

УДК 343.98

М. С. Ратушняк

ОСНОВНІ ВИМОГИ ДО СТРАТЕГІЇ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

Вінницький національний технічний університет

У статті викладено дослідження сучасного рівня кібербезпеки в Україні, наведено приклади важливості її забезпечення. Проведено аналіз національних стратегій кібербезпеки держав Європи, Америки, Африки, Азії. Висвітлено проблеми сучасного вітчизняного законодавства, що регулює діяльність у сфері кібербезпеки. Запропоновано практичні рекомендації щодо створення національної стратегії кібербезпеки України.

Ключові слова: національна стратегія, кібербезпека, кібератака, кіберзлочинність, інформаційна безпека.

BASIC REQUIREMENTS STRATEGY FOR ENSURING CYBER SECURITY UKRAINE

The article presents the current level of cybersecurity research in Ukraine, examples of the importance of security are discussed. National cybersecurity strategies of Europe, America, Africa and Asia countries are analysed. The problems of modern domestic legislation regulating activities in the field of cybersecurity are discussed. Practical recommendations for a national strategy for cybersecurity Ukraine are offered.

Key words: national strategy, cyber security, cyberattacks, cybercrime, information security.

Сьогодні спостерігається широке використання сучасних інформаційних та комунікаційних технологій (ІКТ) у державних і недержавних структурах та у суспільстві в цілому. З огляду на виникнення нових загроз та уразливостей, вирішення проблем інформаційної безпеки (ІБ) та кібербезпеки висуваються в число основних. Окрім прямої шкоди від можливих випадків несанкціонованого доступу до інформації, її модифікації або знищення, масова інформатизація може перетворитися на джерело серйозної загрози державній безпеці і правам людини. Тому, сформована в світі ситуація зобов'язує до побудови загальнодержавної моделі, спрямованої на забезпечення кібербезпеки держави.

У нашій державі, на відміну від більшості європейських держав, сьогодні відсутня стратегія забезпечення кібербезпеки – це породжує цілу низку проблем і загроз різного характеру. З огляду на це, метою цієї роботи є аналіз ключових положень національних стратегій кібербезпеки різних держав світу для формування основних вимог щодо розробки вітчизняної стратегії кібербезпеки.

Цього року Україна стала абсолютним лідером за кількістю внутрішніх і зовнішніх кіберзагроз в Європі. За останні роки наша держава неодноразово ставала жертвою не тільки для дрібних шахраїв, але і для широкомасштабних кібероперацій. Експерти Kaspersky Lab сформулювали перелік загроз, які роблять Україну однією з головних «гарячих точок» на кіберкарті світу [1]. Відповідно до цього, можна охарактеризувати ситуацію щодо кібербезпеки в державі таким чином:

1. Однією із причин зараження вірусами програмного забезпечення (ПЗ) українських користувачів є те, що вони використовують неоновлені версії або піратські копії ПЗ.
2. Поширення спамерами спекуляції на темі політичної ситуації в Україні або ж розсилка листів від імені дівчат з України та інших пострадянських держав, які скаржаться на свою нелегку долю і просять перевести кошти на їх рахунки.
3. Україна посідає перші місця у рейтингах світу за ризиками зіткнення з веб-загрозами в третьому кварталі 2015 року. За цей період майже третина українських користувачів мережі зіткнулися із загрозами, що поширюються через Інтернет.

4. Україна має найбільший ризик зараження шкідливими мобільними застосунками. Досить високий для українців і ризик зіткнення з локальними загрозами, до яких відносяться об'єкти, що проникли на комп'ютери шляхом зараження файлів, знімних носіїв або спочатку потрапили на комп'ютер не у відкритому вигляді (наприклад, ПЗ в складі складних інсталяторів, зашифровані файли і т.д.).

5. В Україні було зафіксовано велику кількість програм-вимагачів і шифрувальників – шкідливе ПЗ, мета яких – заблокувати пристрій або браузер чи зашифрувати файли користувача, зробивши їх недоступними без спеціального ключа, за який вимагається викуп.

