УДК 005.57:005.922.1

Обнявко Олександр Валентинович
к. е. н., доцент кафедри маркетингу та міжнародної логістики,
Одеський національний економічний університет (Україна)
Онищенко Олег Анатолійович
д. т. н., професор кафедри технічної експлуатації флоту,
Національний університет «Одеська морська академія» (Україна)
Нікуліна Олена Валеріївна
к. е. н., доцент кафедри менеджменту ім. професора Й. С. Завадського,
Національний університет біоресурсів та природокористування України (Україна)

ШЛЯХИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ ЯК СКЛАДОВОЇ БЕЗПЕКИ ЕКОНОМІЧНИХ СИСТЕМ В УМОВАХ ВОЄННОГО СТАНУ

JEL classification: *L150*

Інформаційна безпека в XXI столітті виходить на перше місце в системі національної безпеки держави, тому лише та держава може розраховувати на лідерство в економічній, військово-політичній та інших сферах, мати стратегічну і тактичну перевагу, гнучкіше регулювати економічні витрати на розвиток озброєнь і військової техніки, підтримувати перевагу за низкою передових технологій, яка має перевагу в засобах інформації та інформаційної боротьби [1]. Особливого значення та актуальності в спектрі суспільних відносин набувають проблеми забезпечення інформаційної безпеки в умовах масштабного вторгнення збройних сил Росії 24 лютого 2022 року і запровадження у зв'язку з цим в Україні воєнного стану. Під час дії воєнного часу вимоги щодо захисту інформації діють як і в умовах мирного часу та визначені Законом України «Про захист інформації в інформаційно-комунікаційних системах».

Інформаційною безпекою (у контексті безпосередньої діяльності із захисту інформації) може вважатися комплекс заходів, що спрямовані на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи знищення даних [2, с. 9]. В Стратегії інформаційної безпеки зазначено, що інформаційна безпека України – складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом [3].

Інформаційну безпеку за сферою застосування можна розглядати у контексті безпеки держави, організації та особистості [2, с. 9]. Інформаційна безпека держави – це стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди. Шкода може бути заподіяна через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [2, с. 9].

Інформаційна безпека організації (підприємства) – це цілеспрямована діяльність її органів та посадових осіб з використанням дозволених сил і засобів з досягнення стану захищеності інформаційного середовища організації [2, с. 9].

Інформаційна безпека особистості характеризується як стан її безпосередньої захищеності від негативних інформаційних впливів, а також впливів на її власну здатність шукати, збирати, обробляти та використовувати інформацію [2, с. 10].

Росія здійснює гібридну війну і разом з обстрілами ракетами, снарядами, беспілотниками постійно проводить кібернетичні операції проти як економічних систем (об'єктів критичної інфраструктури, підприємств і організацій, бізнесових структур ФОП), так і проти інформаційно-телекомунікаційних систем Збройних Сил України. Щодня Росія здійснює в середньому понад 10 кібератак [4]. В Україні кібератакам потидіє Державна служба спеціального звязку та захисту інформації (Держспецзв'язок) України, Урядова команда реагування на комп'ютерні надзвичайні події CERT-UA, яка діє при Держспецзв'язку, Ситуаційний центр забезпечення кібербезпеки Служби безпеки України та інші органи, які відповідають за кібербезпеку в державі. Діє національна платформа Malware Information Sharing Platform «Ukrainian Advantage» (MISP-UA) для ефективної протидії кіберзагрозам і обміну даними – це платформа, яка в режимі реального часу забезпечує обмін даними про кіберризики, атаки та інциденти на об'єктах критичної інфраструктури, установах і підприємствах, державних електронних інформаційних ресурсах.

У межах реалізації Стратегії кібербезпеки України, на виконання постанови Уряду затверджено Порядок реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, який передбачає розробку відповідних Методичних рекомендацій [5].

Базуючись на пропозиціях науковців [6, с. 47], вважаємо, що при розробці цих Методичних рекомендацій можна використати такі напрямки посилення безпеки інформації економічних, технічних та інших систем, які в умовах воєнного стану стають ще більш актуальними: 1) ізоляція обладнання, що зазнало зараження, та негайне інформування органів влади, відповідних служб і керівництва підприємства про інцидент. Це передбачає: забезпечення безперешкодного доступу посадовим особам і компетентним органам для якнайшвидшого відновлення системи; залучення допомоги досвідчених IT-консультантів; використання резервної бази даних за межами внутрішньої платформи; документування інциденту: фіксацію часу його настання для виявлення заражених систем і витоку даних; залучення криміналістів; опитування осіб, що мають відношення до кіберінціденту; 2) визначення рівня захисту критично важливих систем. Це передбачає пріоритетні дії: виявлення кіберзагрози чи кіберінциденту, мінімізацію ймовірності їх виникнення, відновлення системи, що дозволить виявити взаємозалежність між критичними системами та контролювати відкриті порти доступу; регулярне оновлення даних системи з впровадженням нових продуктів кібербезпеки; обов'язкову сертифікацію пристроїв і обладнання, яке використовується, та оперативний огляд (review) програмного коду контролюючою службою; 3) створення можливостей ідентифікації інциденту, кіберзагрози, уразливості. Це передбачає формування умов для опису загрози, інциденту, включаючи автоматичний збір і агрегацію даних з набору джерел моніторингу, що дозволить швидко виявити перехресні зв'язки системи і аналізувати інформацію, ідентифікувати та ранжувати ризики і зробити візуалізацію потенційних втрат у результаті кібератак; 4) раннє виявлення кібератаки для утруднення злому і запобігання збою критично важливих систем управління підприємством. Це дозволить здійснити захист економічних систем за допомогою: визначення областей уразливості; ранжирування ризиків; ідентифікації та автентифікації всіх користувачів; візуалізації потенційних втрат від можливих кібератак; 5) аналіз ступеню небезпеки. Це передбачає: кількісну оцінку інцидентів та загроз; створення реєстру кіберінцидентів і вразливостей; визначення областей уразливості економічних систем; вимір обсягу системних збоїв і виявлення зловживання політикою використання; визначення неправильної конфігурації або підозрілої поведінки системи.

Література

1. Шульга В. І. Сучасні підходи до трактування поняття інформаційна безпека. *Ефективна економіка*. 2015. № 4. URL: http://www.economy.nayka.com.ua/?op=1&z=5514 (дата звернення: 28.03.2023).

2. *Електронне урядування та електронна демократія* : навч. посіб. : у 15 ч. / за заг. ред. А. І. Семенченка, В. М. Дрешпака. Ч. 13 : Захист інформації в системах електронного урядування / О. М. Хошаба. Київ : ФОП Москаленко О. М., 2017. 72 с.

3. *Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»* : Указ Президента України № 685/2021 від 28.12.2021 р. URL: https://www.president.gov.ua/documents/6852021-41069 (дата звернення: 28.03.2023).

4. *Глава СБУ* : *Щодня ворог здійснює понад 10 кібератак на держресурси та об'єкти критичної інфраструктури України* / Інформаційне агентство «Interfax-Україна» : сайт. URL: https://interfax.com.ua/news/general/894438.html (дата звернення: 28.03.2023).

5. *Уряд затвердив Порядок реагування на кіберінциденти та кібератаки* / Державна служба спеціального зв'язку та захисту інформації України : сайт. URL: https://cip.gov.ua/ua/news/uryad-zatverdiv-poryadok-reaguvannya-na-kiberincidenti-ta-kiberataki (дата звернення: 28.03.2023).