

# Кібербезпека на виборах в Україні

---

**Інтерактивний посібник із кібербезпеки**  
Передовий досвід подолання загроз для проведення виборів в Україні



**Інтерактивний  
посібник із кібербезпеки  
Передовий досвід подолання загроз  
для проведення виборів в Україні**

Листопад 2018 року

Міжнародна фундація виборчих систем

**Автори:**

*Горан Петров і Томас Шанюссо*

**Співавтори/Редактори:**

*Віктор Жора, Гіоргі Іашвілі  
Кетрін Еллена, Джульєт Шмідт*



*Ця брошура була підготовлена Міжнародною фундацією виборчих систем (IFES) за фінансової підтримки Агентства США з міжнародного розвитку (USAID) та британської допомоги (UK aid) від уряду Великої Британії. Будь-які думки, викладені в цій брошурі, належать автору і не обов'язково відображають погляди USAID, уряду США, Посольства Великої Британії в Україні або уряду Великої Британії.*

## Зміст

<b>Роль Міжнародної фундації виборчих систем (IFES): Кібербезпека на виборах</b> .....	5
Про нас .....	5
Нинішня та майбутня допомога в забезпеченні кібербезпеки на виборах .....	5
<b>Вступ</b> .....	7
Мета цього інтерактивного посібника .....	7
Для кого створено цей інтерактивний посібник .....	7
Кібербезпека виборів.....	8
ЦВК як критична інфраструктура.....	8
Хто несе відповідальність за захист виборів від зловмисників?.....	8
Комплексний підхід IFES до кібербезпеки на виборах (підхід HEAT) .....	9
<b>Виборча інфраструктура України</b> .....	10
Напередодні сезону виборів 2019 року.....	10
ЦВК і її Секретаріат .....	11
Державний реєстр виборців (ДРВ).....	11
Система реєстрації виборців в Україні.....	11
Структура ДРВ .....	11
Програмне забезпечення й конфігурація .....	12
Доступ і звітність.....	12
Веб-сайт ДРВ .....	12
Друк і передача списків виборців .....	13
Цілісність і точність ДРВ .....	13
Кадровий потенціал для обслуговування ДРВ .....	13
Підключення до мережі.....	13
Система встановлення результатів виборів (СВРВ).....	14
Характеристики СВРВ .....	14
Введення даних про результати голосування на рівні ОВК.....	14
Система передачі інформації про результати виборів (СПІРВ) .....	15
Термін придатності апаратних засобів і програмного забезпечення.....	15
<b>Антикризове планування, антикризове реагування</b> .....	16
<b>Підготовка до наступних виборів – Десять найбільших ризиків у галузі кібербезпеки, які потребують уваги ЦВК</b> .....	18
1. Кібергігієна, формування культури підвищеного рівня обізнаності в питаннях безпеки всередині й за межами організації .....	19
2. Підвищення суспільної довіри й поінформованості, комунікації та веб-сайт організації.....	22
3. Стійкість до шкідливого програмного забезпечення, регулярне оновлення апаратного й програмного забезпечення .....	26
4. Розбудова людського потенціалу, проблеми збереження й підготовки ключового персоналу.....	28



Інтерактивний посібник із кібербезпеки  
Усі права захищені. © Міжнародна фундація виборчих систем в Україні, 2018

Заява про дозвіл: жодна частина цієї публікації не може бути відтворена в будь-якій формі або будь-якими засобами, електронними чи механічними, включаючи фотокопіювання, запис або будь-який інший спосіб зберігання й пошуку інформації, без письмового дозволу Міжнародної фундації виборчих систем в Україні.

Запити на отримання дозволу повинні містити таку інформацію:

- Опис матеріалу, дозвіл на копіювання якого бажають отримати.
- З якою метою буде використано копійований матеріал і в який спосіб.
- Ваше ім'я, посада, назва компанії чи організації, номер телефону, номер факсу, адреса електронної пошти та поштова адреса.

Будь ласка, надсилайте всі запити на отримання дозволу до:

International Foundation for Electoral Systems  
2011 Crystal Drive, 10th Floor  
Arlington, VA 22202  
E-mail: editor@ifes.org  
Fax: 202.350.6701

