УДК 342.9

Валерій Васильович Сокуренко,
доктор юридичних наук, професор, заслужений юрист України,
начальник ГУНП в Харківській області

Комплексний підхід до вирішення питання кібербезпеки України

Питання про те, чи існує взагалі якась система кібербезпеки в Україні, є базовим для вирішення завдань кібербезпеки в державі в цілому. За всі роки незалежності до цього питання, що є критично важливим, не було системного підходу. Створювалися нормативна база та система захисту, але ключових документів, на основі яких можна було б вибудовувати систему кібербезпеки, не існувало. Навіть у Законі України «Про основи національної безпеки України», який діяв з 2003 по 2018 роки, були лише окреслені загрози в інформаційній сфері. У січні 2016 року РНБО нарешті ухвалила Стратегію кібербезпеки України. Це дало поштовх для вирішення інших завдань, оскільки Стратегія визначила ланцюг напрямів, за якими потрібно далі вибудовувати національну систему кібербезпеки.

Що ж являє собою національна система кібербезпеки? Перш за все, це суб'єкти, визначені Стратегією, зокрема Міністерство оборони, Державна служба спеціального зв'язку та захисту інформації, Служба безпеки, Міністерство внутрішніх справ, Національна поліція України, тобто органи, які забезпечують кібербезпеку в державі. Координатором цієї системи, згідно зі Стратегією, є РНБО. Для функціонування в постійному режимі було створено Національний координаційний центр кібербезпеки, який очолює секретар РНБО. У Центрі постійно проводяться засідання й ухвалюються рішення, які стають основою для рішень РНБО та діяльності всіх органів влади.

У держави є інформаційні ресурси та критична інфраструктура. Для державних інформаційних ресурсів легше вибудовувати систему кібербезпеки на основі чинної законодавчої бази, однак багато об'єктів критичної інфраструктури перебувають у приватній власності, тому захистити обчислювальні ресурси таких об'єктів є великою проблемою. З метою її вирішення сьогодні створюється перелік таких об'єктів для їх подальшого обліку та забезпечення на них кібербезпеки.

Побудову ефективно функціонуючої системи кіберзахисту бажано розділити принаймні на кілька частин. Є державні інформаційні ресурси, якими займаються окремі спеціальні державні організації, – це перший полюс. Другим є приватні системи окремих осіб, дані яких є об'єктом атак окремих зловмисників. Цілеспрямованих атак на такі об'єкти ніхто здійснювати не буде. Посередині залишився ще великий пласт комерційних підприємств із різною формою власності.

Позитивним є той факт, що РНБО почала приділяти серйозну увагу безпеці об'єктів критичної інфраструктури, тобто проблема почала вирішуватися. Водночас сегмент комерційних підприємств становить основу економіки України, але до сьогодні проблемою забезпечення їх кібербезпеки ніхто в державі не займався. Тому вбачається доцільним створити певне співтовариство представників приватного сектора, яке займатиметься створенням штабів, підготовкою відповідного персоналу компаній, виявленням загроз тощо. За ініціативи бізнесу повинні бути створені центри обміну інформацією, які співпрацюватимуть один з одним та з усіма державними органами щодо створення метрики загроз, методології захисту інформації аж до інструкцій з алгоритмом дій у разі виявлення кіберінциденту. Для тих компаній, які не мають ІТ-відділів або відповідних фахівців, потрібно створити «гарячий резерв», фахівці якого могли б бути тимчасово найняті для відновлення ІТ-систем.

Для забезпечення ефективного кіберзахисту необхідно провести аналіз характеристик сучасної кіберзброї, яку можна порівняти із засобами масового ураження, однак стосовно комп'ютерів та інформаційних систем. Кіберзброя може одночасно вивести з ладу велику кількість об'єктів критичної інфраструктури як на рівні однієї держави, так і на рівні об'єднання кількох держав. Кіберпростір – це середовище взаємодії різноманітних нестандартизованих уразливих інформаційних систем, в яких використовуються чутливі до злому дані та комунікаційні можливості. Кіберзброя націлюється як на окремі сегменти економіки та локальні компанії, так і на окремих громадян. Кібератаки дуже ретельно готуються. У 2011 році дослідники кіберзагроз, вихідці зі спецслужб США, розробили методологію «kill chain», яка спочатку використовувалася у військовій концепції, що стосується структури атаки. Вона містить низку послідовних дій або ланцюжок фаз, а порушення будь-якої з них може перервати весь процес. Більшість кібератак включають декілька цих фаз. Сучасні атаки готуються таким чином, щоб вони не могли бути

виявлені й ідентифіковані, а їх дія була максимально тривалою для досягнення поставлених цілей.

Уразливим місцем при подібних кібератаках є відсутність окремих департаментів кібербезпеки. Зазвичай цим опікуються ІТ-відділи, але в них, як правило, немає кризових регламентів, вони не знають, як діяти в таких ситуаціях. А там, де є навички швидкого реагування, часто немає повноважень.

Що потрібно? Перше, це система CERT. При цьому необхідні спеціалізовані CERT. Наприклад, у США є загальний CERT, який займається загальними питаннями кібербезпеки, є ICS (Industrial Control System) CERT, який займається об'єктами критичної інфраструктури, і є NERC – некомерційна організація, що займається питаннями безпеки в енергетиці. Необхідно налагодити обмін інформацією. Компанії зациклені здебільшого на відбитті атак і ліквідації їх наслідків. В Європі та США є організації, які випускають документи щодо запобігання атак, які містять готові «рецепти».

У світі функціонує приблизно 300 таких центрів. В Україні також є команда CERT-UA, яка працює під егідою Держспецзв'язку. Після атаки на фінансовий сектор у січні 2016 року було поставлено завдання щодо формування і затвердження протоколу спільних дій під час кіберінцидентів. Йдеться про вдосконалення нормативної бази, наділення повноваженнями суб'єктів забезпечення кібербезпеки, щоб вони могли швидко реагувати і взаємодіяти для протидії атакам.

Важливу роль у забезпеченні кібербезпеки України відіграють підрозділи МВС, які керуються у своїй діяльності положеннями Концепції Програми інформатизації системи Міністерства внутрішніх справ України на 2018–2020 роки. Основними завданнями, що стоять перед органами Національної поліції України, є захист інформації, що обробляється в інформаційно-телекомунікаційних системах, та контрольована на всіх етапах обробка службової інформації в ЄІС МВС.

Отже, для вирішення зазначених проблем в Україні буде впроваджено дієву систему захисту інформації на всіх етапах функціонування ІТ-інфраструктури, контрольовану технологію обробки службової інформації, захист інформаційних ресурсів під час інтеграції з автоматизованими системами інших державних органів та установ, що дозволить істотно покращити кіберзахист інформаційного простору держави.

Одержано 06.11.2019