DOI: 10.34185/1991-7848.itmm.2020.01.046

КІБЕРБЕЗПЕКА-ПІДХОДИ ДО ВИЗНАЧЕННЯ ПОНЯТТЯ

Карабут Н.О.

Криворізький національний університет, старший викладач

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, КІБЕРБЕЗПЕКА, КІБЕРПРОСТІР, КІБЕРЗЛОЧИНИ.

За останній час спостерігається різке зростання інцидентів в області інформаційної безпеки, які мають широке поширення і набувають загрозливого характеру.

Головними тенденціями розвитку загроз є наступні:

- зростання числа атак, багато з яких ведуть до великих втрат;

- зростання складності атак, які можуть включати кілька етапів і застосовувати спеціальні методи захисту від можливих методів протидії;

- вплив практично на всі електронні (цифрові) пристрої, в числі яких останнім часом все більшої значущості набувають мобільні пристрої, а вони найбільшою мірою схильні до ризиків в області інформаційної безпеки.

Кібербезпека повинна бути націлена на забезпечення захисту в кіберпросторі. Тому основним для аналізу проблем кібербезпеки є поняття кіберпростір.

Поняття кібербезпеки дуже багатогранне і тому непросто і важко формалізується.

«Кіберпростір-сфера діяльності в інформаційному просторі, утворена сукупністю комунікаційних каналів Інтернету та інших телекомунікаційних мереж, технологічної інфраструктури, що забезпечує їх функціонування, і будь-яких форм здійснюваної за допомогою їх використання людської активності (особистості, організації, держави)».

Кіберпростір - це складне середовище, що не існує ні в якій фізичній формі, що виникає в результаті взаємодії людей, ПЗ, Інтернет сервісів за допомогою технологічних пристроїв і мережевих зв'язків.

При чіткій вказівці на пов'язаність кіберпростору з ІКТ інфраструктурою, основна увага звернена не на технології, а на діяльність людей, які використовують ці технології.

Основний зміст кіберпростору полягає в діяльності користувачів цифровими інформаційними ресурсами та ІКТ інфраструктурою.

Кіберпростір визначено на безлічі цифрових пристроїв і систем на їх основі, які оперують з інформацією або багато в чому з її допомогою. В загальному вигляді істотне зменшення числа функціонуючих пристроїв (систем) в кіберпросторі або порушення їх нормальної роботи є загрозою кіберпростору.

Активне оперування інформацією і збереження цією інформацією головних її властивостей: цілісності, доступності, конфіденційності та інших, що визначаються в сучасних стандартах. На відміну від інформаційної безпеки мова йде не про інформацію взагалі, а про ту інформацію, яка циркулює в кіберпросторі і становить важливу частину її змісту. Таким чином, порушення роботи окремого комп'ютера підключеного до кіберпростору або втрата інформації, яка в ньому міститься, або порушення її властивостей, безумовно важливих для користувача даного комп'ютера, навряд чи може розглядатися як загроза кібербезпеки.

Наявність "добропорядних" зв'язків, зв'язків, які складають основу кіберпростору, і без яких розглядати поле цифрових пристроїв (систем) в якості деякої нової сутності навряд чи мало б сенс. Тут мається на увазі здатність кіберпростору передавати, отримувати і обробляти інформацію зі збереженням її істотних для цілей застосування властивостей.

Поняття кібер -. Воно відноситься до управління. Управління в даному випадку має на увазі не наявність прямолінійних команд, які безпосередньо виконуються всіма агентами (учасниками) кіберпростору, а формування і передача таких сигналів, які здатні надати розглянутої області кіберпростору якийсь «розумний» характер поведінки і стійкість до виникаючих загроз.

Способи управління безпосередньо впливають на структуру кіберпростору. Тут важливо враховувати управління технічною основою кіберпростору і чисто фізичними зв'язками між окремими вузлами або навіть областями кіберпростору. Але визначальну роль відіграє управління учасниками кіберпростору: користувачами та їх групами. Під управлінням розуміється комплекс зусиль, спрямований на підвищення кваліфікації учасників, стимулювання сприятливих для розвитку кіберпростору дій і придушення або пряма заборона зловмисних дій. Управління суб'єктами

кіберпростору відіграє визначальну роль у виникненні, існуванні та підтримці основних властивостей цієї освіти.

Зазначені властивості, а саме численність елементів, що становлять кіберпростір, велика кількість взаємозв'язків між ними, можливість застосування спеціальних технік управління діями цих елементів, і визначають розвиток тих загроз, про які говорилося вище. Незвичайно висока і все наростаюча інтенсивність атак походить від величезних масштабів кіберпростору, всіляких і різнохарактерних зв'язків між ними. Складні атаки, що мають комплексну структуру, спираються на можливість різних напрямків поширення інформації і сигналів. Використання методів соціальної інженерії дозволяє вишукувати найбільш продуктивні методи організації атак. У кіберпросторі можуть розвиватися все більш небезпечні і складні загрози. Вони використовують особливості його побудови для досягнення максимального ефекту.

