УДК 004.056

Гахов С.О.

ЗАСТОСУВАННЯ ПОЛОЖЕНЬ ІМУНОЛОГІЇ В ТЕОРІЇ ЗАХИЩЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

У статті досліджуються питання застосування положень імунології в теорії захищених інформаційних систем. Розглянуто принципи функціонування імунної системи живих організмів як основних тверджень теорії захищених інформаційних систем. Встановлено перспективний напрямок розвитку теорії захищених інформаційних систем.

Ключові слова: захищена інформаційна система, кібернетична безпека, кібернетичний захист, імунна система безпеки.

Постановка проблеми. За даними науково-дослідної групи IBM X-Force в 2017 році стався витік понад 2,9 млрд. даних. В результаті кібервимагання компанії втратили більше 8 млрд. дол. США через простій, різного роду витрат і оплати викупу [1]. Число кібератак на впровадження шкідливого коду (в основному, компонентів технологій ботнет і блокчейн) в інформаційні системи в 2017 році збільшилася майже вдвічі і склала 79 відс. всієї шкідливої активності в корпоративних мережах [1]. Особливу небезпеку представляли шкідливі програми WannaCry, NotPetya і Bad Rabbit, які автоматично поширювалися мережею без взаємодії з користувачем і мали деструктивний характер [1].

За оцінками компанії Distil Networks у 2017 році 42,2 відс. загального обсягу інтернет-трафіку було згенеровано ботами. При цьому боти APBs (Advanced Persistent Bots), які реалізують складні функції та мають здатність імітувати поведінку людини-користувача, згенерували 74 відс. об'єму загального трафіку ботів [2].

Швидке зростання трафіку центрів обробки даних (ЦОД) визначається зростом користування хмарними сервісами. Згідно зі звітом компанії Cisco [3] до 2021 року глобальний річний трафік хмарних ЦОД зросте в 3,3 рази і досягне 19,5 зеттабайт (ЗБ) (в 2016 році – 6 ЗБ), річний приріст (CAGR) за вказаний період складе 27 відс. Глобальний хмарний трафік до 2021 року досягне 95 відс. сукупного трафіку ЦОД, в 2016 році цей показник складав 88 відс.

Крім того, стрімкий розвиток та поширення додатків Інтернету речей (Internet of Things, IoT), "розумні" міста і автомобілі, інформаційні системи охорони здоров'я та енергетики, вимагають масштабованих обчислень і нових рішень для зберігання даних. До 2021 року компанія Cisco прогнозує зростання IoT-підключень до 13,7 млрд (показник 2016 року – 5,8 млрд) [Cisco].

Це тільки деякі оцінки, які говорять про актуальність проблеми забезпечення кібернетичної безпеки інформаційних систем та пошуку нових підходів та розвитку теорії захищених інформаційних систем.

Аналіз останніх досліджень і публікацій за темою статті. Необхідно відзначити, що ускладнення інформаційної технології і прискорення процесів виведення на ринок IT-продуктів призводить до зростання числа вразливостей інформаційних систем. Зловмисники стають більш компетентними в інформаційних технологіях і психології людини. Кібератаки стають усе більш цілеспрямованими, просунутими, наполегливими і тривалими.

Підхід до забезпечення кібербезпеки корпоративних інформаційних систем, заснований на застосуванні комплексів різноманітних, фрагментованих, точкових, відокремлено функціонуючих компонентів захисту, збільшує інфраструктуру, ускладнює роботу фахівців, не призводить до суттєвого поліпшення стану та гарантій кібербезпеки.

Деякі компанії та організації використовують не менше 85 продуктів безпеки від більш ніж 40 постачальників одночасно [4]. Це супроводжується величезними витратами усіх видів ресурсів. При цьому рівень загроз не тільки не зменшується, а, навпаки, збільшується.

Провідні виробники рішень в області кібербезпеки вже сьогодні заявляють про можливість побудови "інтегрованої та інтелектуальної імунної системи безпеки" (integrated and intelligent security immune system) як результату "комплексного та цілісного підходу,

заснованого на когнітивному ядрі організаційної та аналітичної безпеки, яке розуміє, пояснює і впізнає множину змінних ризику у всій екосистемі пов'язаних можливостей" [4].

