процесів
Одеського національного університету імені І.І. Мечникова

Статтю присвячено аналізу новітніх напрямів розвитку інформаційних загроз та формуванню загальних тенденцій на ринку інформаційної безпеки. На основі збору інформації з профільних статистичних та методичних джерел охарактеризовано основні типи загроз та вразливостей, а також актуальні способи протидії, які практикуються сучасними організаціями. Спрогнозовано вектори розвитку загроз інформаційних систем й узагальнено можливі рекомендації щодо оптимізації та підвищення ефективності систем інформаційної безпеки.

Ключові слова: інформаційна система, інформаційна безпека, інформаційна загроза, Інтернет речей, шкідливе програмне забезпечення.

Азеев А.С., Чайковская М.П., СОВРЕМЕННЫЕ НАПРАВЛЕНИЯ ТИПОЛОГИЗАЦИИ ИНФОРМАЦИОННЫХ УГРОЗ И ТРЕНДЫ РЫНКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Статья посвящена анализу современных направлений развития информационных угроз и формированию общих тенденций на рынке информационной безопасности. На основе сбора информации из профильных статистических и методических источников охарактеризованы основные типы угроз и уязвимостей, а также актуальные способы противодействия, которые практикуются современными организациями. Спрогнозированы возможные векторы развития угроз информационных систем и подытожены рекомендации по оптимизации и повышению эффективности систем информационной безопасности.

Ключевые слова: информационная система, информационная безопасность, информационная угроза, Интернет вещей, вредоносное программное обеспечение.

Azeev A.S., Chaikovska M.P. MODERN DIRECTIONS OF INFORMATIONAL THREATS AND TRENDS OF THE INFORMATION SECURITY MARKET

This Article is devoted to the analysis of the latest directions in the development of information threats and the formation of common trends in the information security market. The main types of threats and vulnerabilities, as well as the relevant methods of counteraction practiced by modern organizations have been characterized based on the collection of information from profile statistical and methodological sources. Vectors of development of threats to information systems have been predicted and general recommendations with regard to optimization and increase of efficiency of information security systems have been summarized.

Keywords: information system, information security, information threat, Internet of things, malicious software.

Постановка проблеми у загальному вигляді. На сучасному етапі стану суспільства інформаційні технології (ІТ) активно впроваджуються в усі сфери економіки. ІТ є необхідним атрибутом підвищення ефективності бізнес-процесів, зокрема дають змогу господарюючим суб'єктам знизити витрати виробництва, підвищити точність економічного аналізу, правильно обирати стратегію й тактичні заходи в умовах форс-мажорних обставин. Однією з найбільш актуальних проблем, що ускладнюють застосування сучасних ІТ, є забезпечення інформаційної безпеки (ІБ). Побудова ефективної системи ІБ залежить насамперед від постійного моніторингу інформаційного середовища та сво-

єчасного реагування, адаптації та оновлення систем захисту. Аналіз становища на ринку ІБ та прогнозування можливих змін і будуть метою статті.

Аналіз останніх досліджень і публікацій. Теоретичні аспекти формування інформаційного суспільства, інформаційних системи та інформаційної безпеки висвітлено у працях М.В. Грайворонського, О.М. Новікова [1], С.Є. Остапова, С.П. Євсеєва, О.Г. Король [2], Е. Тоффлера [3] та ін. [4]. Поточні статичні добірки та практичні дослідження можна почерпнути з матеріалів аналітичних відділень великих ІТ-корпорацій (IDC, Cisco [5], Symantec [6,7], Worldwide Semiannual Security Spending Guide Symantec [8]) та періодичних публікацій, присвячених ІБ (Norton Cyber Security Report [9], ENISA Reports [10], Symantec Internet Security Threat Report [11] тощо). У процесі активного вивчення знаходиться проблематика своєчасного виявлення курсу еволюції інформаційних загроз й ефективного реагування організації щодо мінімізації супутніх ризиків.

Формулювання цілей статті (постановка завдання). Мета статті – проаналізувати сучасні напрями розвитку інформаційних загроз, висвітлити загальні тенденцій на ринку інформаційної безпеки, спрогнозувати вектори розвитку загроз інформаційних систем й узагальнити можливі рекомендації щодо оптимізації та підвищення ефективності систем інформаційної безпеки.

