СУСЬКИЙ ГЕОРГІЙ ВАЛЕРІЙОВИЧ

аспірант Інституту програмних систем НАН України
Науковий керівник: Сініцин І.П., доктор технічних наук

Питання кібербезпеки та «інформаційного імунітету» країни в період гібридної війни

Після початку повномасштабного вторгнення російських військ на територію України 24 лютого 2022 року відбулись суттєві зміни та ужорсточення систем кібербезпеки, які забезпечують недоторканість мережевих та міжмережевих комунікацій в умовах гібридизації цифрових загроз, зокрема, й з боку країни-агресорки. Результатом осмислення процесів, які відбуваються у сфері інформаційних технологій, у зв'язку з реформуванням світової економіки, із взяттям курсу на інноваційний розвиток – стало підвищення уваги до засобів і систем кібернетичного захисту.

Розвиток інформаційно-обчислювальної техніки спричинив активне поширення глобалізаційних процесів на продукування та транспортування інформації. Все більше підприємств та організацій використовують в повсякденній роботі різні засоби і системи кіберзахисту. Так само приділяється значна увага питанням кіберзахисту системи інформування та обміну даними в сфері комунікацій державних органів. Отже, сьогодні можна казати про наявність необхідності створення загальної системи кіберзахисту та «інформаційного імунітету» країни.

Структура системи кіберзахисту держави базується на підходах, визначених Концепцією

цифрової стійкості держави, яка узгоджена із засадами Концепції забезпечення національної стійкості (Указ Президента України від 27.09.2021 № 479 [2]) в усіх тих аспектах, що належать до цифрової сфери. Задля сталого надання необхідних цифрових спроможностей, у цій Концепції визначено мету, основні принципи та механізми, а також строки впровадження та функціонування національної системи цифрової стійкості (як складника національної системи інформаційної стійкості у період гібридної війни й в подальшому майбутньому).

В разі свого активного запровадження, національна система цифрової стійкості може забезпечувати здатність України як держави і українського суспільства взагалі своєчасно ідентифікувати загрози, виявляти «плями вразливості» та оцінювати ризики національній безпеці у цифровій сфері. Особливо актуальним і конче потрібним в період гібридної війни є

запобігання або мінімізація ворожих негативних впливів, ефективне реагування на кібератаки з боку ворога та можливість забезпечити швидке та повномасштабне відновлення після виникнення загроз, здійснення кібератак або настання надзвичайних та кризових ситуацій різного типу, зокрема, включно із загрозами гібридного типу в інформаційній сфері.

Структури, пов'язані із втіленням Стратегії інформаційної безпеки (Указ Президента України від 28 грудня 2021 року № 685 [3]), передбачають також узгодження своїх дій, а також використання процедур і напрямів дій, передбачених у Стратегії здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2025 р. (Розпорядження КМ України від 17 листопада 2021 р. № 1467-р.[4]). Для забезпечення «інформаційного імунітету» комунікацій всередині українського суспільства і на міжнародному рівні передбачено узгодження дій відповідно до існуючої Стратегії цифрової трансформації соціальної сфери (розпорядження КМ України від 28 жовтня 2020 р. № 1353-р. [5]) і Проекту національної стратегії Індустрії 4.0 [1].

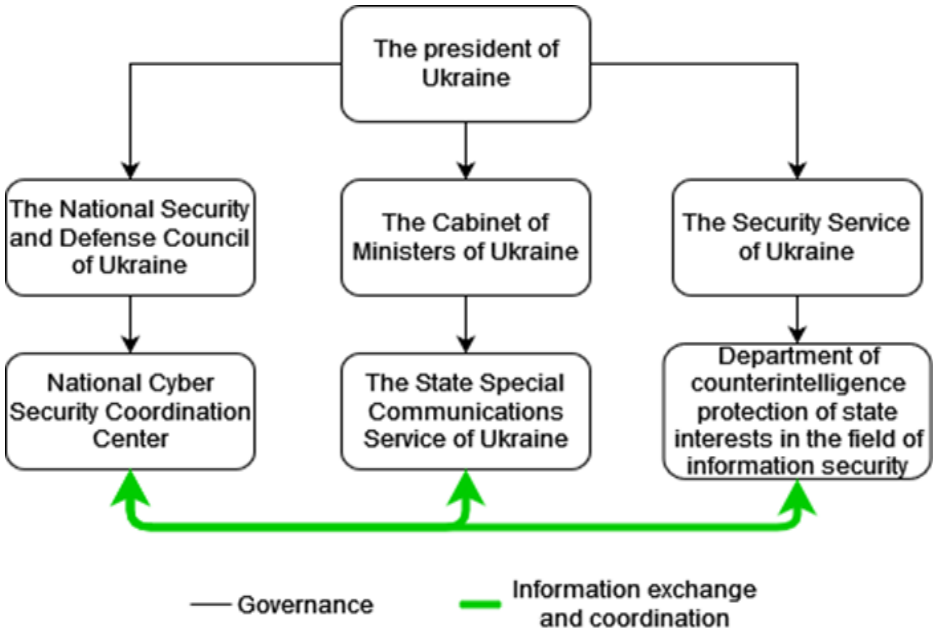

Рис. 1. ***Система організації взаємодії структур, що включені у забезпечення кібербезпеки України***

Вільна та захищена комунікація в мережах та інформаційному просторі в цілому є сьогодні завданням, над яким працюють і спеціалісти IT-сфери, і комунікаційники та піарники як державних органів, так і великої кількості підприємств та організацій. Концепція цифрової стійкості держави віддзеркалює напрями й засади формування єдиної державної

інфраструктури забезпечення цифрової стійкості та кібербезпеки. Необхідне реальне та дієве забезпечення цих процесів втілюється на таких рівнях:

- у середовищі організаційних структур (із забезпеченням добре координованої та конструктивної співпраці профільних підрозділів ІТ-сфери, органів сектору оборони й самоврядування, наявних вітчизняних виробників програмно-апаратного забезпечення, наукових установ, вищих навчальних закладів (за профілем), авторитетних фахових спільнот, ін.;
- у нормативно-методичному «полі» (з необхідним розвитком законодавства та відомчих регламентів цифрової сфери);
- у «полі» інформаційних ресурсів (центри обробки даних тощо) і засобів протидії загрозам (апаратних, програмних, програмно-апаратних).

Висновки: отже, формування нової якості національної системи кібербезпеки потребує чіткого та зрозумілого визначення стратегічних цілей, що мають бути досягнуті протягом визначеного періоду реалізації, що є особливо важливим під час періоду гібридної війни, що була розв'язана з російського боку проти України у лютому 2022 року.

Список джерел:

1. Національна стратегії індустрії 4.0. Проект для Кабінету Міністрів України.
2. Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року "Про запровадження національної системи стійкості". Указ Президента України від 27 вересня 2021 року № 479/2021.
3. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки". Указ Президента України №685/2021.
4. Про схвалення Стратегії здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2025 року та затвердження плану заходів щодо її реалізації. Розпорядження КМ УКРАЇНИ від 17 листопада 2021 р. № 1467-р.
5. Про схвалення Стратегії цифрової трансформації соціальної сфери. Розпорядження КМ України від 28 жовтня 2020 р. № 1353-р.