5. Журнали моніторингу й роботи системи, важливість журналів діяльності («сліду») для кібер аудиту .....	29
6. Важливість політики в галузі кібербезпеки, стандартних операційних процедур і кодексу поведінки в галузі ІТ .....	31
7. Міжвідомча взаємодія, створення команди реагування на кризові ситуації на виборах ....	33
8. Доступ до цифрової інфраструктури .....	35
9. Привілейовані права доступу й неадекватний контроль .....	37
10. Фізичний захист цифрової інфраструктури.....	39
<b>Додаток 1 – Історія найбільш значних кібератак на об’єкти критичної інфраструктури в Україні .....</b>	<b>40</b>
Травень 2014 року – Кібератака на ЦВК.....	40
Жовтень 2015 року – Атаки на ЗМІ («БлекЕнерджі»).....	40
Грудень 2015 року – Атаки на енергорозподільні компанії («БлекЕнерджі») .....	40
Січень 2016 року – Кібератака на міжнародний аеропорт «Бориспіль» («БлекЕнерджі») ....	41
Кібератака на Міністерство фінансів України та Державну казначейську службу .....	41
Грудень 2016 року – Кібератака на Київенерго («Індустройер») .....	41
Грудень 2016 року – Кібератака на ІТ-системи «Укрзалізниця» .....	41
Червень 2017 року – Кібератака на українські компанії (вірус «(Не)Петя»).....	41
Жовтень 2017 року – кібератака на Київський метрополітен та Одеський аеропорт («БедРеббіт»).....	42
<b>Додаток 2 – Процес комплексного тестування вразливостей та адаптування систем (HEAT)....</b>	<b>43</b>
<b>Додаток 3 – Література з кібербезпеки на виборах.....</b>	<b>49</b>
Cybersecurity in Elections: Developing a Holistic Exposure and Adaptation Testing (HEAT) Process for Election Management Bodies [Кібербезпека на виборах: розробка процесу комплексного тестування вразливостей та адаптування систем (HEAT) для органів адміністрування виборів] (IFES, жовтень 2018 року).....	49
NIS CG Compendium of Cyber Security on Election Technology [Компендіум із кібербезпеки виборчих технологій, підготований групою співробітництва з мережевої та інформаційної безпеки] (липень 2018 року) .....	49
Election Infrastructure Security Resource Guide [Керівні принципи використання ресурсів для гарантування безпеки виборчої інфраструктури] (створено DHS, квітень 2018 року) .....	50
A Handbook for Elections Infrastructure Security [Довідник із безпеки інфраструктури виборів] (підготовано Центром Інтернет-безпеки, лютий 2018 року).....	50
Cybersecurity Playbook for Election Officials [Інтерактивний посібник із кібербезпеки для посадовців органів адміністрування виборів] (підготовано Белферським центром, лютий 2018 року).....	50
<b>Додаток 4 - Скорочення.....</b>	<b>51</b>

## Роль Міжнародної фундації виборчих систем (IFES): Кібербезпека на виборах

### Про нас

З 1987 року Міжнародна фундація виборчих систем (IFES) працює у 135 країнах світу задля надання підтримки громадянам, які реалізують своє право на участь у справедливих і демократичних виборах. Незалежна експертна підтримка, яку надає IFES, сприяє зміцненню виборчих систем і розбудові місцевого потенціалу для реалізації довгострокових рішень.

З 1994 року IFES відіграє ключову роль у становленні демократичних виборчих процесів й інститутів в Україні. IFES здобула репутацію надійного джерела інформації для об’єктивного аналізу та висококваліфікованої технічної допомоги в галузі реформування законодавства про вибори та політичне фінансування, а також адміністрування виборів, посилення спроможностей громадянського суспільства і вивчення громадської думки. Наразі IFES реалізує такі проекти в Україні: (1) Програма «Відповідальна та підзвітна політика в Україні», що фінансується Агентством США з міжнародного розвитку, а також (2) «Зміцнення законодавчих та виборчих процесів шляхом посилення громадської участі та надання технічної допомоги», що фінансується Британською допомогою від уряду Великобританії.

### Нинішня та майбутня допомога в забезпеченні кібербезпеки на виборах

Кібербезпека має значний вплив на стабільність України, особливо під час виборів. Наразі IFES надає підтримку Центральній виборчій комісії України (ЦВК) для посилення її кіберстійкості та захисту від кіберзагроз. У червні 2018 року IFES провела Оцінку кібербезпеки на виборах в Україні за участі представників виборчих та державних органів у сфері кібербезпеки та виборів, а також представників громадянського суспільства та комерційних постачальників. Дана Оцінка стала основою для короткострокових та довгострокових рекомендацій для ЦВК, враховуючи, що 2019 року в Україні мають відбутися президентські та парламентські вибори.

IFES продовжує надавати підтримку учасникам виборчих процесів у питаннях кібербезпеки, пов’язаних із виборами в Україні. До видів діяльності в цій сфері належать:

**Технічна підтримка:** IFES ділиться провідними практиками й рекомендаціями з ЦВК та іншими учасниками виборчих процесів в Україні, зокрема за допомогою цього інтерактивного посібника.

**Сприяння координації роботи/зусиль ключових учасників виборчих процесів:** IFES підтримує ЦВК у взаємодії з іншими учасниками виборчих процесів для полегшення обміну інформацією, а також долучається до проведення неформальних експертних «круглих столів», конференцій та інших заходів для фахівців у сфері кібербезпеки та виборів. Крім того, IFES заснувала робочу групу з питань кібербезпеки та виборів, яка постійно отримує оновлені тематичні матеріали англійською та українською мовами.