6. Комп'ютери українських чиновників стали жертвами однієї з найскладніших кібершпійонських кампаній Turla. Це угруповання здійснило зараження сотні комп'ютерів більш ніж в 45 державах світу, які є власністю державних установ.

7. Також українці були серед жертв таких кампаній, як CosmicDuke, MiniDuke, Agent.btz, Epic Turla, TeamSpy, BlackEnergy і Red October.

Правовий фундамент кібербезпеки України становлять Конституція України, закони України «Про основи національної безпеки», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» та інші закони, Конвенція Ради Європи про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, Доктрина інформаційної безпеки України, а також інші нормативно-правові акти. Проаналізувавши чинне законодавство, можна стверджувати, що основною проблемою правового забезпечення системи кібербезпеки України є відсутність розробленого та нормативно закріпленого понятійного апарату у сфері кібербезпеки на найвищому рівні. Насамперед, це стратегія забезпечення кібербезпеки, яка стане вітчизняним документом, що врегульовує відносини у кіберсфері та відповідно до якого буде забезпечуватись кібербезпека.

Перші стратегії кібербезпеки з'явилися на початку минулого десятиріччя [2]. Однією з перших держав, що сприйняла кібербезпеку як питання державного рівня, була США, де 2003 року було опубліковано Національну стратегію безпеки в кіберпросторі. У наступні роки в Європі поширювались плани заходів та стратегії, покликані розв'язати подібну задачу. Через велику кібератаку 2007 року Естонія стала однією з перших держав-членів Євросоюзу, яка опублікувала 2008 року національну стратегію кібербезпеки, у якій особливу увагу зосереджено на безпеці ІКТ.

У зв'язку із тим, що вітчизняна стратегія кібербезпеки досі не затверджена, а лише прийнято проект за основу, варто детально розглянути і звернути увагу на ключові аспекти стратегій держав, які працюють у цьому напрямку не перший рік. Розглянемо деякі з них:

Стратегія кібербезпеки Німеччини (Cyber Security Strategy for Germany) 2011 року [3] створена з метою кримінального переслідування кібератак та запобігання їх виникнення, а також запобігання виходу з ладу ІТ-обладнання через випадкові чинники. Передбачено такі загрози: кібератаки та виведення з ладу критичних інформаційних ресурсів. До принципів забезпечення кібербезпеки віднесено узгодження набору інструментів для реагування на кібератаки; регулярна оцінка ситуації, ризиків та прийняття відповідних засобів захисту; регулярні тренування персоналу та тестування обладнання; зміцнення ІТ-безпеки в сфері держуправління. Наведено визначення таких понять як кіберпростір, кібератака, кібершпійонаж, кіберсаботаж, кібербезпека, цивільна та військова кібербезпека, критична інфраструктура (критичні ресурси). Міжнародна співпраця і партнерство, регулярна перевірка мети стратегії на рівень її досягнення та оновлення відповідно до стану поточної ситуації є пріоритетними.

Метою *Стратегії кібербезпеки Естонії* (Cyber Security Strategy) [4] 2014 року є опис методів забезпечення безперебійної експлуатації та стійкості важливих сервісів і захист критичних інформаційних інфраструктур від кіберзагроз на період до 2017 року. У документі наведено дефініцію поняття кібербезпека. Головним пріоритетом у забезпеченні кібербезпеки є прогноз як запобігання можливості виникнення загрози, так і ефективного реагування на загрози, які матеріалізуються. Визначено такі загрози: кібератаки, шпійонаж, кіберзлочини. Принципи забезпечення кібербезпеки: кібербезпека є невід'ємною частиною національної безпеки, підтримує функціонування держави і суспільства, конкурентоспроможність економіки та інновацій, забезпечується на основі принципу пропорційності, беручи до уваги існуючі та потенційні ризики і ресурси; гарантується дотриманням основних прав і свобод, а також захисту особистої інформації та особистості; починається з індивідуальної відповідальності за безпечне використання засобів ІКТ;

підтримується інтенсивністю і конкурентоспроможністю досліджень і розвитку на міжнародному рівні; забезпечується на узгодженій основі в рамках співпраці між державним, приватним та третім сектором, беручи до уваги взаємозв'язок і взаємозалежність існуючої інфраструктури і сервісів в кіберпросторі; забезпечується за допомогою міжнародного співробітництва з союзниками і партнерами. Завдяки співпраці, Естонія сприяє зміцненню глобальної кібербезпеки і підвищує рівень своєї компетенції.