Сьогодні передові підходи до забезпечення кібербезпеки корпоративних інформаційних систем базуються на широкому застосуванні засобів автоматизації діяльності фахівців з кібербезпеки. Для сучасного етапу розвитку систем забезпечення кібербезпеки характерно застосування інформаційних систем класу SIEM (Security information and event management), які лежать в основі сучасного SOC (Security operations center), але прийняття рішення щодо відповіді на виникаючі кіберінциденти залишається за людиною – адміністратором безпеки.

Постановка завдання. В умовах зростання розмаїття та складності інформаційних технологій відбувається все більше загострення проблеми забезпечення кібербезпеки інформаційних систем. Нагальна потреба вирішення даної проблеми визначає необхідність пошуку нових підходів в теорії і практиці забезпечення кібербезпеки інформаційних систем.

Принципи функціонування складних інформаційних систем в умовах розмаїття кібернетичних вплив необхідно шукати в таких науках як фізіологія та імунологія. Тому, метою даної статті є дослідження можливостей застосування положень імунології в теорії захищених інформаційних систем.

Основний матеріалу дослідження. Корпоративні інформаційні системи виступають в ролі інформаційної інфраструктури – середовища існування бізнес-процесів підприємств, організацій і установ. Для сучасних корпоративних інформаційних систем характерні: структурна масштабованість; територіальна і часова рознесеність; функціональна розширюваність; різноманітність цілей створення, користувачів, інформаційних ресурсів і технологій, що визначає все зростаючу їх складність.

Необхідно підкреслити, що корпоративну інформаційну систему необхідно розглядати як цілісну систему – окрему сутність в кіберпросторі, яка повинна виконувати функції за призначенням та проявляти властивості функціональної стійкості в умовах деструктивних кібернетичних впливів.

Аналіз показав, що основними причинами виникнення деструктивних процесів функціонування інформаційних систем є:

властивості функціональних компонентів даної інформаційної системи;

властивості впроваджених зловмисником функціональних компонентів в дану інформаційну систему;

переходи інформаційної системи в небезпечний стан внаслідок ненавмисних дій користувачів.

Необхідно відзначити, що при вирішенні проблеми забезпечення кібербезпеки на передній план виходять не цілі забезпечення прояву властивостей інформації, яка захищається, а цілі забезпечення безпеки процесів функціонування інформаційних систем. Необхідно забезпечувати функціонування корпоративної інформаційної системи в умовах кібернетичних впливів таким чином, щоб у ній виникали тільки ті процеси (функціональні системи), які відповідають цілям створення даної системи.

Наглядним екстремальним прикладом для розвитку теорії захищених інформаційних систем є імунна система живих істот. У [5, с. 14] зазначається, що "саме сукупність імунологічних процесів, збалансована діяльністю "імунологічного оркестру", забезпечує і захищає життя багатоклітинних організмів, що населяють планету Земля. У людини поліморфізм генів імунної відповіді, що входять в головний комплекс гістосумісності, найбільш високий у порівнянні з іншими біологічними видами. Це, зокрема, зумовило переважний розвиток Homo sapiens і дало йому як виду додаткові можливості для виживання і захисту від зовнішньої (інфекції, алергени) і внутрішньої (мутації, онкоперероджження і інших генетично опосередкованих змін) агресій".

Ключовим поняттям імунології є "імунітет". Аналіз підходів науковців до визначення поняття "імунітет" (табл. 1) показав їх розмаїття та неоднозначність. Поняття "імунітет" розглядається з різних кутів зору як "сукупність реакцій", як "здатність", як "стан", як

“фізіологічна форма”, як “біологічна властивість”, як “спосіб захисту”, як “біологічний феномен”.