Кібербезпека має на меті забезпечення нормального функціонування кіберпростору, захищаючи його від виникаючих загроз ефективним чином.

Кібербезпека не може бути спрямована на захист від максимального числа загроз. Потрібно забезпечити максимально сприятливе середовище для роботи користувачів і всіх систем в кіберпросторі.

У визначенні кібербезпеки основний упор і цільова установка повинні бути зроблені на збереження сприятливого стану кіберпростору, а не на число загроз. Якщо ми змогли захиститися від неймовірно великого числа загроз, але працездатність кіберпростору порушена, то це гірше, ніж захиститися від двох десятків загроз і при цьому зберегти прийнятний рівень працездатності.

Кібербезпека так само, як і кіберпростір може описуватися тріадою складових її сутностей визначених на складових частинах кіберпростору: інформаційних ресурсах, комп'ютерній і мережевій архітектурах (інфраструктурі) і способах взаємодії користувачів.

Кібербезпека охоплює вже не тільки інформацію як об'єкт захисту, не виключно технічні засоби, які визначають можливості функціонування інформації, а захист способів функціонування нової сутності – кіберпростору. Захищається діяльність людей, яка здійснюється за допомогою інформації, поширюваної за допомогою технічної інфраструктури ІКТ.

При забезпеченні кібербезпеки важливо враховувати зазначені особливості кіберпростору та її найбільш важливий аспект – наявність взаємозв'язків між учасниками (користувачами), що призводить до можливості виникнення синергетичного ефекту.

Необхідно детально і ретельно дослідити основні властивості кіберпростору, динаміку його розвитку в різних масштабах часу від миттєвих до багаторічних, методи управління цією динамікою. Важливо обґрунтувати підходи до визначення показників кібербезпеки, розробити моделі для їх оцінки, виробити способи обґрунтування критеріїв.

Без проведення системного аналізу та отримання оцінок застосування тих чи інших заходів неможливо побудувати ефективну систему кібербезпеки.

Представляється доцільним в комплекс досліджень в області кібербезпеки включити наступні напрямки:

1. Вироблення єдиної термінології кіберпростору і кібербезпеки, гармонізованої з існуючою термінологією в області інформаційної безпеки.

2. Розробка комплексної системи показників, що охоплюють всі сторони функціонування кіберпростору та забезпечення його захисту від можливих загроз.

3. Розробка моделей самого кіберпростору і основних факторів, що впливають на його функціонування. Безумовно, необхідна ретельно продумана модель загроз. Одним з найважливіших напрямків є створення математичних моделей, що дозволяють отримувати чисельні характеристики інформаційної безпеки (ступеня загроз інформаційній безпеці, аналізу інформаційних ризиків, оцінки ефективності заходів захисту).

4. Створення спеціальних методів забезпечення стійкості кіберпростору або його областей при впливі загроз. Тут кілька можливих тем:

- аналіз топологічної структури і вироблення рекомендацій щодо її зміни, способів і конкретних алгоритмів їх реалізації;

- нові методи криптографічного захисту, засновані не тільки на чисто обчислювальних механізмах реалізації стійкості, а й на використанні переваг багатозв'язної архітектури зв'язків і великого числа добропорядних користувачів;

- методи інформаційної безпеки на основі соціальних сервісів для протидії кібератакам із застосуванням спеціальних процедур аналізу групової поведінки.

5. Інтелектуальні методи забезпечення кібербезпеки:

- методи інтелектуальної ідентифікації користувачів;

- інтелектуальні методи запобігання вірусних та інших атак;

- інтелектуальні методи виявлення атак і проникнень;

- методи ситуаційного аналізу стану інформаційної безпеки;

- нові методи криптографічного захисту, засновані на нейромережевих технологіях.

References

1. Trustwave 2013-Global-Security-Report
2. http://www.symantec.com/security_response/ publications/threatreport.jsp
3. http://mvd.ru/news/item/1033853
4. http://www.sophos.com/en-us/security-news-trends/ reports/security-threat-report/cyber-attacks.aspx
5. http://www.cybersecurity.ru/crypto/171331.html
6. http://www.politico.com/story/2013/02/washington-cybersecurity-china-attacks-87087.html
7. http://www.nytimes.com/2013/01/28/us/pentagon-to-beef-up-cybersecurity-force-to-counter-attacks.html
8. http://habrahabr.ru/company/kaspersky/blog/169839/
9. http://www.itsec.ru/newstext.php?news_id=91005
10. http://www.cybersecurity.ru/telecommunication/165487. html

CYBERSECURITY APPROACHES TO THE DEFINITION OF A CONCEPT

Karabut Nadiia

Abstract. A significant increase in incidents that occur in the information sphere has led to the need for a systematic analysis of the sources of threats. This requires agreed concepts among specialists, the key of which is cybersecurity. It is interpreted ambiguously by many experts. The article offers an approach to the concept of cyberspace and cybersecurity.

Key words: INFORMATION SECURITY, CYBERSECURITY, CYBERSPACE, CYBERCRIME.