Стратегія кібербезпеки Кенії (Cybersecurity Strategy) [5] була затверджена 2014 року. Метою є чітко визначення бачення кібербезпеки Кенії, цілі та завдання для забезпечення захисту кіберпростору держави, продовжуючи сприяння використанню для економічного зростання Кенії. Визначено такі загрози: ботнети, організована злочинність, DoS-атаки, кібертероризм, шкідливі коди та спеціально націлене шкідливе ПЗ. У стратегії наведено дефініції понять CERT, кіберпростір, кібербезпека, електронне урядування, критична інфраструктура, уряд, ІКТ, інсайдерська загроза, соціальний інжиніринг тощо. Пріоритетними напрямками визначено електронне урядування, підвищення кібербезпеки Кенії, оновлення стратегії, її цілей і завдань.

Концепція кібербезпеки Сінгапуру (*National Cyber Security Masterplan 2018*) [6] затверджено 2013 року. Вона спрямована на створення безпечного і стійкого середовища інфокомунікацій та динамічної екосистеми кібербезпеки. Документом передбачено такі загрози: АРТ-загрози, фішинг, соціальний інжиніринг, DDoS-атаки, шкідливе ПЗ. Дефініцій понять у концепції не наведено. Пріоритетом є підвищення рівня готовності та реагування на значні кібератаки на національному рівні, оцінка безпеки ІКТ, які мають вирішальне значення для функціонування критичних інфраструктур, збільшення людських та інтелектуальних ресурсів тощо.

Концепція кібербезпеки Канади (*Action Plan 2010-2015 for Canada's Cyber Security Strategy*) [7] 2013 року призначена для спрямування зусиль уряду для створення безпечного кіберпростору для канадців. У документі визначено такі принципи забезпечення кібербезпеки: захист державних систем; співпраця з метою захисту ключових систем від кібератак, що знаходяться за межами федерального уряду; забезпечення безпеки канадців в онлайн-мережі. У якості загроз визначено різного роду кіберзлочини та кібератаки. Дефініцій понять не наведено. Пріоритетними визначено наступні дії: безпечне зберігання особистої інформації канадців онлайн, а також ІКТ, інфраструктури уряду; боротьба з кіберзлочинністю; посилення безпеки кіберсистем федерального рівня та підвищення інформованості суспільства в галузі кібербезпеки.

Отже, проаналізувавши стратегії та з огляду на постійне збільшення ризику виникнення нових кіберзагроз та їх еволюції, збільшення впливу на особу, суспільство, кожній державі необхідно мати продуману та чітко сформульовану, комплексну стратегію кібербезпеки. Оскільки загрози такого типу не мають кордонів, потрібно постійно підтримувати тісне міжнародне співробітництво, що є необхідним не лише для підготовки до кібератак, а й для своєчасного реагування на них. Провівши аналіз ключових положень національних стратегій кібербезпеки держав світу та врахувавши сучасний стан цієї галузі в Україні, при розробці вітчизняної стратегії кібербезпеки необхідно:

- розробити єдиний понятійний апарат, у якому чітко визначити терміни й поняття, пов'язані із забезпеченням кібербезпеки держави (вони мають бути узгодженими з міжнародними стандартами і враховувати національні особливості);

- визначити основні загрози та критичні інфраструктури держави, забезпечення кібербезпеки яких є найбільшим пріоритетними (розробити механізми ідентифікації та пріоритезації найбільш важливих об'єктів інформаційної інфраструктури);

- визначити основні принципи забезпечення кібербезпеки держави та усіх її стейкхолдерів (врахувати усі їх інтереси в різних сферах, а також питання взаємовпливу та співпраці);

