ЗАХИСТ ІНФОРМАЦІЇ

УДК 004.681.3

Г.М. Гулак

ПОНЯТІЙНИЙ АПАРАТ ТА МОДЕЛЬ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

У статті розглядаються різні підходи до визначення понятійного апарату та термінів, що обумовлені проблемою забезпечення кібернетичної безпеки, а також до побудови моделі такої безпеки.

***Ключові слова**: кібернетичний простір, кібернетична безпека, модель.*

В статье рассматриваются понятийный аппарат и термины, обусловленные проблемой обеспечения кибернетической безопасности, а также создания модели такой безопасности.

***Ключевые слова:** кибернетическое пространство, кибернетическая безопасность, модель.*

Models and terms for carrying out of cyber security are considered.

***Keywords:** cyberspace, cyber security, model.*

Вивчення виданих у 2011–2012 рр. аналітичних оглядів провідних експертів з питань інформаційної безпеки [1, 2] свідчить про вступ світового суспільства до якісно нової фази протиборства у глобальному інформаційному просторі. Ця фаза характеризується:

- колосальними масштабами проведення атак по географії розповсюдження шкідливих кодів шпигунських програм, а також інтенсивності фіктивних запитів у випадку проведення DDoS атак на інформаційні ресурси;
- широким спектром об'єктів атак (у переважної більшості це автоматизовані системи урядових установ, збройних сил, правоохоронних органів та великих комерційних компаній);
- активними та скоординованими діями порушників що застосовували кваліфіковано спроектовані засоби нападу.

За різними оцінками, щорічні світові втрати від вандалізму кіберзлочинців складають від 290 до 750 мільярдів євро.

Необхідність відповіді на виклики сучасності потребує адекватних дій на урядовому рівні, зокрема, прийняття необхідних законодавчих актів, розробки стратегії реалізації організаційних та інженерно-технічних заходів щодо убезпечення не тільки інформаційно-комунікаційних технологій, а й усіх *інтелектуалізованих інфраструктур найважливіших галузей суспільного виробництва та забезпечення життєдіяльності людини.*

Саме наповнення "інтелектом" звичайних сфер транспорту, промисловості, енергетики, охорони здоров'я та багатьох інших за допомогою потужних комп'ютерів і вбудованих мікроконтролерів робить їх не тільки більш ефективними, життєво

важливими для кожної людини, народу і всього людства, але і, нажаль, більш вразливими до загроз антропогенного і техногенного характеру, природних катаклізмів.

Останнім десятиріччям у більшості провідних країн світу створені спеціальні урядові структури або ініційовані процеси формування органів, що покликані забезпечити безпеку національного інформаційного простору, критичних інфраструктур. Їх повноваження і зона відповідальності визначені з урахуванням історичних традицій, національних пріоритетів та законодавства.

Серед множини різних функцій цих органів слід відмітити найбільш важливу та загальну, а саме, в тому чи іншому формулюванні в якості пріоритету діяльності визначена задача забезпечення безпеки кібернетичного простору, захисту критично важливих для людини, суспільства і держави інфраструктур.

В документах Всесвітньої конференції міжнародного електрозв'язку WCIT-2012 (Дубай, ОАЕ, 3-14.12.12) відмічено, що відсутність узгодженого на міжнародному рівні визначення кібербезпеки стримує міжнародні та національні зусилля з захисту мереж і комп'ютерних систем, що фактично не мають границь.

Зауважимо, що вже на початку лютого поточного року (7.02.2013) була презентована стратегія дій Євросоюзу в області кібербезпеки. Її ключовою ланкою є директива, що зобов'язує уряди країн ЄС створити профільні адміністративні органи та забезпечити їх фінансування.

У світлі розв'язання актуальних проблем що стоять перед Україною в плані забезпечення національної безпеки нагальною постає задача визначення власних пріоритетів у цій сфері. Вирішення цього завдання неможливо без науково обґрунтованого термінологічного апарату та побудови моделей атак та захисту власного кричного середовища.