Виклад основного матеріалу дослідження. Одержання прибутку є основним мотивом зловмисників. Проте деякі з них зосереджені на блокуванні або навіть знищенні атакованих систем і процесів [1, с. 25]. Зазвичай дані активності розглядаються як провісник ще більш руйнівного типу атаки – Destruction of Service (Deos), спрямованої на знищення сервісу. Як показали результати атаки шифрувальника Nyetya (Petya) влітку цього року, дана атака була не вимагацьким програмним забезпеченням (ПЗ), а власне Deos-атакою, яка просто знищувала дані заражених систем у всьому світі.

Останніми роками все частіше спостерігається розгалуження периметра мережі, який традиційно повинен захищати. Замість цього такі технології, як мобільність, хмарні обчислення та ін., тільки збільшують можливу площу для атаки [2, с. 130]. Недавні атаки програм-здирників наочно демонструють, як зловмисники адаптуються до вразливостей у пристроях і мережах для завдання максимальних збитків.

Спостерігаючи за розвитком IoT-технологій (Internet of Things, «Інтернет речей») [3, с. 420] і моделюючи зростаючі ІБ-загрози цієї стрімко зростаючої та слабо захищеної індустрії, ми вже можемо бачити, як IoT-пристрої стають не тільки жертвою, але й зброєю в руках зловмисників [4, с. 880]. Прикладом такого використання може служити ботнет Mirai, який у результаті DDoS-атаки з уражених IoT-пристроїв на DNS-сервіс компанії Dyn паралізував роботу цілої низки компаній, включаючи Twitter, the Guardian, Netflix, Reddit, CNN і багато інших.

Аналізуючи методи, використані зловмисниками, важливо відслідковувати зміни, що відбуваються в їхній тактиці. Розглянемо нові тренди розвитку шкідливого ПЗ (malware), веб-атак і спама, ризики, пов'язані з потенційно непотрібним ПЗ (PUA – Potentially Unwanted Applications) типу шпигунського (spyware), компрометацію бізнес-пошти (BEC – Business Email Compromise), а також зміни економіки кіберзлочинів.

BEC стала високоприбутковим вектором атаки й по своїй прибутковості значно обійшла програми-здирники. Шпигунське ПЗ, що маскується під PUA, являє великий ризик для організацій і призводить до крадіжки інформації компаній та окремих користувачів, збільшуючи інфікування шкідливим ПЗ. За оцінкою експертів Cisco, три виділені групи сімейств spyware були знайдені в 20 з 300 вивчених компанії [5, с. 17].

Спостерігається загальне збільшення спамо-активностей починаючи із середини 2016 р., яке збіглося зі зменшенням активності Exploitkit у ті ж проміжки часу. Зловмисники, які покладалися на доставку програм-здирників через Exploit-Kit, перемкнулися на спам-розсилання, включаючи в них документи, що містять макроси, які «обходять» багато систем Sandbox через необхідність користувацької участі в інфікуванні.

Атаки ланцюжка поставки вироблені на багато організацій через один компрометований сайт. Найчастіше компрометації зазнають сайти виробників програмних рішень, у код інсталяційних пакетів яких інтегруються модулі malware. Так було з вектором поширення шифрувальника Nyetya через сайт компанії M.E.doc і з останньою компрометацією сайту й інсталятора програми CCleaner, коли цілі серії релізів ПЗ у минулому заражені, і сайт виробника був часом не тільки платформою поширення шкідника, а й – у випадку Nyetya – частиною прихованого C&C-каналу.

Exploitkit-активності помітно знизилися одночасно із числом внесених у них інновацій після зникнення Angler і деяких інших гравців даного ринку, але, ймовірно, це тимчасове явище. Підвищена складність експлуатації вразливостей файлів на основі платформи Adobe Flash перешкоджає процесу повернення популярності експлойта: зокрема, фіксується зменшення часу для установки патчів 80% вразливостей в Adobe Flash із 308 днів у 2014 р. до 62 у 2016 р. [5, с. 11]. Проте, розуміючи, що інформаційна злочинність – це багатомільярдний ринок, разом із появою нових векторів атак, які легко експлуатувати, очікується повернення популярності Exploit Kit.

Зловмисники шукають шляхи усунення мережі «безпеки», яку організації використовують для відновлення систем і даних після ураження шкідливим або вимагацьким ПЗ, а також інших ІБ-інцидентів. У чому можна бути впевненим, так це в тому, що IoT-пристрої, які багаті на вразливості, будуть відігравати центральну роль у таких загрозах, збільшуючи можливі наслідки атак.