- створити систему державних органів, на які покладаються завдання щодо забезпечення кібербезпеки, чітко визначити їх обов'язки та межі відповідальності;

- приділити увагу багаторівневій системі підготовки фахівців у сфері кібербезпеки (передбачити різні освітні напрямки для фахівців, орієнтованих на різні галузі народного господарства);

- врахувати зміни у суміжних нормативно-правових актах шляхом внесення поправок чи прийняття нових їх редакцій (зокрема це стосується тих документів, які на сьогодні становлять правовий фундамент забезпечення кібербезпеки нашої держави);

- передбачити усі види відповідальності за різного роду правопорушення та злочинів у

кіберпросторі;

– визначити часові рамки реалізації стратегії, відповідальні за кожен напрямок підрозділи, передбачити можливість адаптації стратегії відповідно до міжнародних норм та актуальних викликів у кіберпросторі, а також проведення зовнішнього аудиту виконання передбачених у стратегії заходів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. 8 тезисов про кибербезопасность в Украине. [Електронний ресурс]. – Режим доступу: <http://ain.ua/2015/11/25/617473>
 2. Гнатюк С. О. Кібертероризм : історія розвитку, сучасні тенденції та контрзаходи / С. О. Гнатюк. – Безпека інформації. – Том 19. – № 2. – 2013. – С. 118 – 129.
 3. Cyber Security Strategy for Germany [Електронний ресурс]. / Federal Ministry of the Interior. – Berlin, 2011. – Режим доступу: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?blob=publicationFile
 4. Cyber Security Strategy of Estonia [Електронний ресурс]. / Ministry of Economic Affairs and Communication. – 2014. – Режим доступу: https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf
 5. Cybersecurity Strategy [Електронний ресурс]. / Ministry of Information Communications and Technology. – Nairobi, 2014. – Режим доступу: <http://www.icta.go.ke/wp-content/uploads/2014/03/GOK-national-cybersecurity-strategy.pdf>
 6. National Cyber Security Masterplan 2018. [Електронний ресурс]. / Infocomm Development Authority of Singapore. – 2013. – Режим доступу: <https://www.ida.gov.sg/~media/Files/Programmes%20and%20Partnership/Initiatives/2014/ncsm2018/NationalCyberSecurityMasterplan%202018.pdf>
 7. Action Plan 2010-2015 for Canada's Cyber Security Strategy, 2013 [Electronic resource]. – Access mode: <http://www.securitepublique.gc.ca/cnt/rsrscs/pblctns/ctn-pln-cbr-scrt/ctn-pln-cbr-scrt-eng.pdf>
- Ратушняк Марія Сергіївна**, студентка групи УБ-16м, факультет менеджменту та інформаційної безпеки, кафедра менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: ratushnyak95@outlook.com
Науковий керівник: **Томчук Микола Антонович**, к.т.н, доцент кафедри БЖДПБ, Вінницький національний технічний університет, Вінниця, e-mail: tomchuk68@mail.ru

Maria S. Ratushnyak, student of group UB-16m, Department of Management and Information Systems Security, Vinnytsia National Technical University, Vinnytsia, email : ratushnyak95@outlook.com;
Supervisor: **Nicholas A. Tomchuk**, PhD, department of HSS, Vinnytsia National Technical University, Vinnytsia, e-mail : tomchuk68@mail.ru

УДК 624.316

А. М. Ратушна

ВИКОРИСТАННЯ ІННОВАЦІЙНИХ ТЕХНОЛОГІЙ В ДОСЛІДЖЕННІ ЕЛЕКТРОПРИВОДУ ГІБРИДНОГО МІСЬКОГО АВТОМОБІЛЯ

Вінницький національний технічний університет

Розроблено паралельна схема підключення, оскільки вона характеризується простотою (можливе застосування разом з механічною коробкою передач) і низькою вартістю. При такій схемі підключення двигун внутрішнього згоряння, і електродвигун механічно з'єднані з колесами допомогою диференціала, який забезпечує можливість як їх роботи окремо, так і спільно.

Ключові слова: паралельна схема підключення, механічною коробкою передач, двигун внутрішнього згоряння, електродвигун.