Таким чином, слід відповісти на такі питання:

– що таке "кібернетичний простір", "кібернетична безпека" і "забезпечення безпеки кіберпростору"?

– чим відрізняється "забезпечення безпеки кіберпростору" від "захисту інформації"?

Відповідь на останнє запитання зумовила два основних підходи до вирішення проблем у цій сфері.

Російський підхід фактично визнає існування такого феномену як кібернетичний простір, але на законодавчому рівні термін не закріплений.

Засадничий керівний документ РФ в області національної безпеки – Доктрина інформаційної безпеки [5] вводить поняття "інформаційна безпека", яке включає дві компоненти: "захищеність національного інформаційного простору від впливу зовні" та "захист інформаційних ресурсів в електронному вигляді".

Положення Доктрини в основному фокусуються на різних аспектах захисту інформації в такій категорії автоматизованих систем, як інформаційні та телекомунікаційні системи. Виходячи з контексту, можна припускати, що при цьому мова переважно йде про захист "змістовної", документальної інформації.

Разом з тим, слід відзначити той факт, що в сучасному промисловому світі постійно збільшується кількість використовуваних систем типу "автоматизовані системи управління технологічними процесами (АСУ ТП)" в тому числі, в областях особливо небезпечних для життя людини, включаючи управління різного роду хімічними виробництвами, усіма видами транспорту (включаючи повітряний, наземний і морський), керування виробництвом і розподілом електроенергії і т.д.

У той же час, в наукових колах, зокрема, у рамках американо-російських наукових симпозіумів в 90-х роках минулого сторіччя було відмічено виникнення такого феномену, як "кібернетичний простір" (Cyberspace) і його вплив на критичні галузі суспільного виробництва [3]. В наступних роботах російських вчених між поняттями "інформаційна безпека" і "кібернетична безпека", висловлюючись мовою математичних операцій, фактично ставлять знак "суворе включення" на користь першого [4].

Відсутність у ряді російських досліджень проблем "інформаційних воєн" чіткого розмежування між поняттями "захист від інформації" і "захист інформації" призводить до змішання методів і засобів інформаційно-психологічного впливу на населення з методами і засобами інженерно-технічних атак на цифрове інформаційний простір [6], визнання факту існування "кібернетичного простору" без його конкретного тлумачення [7].

У цих умовах, представляється логічним, слідуючи логіці захисту основних властивостей інформації, виділити соціально-політичні технології інформаційних війн в самостійну дисципліну [8], а також доцільно окремо досліджувати інженерно-технічні аспекти інформаційних війн [9].

При цьому інформаційну зброю слід класифікувати за характером його впливу на мережеві ресурси/ автоматизовані системи, окремо розглядаючи засоби нападу, що призначених для:

– утворення каналів витоку інформації з обмеженим доступом (мета – шпигунство, інакше порушення конфіденційності) або

– порушення штатного функціонування системи та/або руйнування технічних чи програмних засобів, а також цифрових інформаційних ресурсів (мета – диверсія, терор або порушення цілісності та доступності).

Що стосується США, офіційне тлумачення терміну "кіберпростір" було дано в ряді директив Білого дому [11]. Ці документи визначають кіберпростір як взаємозалежну мережу інфраструктур інформаційних технологій, включаючи Інтернет, телекомунікаційні мережі, комп'ютерні системи, а також процесори та контролери, вбудовані в критичні галузі виробництва.

До об'єктів потенційних атак цілями терористів віднесено сукупність об'єднаних життєво важливою інфраструктурою ключових ресурсів, що належать і керованих приватним сектором, державою або органами місцевого самоврядування. Слід звернути увагу, що в цих документах присутні два взаємодоповнюючих механізми безпеки: "охорона критичних структур" і "забезпечення безпеки кіберпростору".