Уже сьогодні ІБ-фахівці мають дуже багатий інструментарій для захисту своїх мереж. Експерти у сфері захисту інформації з різних індустрій звітують про установку численних рішень різних виробників, тим самим застосовуючи досить складний підхід до побудови ІБ, тоді як він повинен бути простим і цілісним. Фрагментований мультивендорний підхід до безпеки не дає змоги підприємству ефективно управляти загрозами. Крім того, такий підхід експоненційно збільшує кількість повідомлень безпеки, які доводиться обробляти й без того навантаженим ІБ-фахівцям. Якщо команди фахівців об'єднають рішення у використанні вендорів і застосують відкритий, інтегрований і спрощений підхід до безпеки, вони зможуть знизити свою вразливість до загроз.

За даними досліджень Flashpoint, BEC є куди більш ефективним методом здобування прибутку [6]. Звичайно, BEC-атака використовує пошту, найчастіше із застосуванням спуфінгу (від англ. spoof – містифікація, підміна; спуфінг – ситуація, в якій програма успішно маскується під іншу шляхом фальсифікації даних і дає змогу одержати незаконні переваги) для того, щоб виглядати як лист від колеги. Такі листи відправляються фінансовим працівникам, які можуть здійснювати грошові перекази. Зловмисник, як правило, проводить попереднє вивчення компанії, її ієрархії й співробітників, їх профілів у соціальних мережах, щоб воєдино зібрати ланцюжок ухвалення рішення. Лист може виглядати адресованим від генерального директора або іншого вищого співробітника й містити прохання відправити грошовий переказ бізнес-партнерові або вендору. У листі буде викладена необхідність терміново виконати дану операцію, що здебільшого закінчується переведенням коштів у локальний або іноземний банк на рахунок зловмисника.

Такий тип шахрайства спрямований на великий бізнес, а він стає його жертвою, навіть маючи серйозні системи захисту від загроз і від фрода (від англ. fraud – шахрайство – вид шахрайства у сфері інформаційних технологій, зокрема несанкціоновані дії й неправомірне користування ресурсами й послугами в мережах зв'язку). Facebook і Google у числі інших постраждали від подібних атак. Даний тип атак не містить шкідливих компонентів або підозрілих посилань і зазвичай обходить більшість комплексних рішень захисту. Internet Crime Complaint Center (IC3) у партнерстві із ФБР, Міністерством юстиції США й National White Collar Crime Center надав звіт про збиток в $5,3 млрд., украдених унаслідок фрода BEC з жовтня 2013 по грудень 2016 р., у середньому це $1,7 млрд. на рік. Для порівняння, дохід програм-здирників за 2016 р. становив порядку $1 млрд. За зазначений період часу в США зареєстровано 22 300 випадків фрода з використанням BEC [7].

Для боротьби з BEC-фродом потрібно поліпшувати бізнес-процеси, а не інструментарій захисту. Організаціям рекомендується перевіряти дозвіл на грошові перекази за допомогою окремого співробітника, який буде, наприклад, по телефону звіряти коректність операції. Що стосується інструментарію для захисту від таких атак, рекомендується застосовувати Sender Policy Framework (SPF) для захисту від підроблених електронних листів із підмінними адресами. Однак організації не поспішають включати даний функціонал, оскільки він може блокувати легітимні листи у разі некоректного налаштування IT-службою.

Слід відзначити еволюцію шкідливого ПЗ першої половини 2017 р., яка проливає світло на плани авторів цього ПЗ та їх стратегії – доставку, скритність і запобігання виявленню.

Зловмисники використовують системи поширення шкідників, що вимагають якої-небудь користувацької дії для своєї активації. Виявлена велика кількість шкідливих вкладень, які обходять автоматизовані «пісочниці» і доставляються користувачеві у вигляді

захищеного паролем шкідливого документу, пароль до якого «дбайливо» поданий у тілі листа, або виводить користувачу діалогове вікно, де потрібно натиснути кнопку дозволу («Натисніть ОК» тощо).

Творці malware використовують відкриті бази коду. Автори шкідливого ПЗ створюють свої продукти швидко й ефективно, використовуючи відкриті приклади коду, надані для навчання, який вони модифікують, щоб він не виглядав схожим на оригінал. Багато екземплярів програм-здирників засновані на open-source-коді для навчання.