Таблиця 1

Підходи до визначення поняття “імунітет”

Автори визначення, джерело	Зміст поняття
Кузнецова Л.В., Бабаджан В.Д., Харченко Н.В. та ін. [8, с. 9]	Імунітет – це еволюційно обумовлена сукупність реакцій взаємодії між системою імунітету і біологічно активними агентами (антигенами), що направлені на збереження фенотипічної постійності внутрішнього середовища (гомеостазу) організму.
Ярилин А.А. [7, с. 28]	Імунітет – це здатність багатоклітинних організмів підтримувати сталість свого макромолекулярної складу шляхом видалення чужорідних молекул, що забезпечує стійкість до інфекційних агентів і резистентність до пухлин.
Хаитов Р. М. [5, с. 24, 25]	Імунітет – особлива біологічна властивість багатоклітинних організмів, в нормі призначене для захисту від генетично чужорідних факторів, включаючи інфекційних агентів та інших зовнішніх патогенів, здатних при попаданні у внутрішнє середовище вступати в міцні зв’язки з клітинами та/або міжклітинною речовиною. Терміном “імунітет” позначають: стан несприйнятливості організму до дії носія чужорідної генетичної або антигенної інформації (бактерії, віруси, рикетсії, паразити, гриби, клітини чужорідного трансплантата або пухлин і ін.); реакції імунобіологічного захисту організму проти чужорідних антигенів; фізіологічну форму імуногенної реактивності організму, що спостерігається при контакті клітин імунної системи з генетично або антигенно чужорідною структурою. Така структура блокується і руйнується.
Ганковская Л.В. и др. [9, с. 11]	Імунітет – спосіб захисту організму від живих тіл і речовин, що несуть ознаки генетично чужорідної інформації (включаючи мікроорганізми, чужорідні клітини, тканини або генетично змінені власні клітини, в тому числі пухлинні).
Климов В.В. [10]	Імунітет (immunity) – це біологічний феномен, який полягає в довготривалій самопідтримці всередині окремого організму балансу між генетично “своїм” і “несвоїм” в умовах чужорідного оточення.

Для конструктивного застосування поняття “імунітет” в теорії захищених інформаційних систем його треба розглядати:

як складну властивість, яку проявляє організм в умовах виникнення функціональних систем, які відповідають меті чужорідних агентів (відповідає виразу – “проявляє імунітет”);

як стан несприйнятливості організму до дії функціональних систем, які відповідають меті чужорідних агентів (відповідає виразу – “має імунітет”).

“Стратегічною функцією” системи кібернетичної безпеки має бути забезпечення (тобто створення необхідних і достатніх умов) функціонування корпоративної інформаційної системи за призначенням в умовах кібернетичних впливів.

Основними “тактичними функціями” системи кібернетичної безпеки в інформаційних системах повинні бути:

захист від втілення “чужих” функціональних компонентів і виникнення “чужих” процесів функціонування;

елімінація (усунення, блокування) модифікованих “своїх” функціональних компонентів і виникнення ненавмисних процесів функціонування в системі;

управління складом функціональних компонентів інформаційної системи і контроль за процесами її функціонування.

Дані функції в живому організмі реалізуються механізмами вродженого і адаптивного імунітетів (рис.1).