Для реалізації федеральних завдань у сфері національної безпеки, запобігання атак і реагування на протиправні дії в мережевому середовищі було створено

у листопаді 2002 року – Міністерство національної безпеки США (US Department Homeland Security);

у січні 2013 на базі ФСБ Росії – державну систему виявлення, попередження і ліквідації наслідків комп'ютерних атак на інформаційні ресурси РФ [10].

Порівняльний аналіз підходів до забезпечення захищеності критичної інформаційної інфраструктури Росії від комп'ютерних атак і безпеки кіберпростору США дозволяє зробити висновок щодо їх збігу по ряду основних позицій і відмінності в деяких деталях. Головне в обох випадках – наявність потужного федерального центру що забезпечує організацію розслідувань інцидентів, технічну підтримку попередження атак, а також ліквідацію їх наслідків.

Певні завдання та повноваження щодо забезпечення кібернетичної безпеки делегуються органам, що забезпечують керування об'єктами критичної інфраструктури.

Зокрема, на поточний час в США діє план *NERC CIP* (*North American Electric Reliability Corporation critical infrastructure protection*) – керівний документ зі забезпечення безпеки магістральних електричних мереж, якій встановлює основні вимоги щодо провадження відповідної діяльності.

План *NERC CIP* включає 9 стандартів та 45 вимог щодо безпеки електронних периметрів та захисту критично важливих кібернетичних активів, а також роботи з персоналом і його навчання, управління безпекою та планування відновлення у випадку катастроф, у т. ч.

–*CIP*-002-1: "Ідентифікація критичних кібернетичних активів" (*Critical Cyber Asset Identification*);

– *CIP*-003-1: "Контроль управління безпекою" (*Security Management Controls*);

– *CIP*-004-1: "Персонал та навчання" (*Personnel and Training*);

– *CIP*-005-1: "Безпека електронного периметру" (*Electronic Security Perimeters*);

– *CIP*-006-1: "Фізична безпека критичних кібернетичних активів" (*Physical Security of Critical Cyber Assets*);

– *CIP*-007-1: "Менеджмент безпеки систем" (*Systems Security Management*);

– *CIP*-008-1: "Звіти про інциденти і плани реагування" (*Incident Reporting and Response Planning*);

– *CIP*-009-1: "Плани відновлення критичних кібернетичних активів" (*Recovery Plans for Critical Cyber Assets*).

З урахуванням викладеного вище можливо охарактеризувати цифровий інформаційний (кібернетичний) простір як глобальну мережеву структуру, вузли комутації якої у свою чергу є мережевими структурами, при цьому кожен вузол може мати кілька шляхів, що зв'язують його з усіма іншими вузлами.

Кожен вузол, за наявності з'єднує шляху, може ініціювати звернення до іншого вузла структури для отримання дозволу на прийом даних – здійснення операції читання або передачі даних – операції запису.

Дозволи і заборони на проведення операцій (встановлення логічного зв'язку) складають частину стратегії забезпечення безпеки простору, оскільки нелегальна операція читання несе загрозу конфіденційності інформації, нелегальний запис становить загрозу цілісності інформації, нелегальні запити, навіть не будучи реалізованими, можуть частково або повністю заблокувати той чи інший шлях доступу до деякого вузлу.

Вплив одного вузлу мережі на інший може призводити до ураження його штатних функцій аж до повного контролю (наприклад, шляхом впровадження відповідних програм – вірусів).

Формально у математиці ця модель описується графом $G:=(V, E)$ з множиною вершин V (вузлів мережі) та дуг E (фізичних маршрутів доступу) [12]. Кожна вершина графа G при детальному аналізі у свою чергу може являти собою граф, який включає деяку множину вершин що з'єднані дугами.

При цьому деяку групу, об'єднаних дугами вершин $G_i:=(V_i, E_i)$, але не маючих зв'язку з іншими вершинами графа G, назвемо ізольованим кластером. У цьому випадку вихідний граф може бути поданий у вигляді логічного об'єднання декількох ізольованих один від одного кластерів: $G=G_1 \cup G_2 \cup .... \cup G_n$. У такому варіанті

побудови мережі процеси, що відбуваються у будь-якому ізольованому кластері, не може вплинути на інші ізольовані кластери.