Швидко ростуть платформи Ransomware-as-a-service (Raas). Такі платформи, як Satan, ідеальні для ледачих зловмисників, що бажають увійти на цей ринок і запустити успішну атаку без необхідності програмувати й виділяти ресурси для інноваційних типів атак. Оператори таких платформ забирають собі частину виторгу своїх передплатників, а деякі платформи навіть надають статистику заражень.

Безфайлові або «живучі в пам'яті» шкідники стають більш популярними. Вони ґрунтуються на технологіях Powershell або WMI для запуску шкідника повністю з пам'яті, без запису яких-небудь артефактів на жорсткий диск, поки зловмисник не захоче встановити модуль постійної присутності в системі.

Зловмисники все частіше покладаються на більш анонімну й децентралізовану інфраструктуру для приховування серверів C&C. Відзначається зростання використання так званих «мостових сервісів» для надання доступу до C&C-інфраструктури, яка розміщена в мережі TOR. Наприклад, такий сервіс, як Tor2Web, перенаправляє Інтернет-системи в Tor-мережу без необхідності установки якої-небудь клієнтської частини додатка.

Експерти Cisco з партнерами з RSA виявили, що атаки ланцюжка поставки приносять максимальні втрати за мінімальних витрат [9]. У розглянутому прикладі (Kingslayer) зловмисники інтегрували троян у легітимний софт, який зазвичай використовується системними адміністраторами для аналізу системних логів Windows. Компрометоване ПЗ було доступне для завантаження на сайті фірми-виробника разом з апдейтами. У такий спосіб вектор компрометації сайту виробника ПЗ призводить до цілої низки компрометацій компаній, що використовують це ПЗ, завантажене з легітимного сайту. Ситуація значно погіршується, якщо ПЗ має автоматичне оновлення із сайту виробника.

Для захисту від даного виду загроз одним із найкращих інструментів буде захист на рівні хоста, що повідомляє співробітників ІБ про всі компоненти, що йдуть у комплекті з ПЗ, і про те, які зовнішні комунікації вони встановлюють.

Проксі-сервери використовуються з часів зародження Web, на поточний день ІБ-служба найчастіше застосовує їх для аналізу контенту з метою виявлення потенційних загроз. Такі загрози включають:

- потенційно не потрібне ПЗ, наприклад шкідливі розширення для браузера;
- трояни-дроппери (дроппер – сімейство шкідливих програм, як правило, троянських, призначених для несанкціонованого і прихованого від користувача встановлення інших шкідливих програм, які містяться в тілі дроппера або завантажуються через мережу);
- трояни-завантажувачі (завантажувач операційної системи – системне ПЗ, яке забезпечує завантаження ОС безпосередньо після вмикання комп’ютера);
- посилання на WEB Scam і AD-фрод;
- вразливості з боку браузера, такі як JavaScript і рушій рендерингу зображень;
- редіректи браузерів, clickhacking та інші методики перенаправлення користувачів на шкідливий Web-контент.

Більшість представленого сьогодні ПЗ, що відноситься до класифікації PUA, насправді є шпигунським ПЗ. Виробники PUA позиціонують його як легітимний софт для надання зручних інструментів і сервісів, але незалежно від того, як вони це обставляють, шпигунське ПЗ – це теж саме malware.

Програми-шпигуни, маскуючись під PUA, збирають і передають інформацію про користувача, комп'ютер і його активності. Найчастіше spyware встановлюється на комп'ютер жертви без її відома.

Аналітична компанія IDC прогнозує, що в кінці 2017 р. видатки на забезпечення кібербезпеки в усьому світі сягнуть $81,7 млрд., що на 8,2% більше, ніж у 2016 р. За таких темпів до 2020 р. обсяг ринку перевищить $100 млрд. [8].

За даними IDC, у 2017 р. постачальники програмних та апаратних засобів, орієнтованих на безпеку, зароблять $81,7 млрд. IDC також очікує збереження динаміки: сукупні темпи річного приросту у найближчі три роки будуть становити 8,7% і до 2020 р. сягнуть $105 млрд. [9].

За прогнозами IDC, ще три галузі – безперервне виробництво, професійні послуги й

телекомунікації – витратять у 2017 р. близько $5 млрд. на продукти, пов'язані із забезпеченням безпеки [10].

