Заява за підсумками проведеного IFES Тижня кібербезпеки та оцінювання кібербезпеки

Київ, Україна

27 червня 2018 р.

Російська окупація Криму та конфлікт у Східній Україні мають чіткі характеристики гібридної війни - поєднання звичайної, інформаційної війни (у формі кампанії дезінформації) та кібервійни. З наближенням України до президентських та парламентських виборів 2019 року перспективи кібератак, потенційно здатних заподіяти серйозну шкоду критично важливим системам, є реальною небезпекою, яка існує вже зараз і може мати серйозні наслідки не лише для України. Важливість забезпечення кібербезпеки виборчого процесу в Україні неможливо переоцінити.

4-8 червня 2018 року Міжнародна фундація виборчих систем (IFES) за підтримки Агентства США з міжнародного розвитку (USAID) та британської допомоги (UK aid) від уряду Великої Британії забезпечувала роботу команди міжнародних та національних експертів, метою якої було проведення оцінювання рівня кібербезпеки українського виборчого процесу та відповідної інфраструктури.

Команда зустрілася із різними зацікавленими сторонами, у тому числі представниками Центральної виборчої комісії (ЦВК), органів безпеки, залучених до протидії кіберзагрозам, та організацій громадянського суспільства. 7 червня 2018 року IFES організувала круглий стіл на тему “Кіберзагрози для виборчого процесу в Україні” за участі провідних експертів та вищих посадових осіб державних органів, уряду, виборчої адміністрації, громадянського суспільства та приватного сектору, щоб підвести підсумки поточної ситуації.

Основні результати Тижня кібербезпеки IFES зводяться до наступного:

1. Протягом останніх років в Україні мала місце серія руйнівних кібератак на високому рівні, в тому числі в енергосистемах, аеропортах та фінансових системах. Усього за три дні до президентських виборів 2014 року ЦВК стала об’єктом комплексної та складної кібератаки. Ініціатори атаки вимкнули вузли мережі ЦВК та знищили численні компоненти інформаційної системи, використавши при цьому складні шкідливі програми. Це є переконливим свідченням потенційної величину збитку, який може бути завданий виборчому процесу добре підготовленою атакою. Представники українських зацікавлених сторін усвідомлюють ці загрози, налаштовані рішуче протидіяти їм, але потребують для цього додаткових ресурсів;
2. Протягом останніх років в ІТ системи ЦВК було впроваджено деякі суттєві покращення, у тому числі ізоляцію критичних мереж, обмеження віддаленого доступу, запровадження моніторингу мережевого потоку даних та створення системи запобігання несанкціонованим втручанням. Було також створено новий центр відновлення даних після аварійного відключення;
3. Україна підписала Будапештську Конвенцію Ради Європи про боротьбу з кіберзлочинністю 2006 року та прийняла новий Закон “Про основні засади забезпечення кібербезпеки України”, який набув чинності в травні 2018 року. Закон ґрунтується на високорівневому аналізі кібербезпеки та кіберзахисту і запроваджує нові правила захисту

інституцій та об'єктів, віднесених до критичної інфраструктури (КІ). IFES вважає, що ЦВК має бути частиною цієї системи. Однак при цьому мають закріплюватись положення, які забезпечуватимуть належний захист незалежності цього органу. До початку серпня Кабінет Міністрів має прийняти низку підзаконних актів, що мають встановити рівень захисту державою об'єктів та інституцій КІ, у тому числі через мережевий моніторинг та ведення журналів доступу, стійкість до DdoS атак, аудит систем, включаючи використання тестів на вторгнення (випробування на проникнення) та сертифікацію. Органом, відповідальним за реалізацію цих заходів, має стати Державна служба спеціального зв'язку та захисту інформації (ДССЗЗІ);