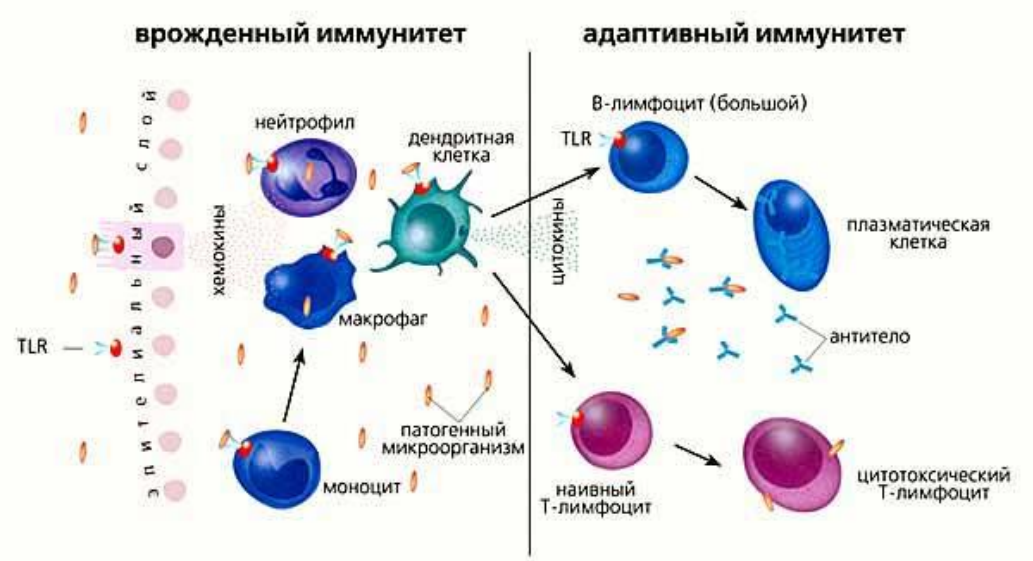

Рис. 1. Схема імунної відповіді на втілення патогенних мікроорганізмів [6]

У [7, с. 23] зазначається, що “перша умова формування імунітету – наявність замкнутої території, яка “охороняється”, з її обов’язковим відмежуванням від зовнішнього середовища. Друга умова – поява факторів, спеціалізованих для забезпечення сталості внутрішнього середовища, яке охороняється, шляхом її вивільнення від агентів, які проникли ззовні (тобто для забезпечення імунітету в його прямому первісному сенсі – вивільнення)”. Звідси, основними принципами побудови захищених інформаційних систем слід вважати принцип “захищеного периметра” і принцип “захищеного внутрішнього середовища”.

Сучасний захист “периметра” корпоративної інформаційної системи забезпечується технологіями шлюзів безпеки (UTM), міжмережевого екранування (FW), віртуальних приватних мереж (VPN), виявлення та запобігання вторгнень (IDS/IPS), ідентифікації та аутентифікації суб’єктів та ін. “Захищене середовище” забезпечують технології антивірусного захисту (AV), запобігання витоків даних з інформаційної системи зовні (DLP), моніторингу стану кібербезпеки (SIEM) і ін. Але треба розуміти, що сучасні інформаційні системи на кілька порядків простіші між живі організми.

У [7, с. 24] зазначається, що “важлива умова ефективної роботи цього гомеостатичного механізму – здатність захисних клітин відрізняти потенційно агресивні чужі клітини від власних”. Загальний принцип розпізнавання чужорідних агентів та необхідність його реалізації спонукає до пошуку методів та побудови ефективних систем розпізнавання процесів функціонування інформаційних систем, які відповідають меті їх створення.

У ході реакції імунної системи організму виникають функціональні системи, які реалізують вроджений та адаптивний імунітет. Існують відмінності принципів розпізнавання чужорідних агентів. Під час прояву вродженого імунітету розпізнавання здійснюється за ідентифікаторами цілих груп подібних чужорідних агентів, які виступають в якості образів (паттернів) патогенності. Під час прояву адаптивного імунітету розпізнавання здійснюється

за ідентифікаторами конкретних індивідуальних чужорідних агентів або їх дуже подібних невеликих груп із формуванням імунної пам'яті.

"Адаптивний імунітет має ще одну перевагу, відсутнє у вродженого імунітету – здатність захищати організм від агресії зсередини (тобто від злоякісних новоутворень)" [7, с. 28]. Це визначає необхідність реалізації функції виявлення "чужих" функціональних компонентів і виникнення "чужих" процесів функціонування на будь-якому функціональному рівні інформаційної системи.

Сучасні підходи до забезпечення кібернетичної безпеки корпоративних інформаційних систем базуються на функціональних системах, які виникають в середовищі "людина – SIEM-система – компоненти та процеси інформаційної системи". В основі механізму інтелектуальної обробки даних сучасних SIEM-систем лежить контекстна, поведінкова і часова аналітика.