Більша частина видатків на безпеку припадає на сервісний сегмент: компанії витрачають на інтеграційні й консалтингові послуги, а також послуги керування ІБ у 2017 р. близько $31,2 млрд., що становить близько 38% від загальносвітового значення. Найбільша стаття видатків – мережна безпека ($15,2 млрд.), захист робочих станцій і персональних пристроїв на другому місці – $10,2 млрд.

Категорії технологій, які покажуть найбільше зростання до 2020 р.: ПЗ для оцінки уразливості устаткування (16%); оцінка вразливості ПЗ (14,5%); сервіси керування ІБ (12,2%); аналіз поведінки користувачів (12,2%); уніфіковане керування загрозами (11,9%). Найбільшим ринком із географічного погляду залишаються США ($36,9 млрд. у 2017 р.), далі – Західна Європа ($19,2 млрд.), Азіатсько-Тихоокеанський регіон за винятком Японії – 18,5% [11].

Дві третини видатків становлять компанії, що належать до великого й дуже великого бізнесу. ДО 2019 р., на думку аналітиків IDC, розміри видатків корпорацій зі штатом більше 1 000 осіб, подолають планку в $50 млрд. [4].

За даними підготовленого компанією Cisco Systems звіту щодо інформаційної безпеки за 2017 р. (Annual Cybersecurity Report, ACR), більше третини організацій, чиї інформаційні системи були зламані в 2016 р., повідомили про істотні (понад 20%) втрати доходів, втрачені можливості й відтік замовників. 90% цих організацій після атак стали вдосконалювати технології й процеси захисту від загроз, розділяючи функції IT і забезпечення ІБ (38%), інтенсифікуючи тренінги з ІБ (38%) і впроваджуючи методи зниження ризиків (37%). У порівняльному дослідженні рішень безпеки, що проводився в рамках підготовки Cisco ACR (Security Capabilities Benchmark Study), взяли участь майже 3 тис. директорів з ІБ та керівників ІБ-підрозділів [12, с. 255].

Основними перешкодами на шляху просування стратегічних планів захисту є бюджетні обмеження, недостатня сумісність систем і відсутність кваліфікованих фахівців. Керівники підрозділів ІБ також відзначають той факт, що структури їхніх підрозділів постійно ускладнюються, і вже понад 65% організацій використовують від шести до 50 й більше продуктів ІБ, що потенційно сприяє утворенню проломів у захисті.

Як свідчать дані звіту Cisco ACR, кіберзлочинці користуються цими проломами, відроджуючи такі «класичні» напрями атак, як рекламне ПЗ та поштовий спам, причому рівні останнього зашкалюють до показників, яких не спостерігалося з 2010 р. На спам припадає майже дві третини (65%) повідомлень усієї електронної пошти, з них 10% розглядаються як небезпечні. Зростає глобальний обсяг спама, який розповсюджується великими ботнетами.

У цих умовах критичним фактором стає оцінка ефективності методів забезпечення інформаційної безпеки. Компанії невпинно працюють над скороченням часу виявлення (time to detection, TTD), тобто часу від компрометації до виявлення загрози. Чим менший час виявлення, тим більше обмежений оперативний простір атакуючих і менше наслідків вторгнень [5].

Починаючи з 2016 р. хакерські групи стали більш «корпоративними». Зумовлені цифровізацією динамічні зміни технологічного пейзажу відкривають перед кіберзлочинцями нові можливості. З одного боку, атакуючі продовжують користуватися перевіреними часом технологіями, з іншого – вдаються до нових методів, що відображають структуру керування «середньої верстви» їхніх корпоративних мішеней.

Нові методи атак імітують корпоративну ієрархію. У низці кампаній із поширення шкідливої реклами використовуються т. зв. брокери, або «шлюзи», які діють як менеджери середньої ланки, що маскують шкідливу активність. Це дає змогу зловмисникам прискорювати свої дії, захоплювати операційний простір та уникати виявлення.

Позитивним моментом стало падіння популярності таких великих наборів експлойтів, як Angler, Nuclear і Neutrino, діяльність власників яких була припинена в 2016 р., але на їхнє місце ринулися дрібніші гравці.