4. Офіційний старт виборчого процесу з виборів Президента України у березні 2019 року припадає на грудень 2018 року. Строк до початку виборчого процесу невпинно скорочується, і ЦВК та інші державні інституції мають дуже обмежений час для реалізації будь-яких нових ініціатив, у тому числі ініціатив у сфері кібербезпеки;
5. Строк повноважень 13 з 15 членів ЦВК вже давно закінчився. Цей факт негативно впливає на ефективність здійснення ЦВК своїх повноважень та рівень спроможності цього органу у пошуку варіантів вирішення проблем та прийнятті рішень щодо будь-яких майбутніх проектів;
6. ЦВК надіслала запит про виділення 36 мільйонів гривень з державного бюджету на 2018 рік, але не отримала відповідні кошти у зв'язку з тим, що вибори проводитимуться у 2019 році. Таким чином, у ЦВК відсутні достатні фінансові ресурси для вдосконалення своєї інфраструктури кібербезпеки. Водночас, на сьогодні міжурядові інституції та проекти технічної допомоги, з якими ЦВК співпрацює у напрямі удосконалення систем кібербезпеки, надають значний обсяг підтримки забезпеченню кібербезпеки.

За результатами Тижня кібербезпеки та оцінювання кібербезпеки IFES разом з ключовими партнерами працює над підготовкою відповідного комплексного звіту. У цьому звіті буде відображено низку рекомендацій, у тому числі наступні:

1. **Існує потреба у посиленні спроможності IT-персоналу ЦВК** за рахунок виділення додаткових ресурсів **та проведення цільового навчання;**
2. **Слід підвищити рівень обізнаності** працівників ЦВК з питань кібербезпеки, в той час як для учасників виборчого процесу має бути проведений **тренінг з питань кібербезпеки та поводження з даними;**
3. Задовго до майбутніх виборів ЦВК має розробити чітку **комунікаційну стратегію щодо кібербезпеки та виборів, що забезпечить** підтримання довіри громадян до виборчого процесу;
4. Для підвищення операційної стійкості ЦВК **слід посилити та оптимізувати координацію взаємодії** з органами безпеки та іншими зацікавленими сторонами;
5. У взаємодії з органами безпеки, які будуть залучені до виборчого процесу, ЦВК варто напрацювати **комплексну стратегію забезпечення кібербезпеки**, яка визначатиме механізми реагування на наявні кризові ситуації в питаннях кібербезпеки. Рівень готовності до реагування має бути підвищений шляхом моделювання кризових ситуацій, яке має бути проведене за участі основних зацікавлених сторін і задовго до проведення виборів;
6. ЦВК потребує нового обладнання для **заміни застарілих апаратних компонентів** у всіх своїх системах. Ці "слабкі ланки " можуть бути використані для отримання несанкціонованого доступу до систем ЦВК. Закупівля необхідних нових компонентів має бути проведена

завчасно – у строки, які дозволять провести їх конфігурацію та тестування, в той час як відповідні працівники повинні завчасно пройти необхідну підготовку, яка б мінімізувала ризики внесення ними нових та недосліджених вразливих елементів в нове обладнання при проведенні його налаштування та експлуатації;

7. Слід розглянути можливість запровадження обов'язкових **післявиборчих аудитів** систем для зміцнення рівня довіри виборців;
8. Уряду варто невідкладно **виділити ЦВК достатній обсяг фінансових ресурсів** для забезпечення потреб Комісії у сфері кібербезпеки з огляду на необхідність вжиття ЦВК заходів щодо низки ключових питань, які включають закупівлю, налаштування, тестування обладнання та навчання персоналу.

IFES ініціювала створення неформальної мережі "Кібербезпека українських виборів" для обміну ідеями, які можуть стати джерелом інформації для практиків. **IFES готова й надалі продовжувати надання Україні допомоги у виборчій сфері, у тому числі докладаючи максимум зусиль, спрямованих на посилення кібербезпеки у сфері виборів.**

Ця заява була підготовлена Командою з оцінювання кібербезпеки Міжнародної фундації виборчих систем (IFES) за підтримки Агентства США з міжнародного розвитку (USAID) та британської допомоги від уряду Великої Британії. Думки, викладені у цьому документі, належать автору і не обов'язково відображають погляди USAID, уряду США або уряду Великої Британії.