Так, наприклад, в IBM QRadar SIEM дана функція реалізується за допомогою механізму правил, які створюються (custom rules engine, CRE). Кожне з типів правил (правила події, потоку, загальне, порушення, порогове, поведінкове, аномалії) виступає образом для моніторингу стану інформаційної системи, який застосовується для кореляції вхідних даних із різних джерел різних функціональних рівнів інформаційних систем в реальному часі.

У своєму розвитку системи забезпечення кібербезпеки пройшли такі основні етапи еволюції, які тісно пов'язані з розвитком інформаційних технологій:

розробка і застосування окремих компонентів, які реалізують конкретні функції захисту;

застосування комплексів компонентів, що реалізують певну множину функцій захисту;

створення і застосування автоматизованих систем забезпечення кібербезпеки (використання інформаційних систем класу SIEM).

Можна спрогнозувати, що наступний етап еволюції систем забезпечення кібербезпеки інформаційних систем буде характеризуватися створенням і застосуванням автоматичних систем забезпечення кібербезпеки, здатних реалізовувати когнітивну функцію (рис. 2).

Рис.2. Етапи еволюції систем забезпечення кібернетичної безпеки та їх перспективи розвитку

Висновки. Перспективним напрямком збагачення теорії захищених інформаційних систем та їх реалізації є усвідомлення та застосування здобутків фізіології та імунології.

Основними напрямками розвитку системи забезпечення кібернетичної безпеки корпоративних інформаційних систем є інтеграція технологій захисту в єдину систему кібербезпеки, широка інтелектуалізація реалізації функцій захисту і автоматизація процесів забезпечення кібербезпеки.

На нашу думку, використання принципів функціонування імунних систем живих організмів призведе до подальшого розвитку теорії та практики забезпечення кібербезпеки інформаційних систем.

Знання напрямків і перспектив розвитку теорії та практики забезпечення кібернетичної безпеки корпоративних інформаційних систем необхідно для подальших наукових досліджень у цій галузі, обґрунтування вимог до систем кібербезпеки та їх створення, а також для підготовки майбутніх фахівців.

Список використаних джерел:

1. IBM X-Force Threat Intelligence Index 2018 [Електронний ресурс] – Режим доступу: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=77014377USEN.

2. Distil Networks. 2018 Bad Bot Report. The Year Bad Bots Went Mainstream [Електронний ресурс] – Режим доступу: http://www.gmi.com/wp-content/uploads/2018/04/General-Microsystems_2018-bad-bot-report.pdf.

3. Cisco Global Cloud Index: Forecast and Methodology, 2016–2021 [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.pdf.

4. The security immune system [Електронний ресурс] – Режим доступу: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEB03029USEN.

5. Хаитов Р. М. Иммунология: учеб. / Р. М. Хаитов. – 2-е изд., перераб. и доп. – М.: ГЭОТАР-Медиа, 2011. – 528 с.: ил.

6. Лебедев К. А. Новый этап развития иммунологии / К. А. Лебедев, И. Д. Понякина // Природа. – 2006. – № 4. – С. 3-10.

7. Ярилин А. А. Иммунология: учебник / А. А. Ярилин. – М.: ГЭОТАР–Медиа, 2010. –752 с.: ил.

8. Імунологія: підручник / Л. В. Кузнецова, В. Д. Бабаджан, Н. В. Харченко та ін.; за ред. Л. В. Кузнецова, В. Д. Бабаджан, Н. В. Харченко. – Вінниця: ТОВ «Меркьюрі Поділля», 2013.– 565 с.

9. Основы общей иммунологии: Учеб. пособие для студентов мед. вузов / [Ганковская Л.В. и др.]; под ред. Л.В. Ганковской, Л.С. Намазовой-Барановой, Р.Я. Мешковой. – М.: ПедиатрЪ, 2014 – 124 с.

10. Климов В.В. Основы общей иммунологии. Мультимедийный курс по иммунологии [Электронный ресурс] – Режим доступа: http://www.immunology.klimov.tom.ru/Demo_ru/Index.html.

Надійшла: 27.01.2018 Рецензент: к.т.н. Довбешко О.А.