У звіті з безпеки за 2007 р. було відзначено 4 773 попередження про порушення безпеки Cisco IntelliShield Security Alerts, що відповідало рівню Національної бази даних уразливостей (National Vulnerability Database). У звіті ж 2017 р. число оприлюднених вендорами попереджень про вразливості за аналогічний період виросло на 33% і становило 6 380 [5]. Насамперед, таке зростання зумовлене більшою інформованістю в питаннях безпеки, розширенням сектору атак і посиленням активності зловмисників.

Якщо раніше експерти в переважній своїй більшості рекомендували прийняти цілісний під-

хід до забезпечення ІБ, інтегрувати інструментарій, процеси й політики, вести просвітницьку діяльність серед зацікавлених осіб, то сьогодні перед директорами ІБ постала проблема надзвичайної ускладненості середовища.

Необхідно із цим боротися шляхом архітектурного підходу до ІБ і допомагаючи витягати максимальну користь із наявних інвестицій, збільшуючи можливості й зменшуючи складність захисту підрозділів [13, с. 320]. Більшість керівників компаній розуміє, що відповідають за ІБ та захист даних поза залежністю від конкретного місця й часу виникнення загроз в інформаційних системах підприємства. Для забезпечення належного рівня захисту необхідні процеси та інструменти збору й аналізу інформації про інформаційні загрози в режимі реального часу, а також обмін цими даними між компаніями [14, с. 235].

Управління кіберзагрозами – це багатобічний, складний процес, у якому використовуються кілька взаємозалежних систем збору, зіставлення й аналізу інформації про загрози, одержаної з різних джерел.

Хмарно орієнтований підхід допомагає зробити цей процес простішим, поєднуючи й застосовуючи аналіз із декількох джерел і рішень і забезпечуючи безпеку даних. Хмарна модель надає обчислювальну потужність, необхідну для моніторингу та аналізу всього процесу обміну інформацією у цифровому форматі, і створює єдине сховище даних, з якого витягають відомості, необхідні для вживання практичних заходів захисту.

Хмарна система збору інформації про загрози дає змогу вибудувати превентивний захист від вторгнень. В остаточному підсумку це дасть змогу підприємствам створювати конкурентні переваги, засновані на захисті даних клієнтів, активів підприємства й репутації бренда.

Моніторинг та аналіз даних у режимі реального часу – основні засоби управління попередженням інформаційних загроз. Ці технології забезпечують контекстний підхід до загроз і дають змогу зрозуміти тактику, методи й послідовність дій зловмисників. Об'єднавши інструменти аналітики й обробки даних про загрози в хмарному середовищі, можна створити єдине джерело, що охоплює усі дані компанії й зовнішніх постачальників.

Адаптивна автентифікація стала ще одним популярним трендом у сфері ІБ. У міру збільшення обсягу інформації в інформаційних системах компанії починають використовувати окремі елементи даних для виявлення підозрілих дій і алгоритмів. В адаптивній автентифікації для виявлення незвичайної поведінки використовуються такі параметри, як час входу користувача в систему, його місце розташування, графік роботи, вид використаного пристрою й інших.

Здійснення адаптивної автентифікації ускладнюється відсутністю універсальних рішень. Тому для визначення параметрів ризику шкідливої активності використовується сполучення наявних інструментів і засобів аналізу їхньої поведінки на базі системи керування інформацією та подіями (SIEM) ІБ. З ускладненням механізму кібератак багато організацій почали ділитися інформацією про загрози з колегами, галузевими групами й органами державної влади, щоб спільними зусиллями вдосконалити збір інформації про кібератаки і поліпшити заходи забезпечення ІБ.

Обмін інформацією може забезпечити організацію даними, на підставі яких можна вживати конкретні заходи, виявляти основні ризики компанії й підвищувати оперативність виявлення інцидентів у сфері ІБ й реагування на них. Для того щоб уважатися по-справжньому ефективною, система обміну інформацією має бути здатна обробляти дані, аналізувати різні дії, підтверджувати наявність загрози, визначати її тип і повідомляти про виявлені загрози в режимі реального часу. Вона також повинна служити джерелом контекстної інформації про вплив загроз на сферу діяльності організації й індустрії.

Як і у випадку з будь-якою іншою новою платформою, що повинна бути сумісна з декількома окремими системами, різними типами даних і зовнішніх організацій, створення такої системи обміну даними пов'язане з низкою серйозних труднощів. Головною проблемою серед них є відсутність єдиної концепції обміну даними.