Глобалізація інформаційних технологій призводить до зменшення кількості і розмірів ізольованих кластерів. А це відповідає ситуації, коли з більшості вузлів мережевої структури можна встановити логічний зв'язок практично з будь-яким її вузлом, якщо правила розмежування доступу не заблокують цей зв'язок і, відповідно, загрози породжувані таким з'єднанням.

Таким чином, можливо стверджувати що кіберпростір не існував поки вузли мережевої структури однозначно не ототожнилися з певними галузями забезпечення життєдіяльності людства таким чином, що порушення зв'язаності всієї мережевої структури могло призвести до порушення істотних умов реалізації такої діяльності. Крім того, постійно зростаюча зв'язаність мережевої структури одного разу створює передумови для реалізації загроз, які виходять з деякої її частини, іншим частинам.

Як наслідок, цілком очевидний висновок про необхідність якнайшвидшого вирішення питання про створення в нашої державі єдиного центру з питань мережевої безпеки з основними завданнями:

– реагування на інциденти в галузі безпеки та кризового управління процесами відновлення критичних інфраструктур;

– організації розслідування інцидентів в області безпеки критичних інфраструктур;

– організації інформаційно-технічної взаємодії з власниками критичних інфраструктур у державному та комерційному секторах, розробки методик виявлення атак і методичних рекомендацій щодо захисту, а також планів попередження/блокування атак на об'єкти критичної інформаційної структури економіки, транспорту, паливно-енергетичного комплексу та ін, включаючи використання повноважень правоохоронних органів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. "Red October" Diplomatic Cyber Attacks Investigation [Електронний ресурс]. – Режим доступу :http://www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation;

2. *Лукацкий А.* Почему атакуют объекты ТЭК? [Електронний ресурс]. – Режим доступу : http : // www.securitylab.ru/blog/personal/Business_without_danger/29330.php;

3. Высокотехнологичный терроризм : Материалы российско-американского семинара, Москва, 4–6 июня 2001 г. – Российская академия наук в сотрудничестве с Национальными академиями США. – 320 с.

4. *Смирнов А.И.* Информационная глобализация и Россия : вызовы и возможности / А.И. Смирнов. – М. : Изд. дом "Парад", 2005. – 392 с.

5. Доктрина информационной безопасности РФ // Научные и методологические проблемы информационной безопасности (сборник статей) ; под ред. В.П. Шерстюка. – М. : МЦНМО, 2004. – С. 149–197.

6. *Воронцова Л.В.* История и современность информационного противоборства / Л.В. Воронцова, Д.Б. Фролов. – М. : Горячая линия. – Телеком, 2006. –192 с. : ил.

7. *Гриняев С.Н.* Поле битвы – киберпространство : Теория, приемы, средства, методы и системы ведения информационной войны / С.Н. Гриняев. – Мн. : Харвест, 2004. 448 с.

8. *Бухарин С.Н.* Методы и технологии информационных войн / С.Н. Бухарин, В.В. Цыганов. – М. : Академический проект, 2007. 382 с.

9. *Васенин В.А.* Информационная безопасность и компьютерный терроризм / В.А. Васенин // Научные и методологические проблемы информационной безопасности (сборник статей) ; под ред. В.П. Шерстюка. – М. : МЦНМО, 2004. – С. 67–83.

10. О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации : Указ Президента РФ от 15 января 2013 г. № 31с [Електронний ресурс]. – Режим доступу : http : //text.document.kremlin.ru/SESSION/PILOT/main.htm.

11. *Смирнов А.И.* Национальная стратегия обеспечения безопасности киберпространства США (неофициальный перевод) // Информационная глобализация и Россия : вызовы и возможности. – М. : Изд. дом "Парад", 2005. – С. 363–370.

12. *Оре О.* Теория графов / О. Оре. – М. : Наука, 1968. – 336 с.

Отримано 11.04.2013