Висновки з цього дослідження. Різноманітність атак відображає складність сучасного ландшафту загроз ІБ. Чим інтенсивніше зростає й розвивається ринок Інтернету речей, тим із більшим числом труднощів його захисту доведеться зіштовхнутися фахівцям з ІБ. Організації, яка захищається, навіть упевненій у засобах захисту, доводиться діяти в умовах наявності складних систем і недоліку персоналу, що дає атакуючим перевагу в часі й оперативному просторі. Для запобігання, виявлення й усунення наслідків атак, а також для мінімізації ризиків будуть корисними такі рекомендації:

- забезпечення ІБ має стати одним із бізнесів-пріоритетів. Топ-менеджери повинні

безпосередньо відповідати за безпеку, пропагувати її й фінансувати на пріоритетній основі;

• оцінка операційної дисципліни. Необхідно провести ревізію методів захисту, корегування ПЗ, точок контролю доступу для мережних систем, додатків, функцій і даних;

• тестування ефективності захисту. Варто задати чіткі метрики та використати їх для оцінки й удосконалення методів захисту;

• прийняття інтегрованого підходу до захисту. Інтеграція й автоматизація повинні перебувати на верхніх рядках списку критеріїв оцінки заходів для поліпшення контролю, вдосконалення взаємної сумісності та скорочення часу виявлення і припинення атак. У цьому разі підрозділи забезпечення ІБ зможуть зосередитися на аналізі й усуненні реальних загроз.

ЛІТЕРАТУРА:

1. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем / М.В. Грайворонський, О.М. Новіков. – К. : BHV, 2009. – 608 с.

2. Остапов С.Є. Технології захисту інформації / С.Є. Остапов, С.П. Євсеєв, О.Г. Король. – Харків : ХНЕУ, 2013. – 476 с

3. Тоффлер Э. Шок будущего / Э. Тоффлер. – М. : АСТ, 2001. – 560 с.

4. Азеев А.С., Чайковська М.П. Моделювання комплексної системи інформаційної безпеки організацій в сучасних економічних реаліях / А.С. Азеев, М.П. Чайковська // Global aspects of World Economy and International Relations in an unstable economy. – Polska, Czestochowie, Akademia Polonia, 2016. – p. 879–889.

5. Cisco 2017 Midyear Cybersecurity Report. – Cisco, 2017. – 90 с.

6. «Business E-mail Compromise, E-Mail Account Compromise: The 5 Billion Dollar Scam» // Internet Crime Complaint Center (IC3) and the Federal Bureau of Investigation (FBI) [Електронний ресурс]. – Режим доступу : ic3.gov/media/2017/170504.aspx.

7. Kingslayer – a supply chain attack // RSA [Електронний ресурс]. – Режим доступу : rsa.com/en-us/resources/kingslayer-a-supply-chain-attack.

8. Worldwide Semiannual Security Spending Guide // IDC [Електронний ресурс]. – Режим доступу : idc.com/getdoc.jsp?containerId=IDC_P33461.

9. Annual Cybersecurity Report 2017 // Cisco [Електронний ресурс]. – Режим доступу : b2me.cisco.com/en-us-annual-cybersecurity-report-2017.

10. 2017 Midyear Cybersecurity Report. – Cisco, 2017. – 90 с.

11. Internet Security Threat Report // Symantec – 2017. – 77 с.

12. Азєєв А.С., Чайковська М.П. Управління якістю системи інформаційної безпеки WEB-додатків / А.С. Азєєв, М.П. Чайковська // Проблеми та перспективи ринково-орієнтованого управління підприємствами: теорія, методологія, практика : [монографія] / За ред. Ю.М. Сафонова. – К. : КМА, 2015. – С. 254–267.

13. Азєєв А.С., Чайковська М.П. Управління системою інформаційної безпеки підприємства на базі ЛСП / А.С. Азєєв, М.П. Чайковська // Моделювання та інформаційні технології в економіці : [монографія] / За ред. В.М. Соловйова. – Черкаси : Брама-Україна, 2014. – С. 306–328.

14. Азеев А.С., Чайковская М.П. Применение процессного подхода к управлению информационной безопасностью при реализации ИКТ-проектов / А.С. Азеев, М.П. Чайковская // Материалы VI В Международной научно-практической конференции «Развитие современных экономических систем: вызовы и альтернативы XXI столетия». – Кишинев : Славянский університет, 2016. – С. 232–237.