**Симуляція кризової ситуації із кібербезпеки:** в листопаді 2018 року IFES розробила та провела симуляцію кризової ситуації із кібербезпеки, щоби поліпшити навички працівників ЦВК з управління кризовими ситуаціями, таким чином посиливши їхню підготовку до кризових явищ у царині кібербезпеки в межах виборчого циклу.

**Інтерактивний тренінг із кібергігієни:** ґрунтуючись на власному багаторічному досвіді проведення інтерактивних тренінгів, серед яких – проект BRIDGE (Building Resources in Democracy, Governance and Elections), IFES розробили Інтерактивний курс із кібергігієни для членів ЦВК, працівників ЦВК та інших фахівців, що залучені до організації та проведення виборів, проте не є спеціалістами з інформаційних технологій. IFES проводить тренінги за допомогою власної мережі досвідчених тренерів.

**Тренінг для працівників IT-відділів ЦВК та Державного реєстру виборців (ДРВ):** IFES у співпраці з ЦВК організували низку тренінгів із питань інформаційної безпеки, безпеки мережі та методів аудиту безпеки, щоби підвищити рівень знань працівників IT-відділів, які матимуть справу з можливими кризовими явищами в галузі кібербезпеки.

**Міжнародний досвід та навчальні поїздки:** IFES надає можливість для спеціалістів з усього світу ділитися відповідними знаннями й власним набутим досвідом в Україні та за допомогою міжнародних навчальних поїздок, забезпечуючи порівняльний підхід та релевантний передовий досвід.

## Вступ

Все більше нових і різноманітних загроз з'являється в сучасних виборчих процесах. Деякі загрози вже добре відомі в Україні, зокрема, потенційні «чорні» хакерські атаки з боку кіберзлочинців усередині країни або ускладнені сталі загрози (від англ. Advanced Persistent Threats), ініційовані іноземними суб'єктами, під час яких зловмисники намагаються здобути та утримати несанкціонований доступ до комп'ютерної мережі впродовж тривалого періоду часу. До прикладів груп, які реалізували АРТ, належать АРТ28 або Fancy Bear («Прикольний ведмідь»), а також АРТ29, також відома як Cozy Bear («М'який ведмідь»). Існує думка, що саме група АРТ28 була організатором атаки на інфраструктуру ЦВК України в 2014 році. Інші хакерські групи менш відомі, але можуть мати не менш шкідливий вплив на демократичний виборчий процес.

## Мета цього інтерактивного посібника

Попри те, що наразі кібербезпека загалом отримує достатню кількість уваги, від початку запровадження інформаційних технологій у виборчих процесах питаннями кібербезпеки серйозно нехтували. Цей інтерактивний посібник розроблено на основі американського та європейського масиву знань та світового досвіду IFES задля поширення провідних практик у виборчій сфері. Він також містить інформацію щодо найпоширеніших загроз, щоби посилити обізнаність користувачів щодо ймовірних ризиків.

Поточний посібник не є вичерпним вузькоспеціалізованим документом. Значна кількість інформації розрахована на базове розуміння інформаційних технологій та певний рівень розуміння небезпек, пов'язаних зі зривом виборчих процесів.

Питання кібербезпеки виборчої системи України та захисту виборчої інфраструктури розглядаються у контексті передового міжнародного досвіду. В інтерактивному посібнику застосовано цілісний підхід, розроблений IFES для зниження рівня ризиків у сфері кібербезпеки, та запропоновано рекомендації як на загальному рівні, так і більш детальні (технічні) поради для короткострокових та довгострокових удосконалень.

Цей інтерактивний посібник не має на меті повністю охопити всі проблеми, пов'язані з кібербезпекою під час виборів. Наприклад, тема дезінформації під час виборчої кампанії не розглядається, оскільки ця сфера не є безпосередньою сферою відповідальності органів адміністрування виборів (ОАВ) чи ЦВК України зокрема, за винятком випадків поширення дезінформації щодо виборчих процесів.

Питання, що їх висвітлює посібник, добре відомі експертам із інформаційних технологій ЦВК, які також відповідають за безпеку дотичних систем: ДРВ, системи встановлення результатів виборів та системи цифрового завантаження даних. Ми сподіваємося, що цей документ буде корисним для експертів при покращенні захисту від кіберзагроз виборів в Україні.

Водночас інтерактивний посібник є живим динамічним документом, тому з коментарями та виправленнями звертайтеся, будь ласка, за адресою: [secureelectionsua@ifesukraine.org](mailto:secureelectionsua@ifesukraine.org).

## Для кого створено цей інтерактивний посібник

Цей посібник створено насамперед для членів ЦВК України та Секретаріату, однаковою мірою для спеціалістів з інформаційних технологій та інших спеціалістів. Він може бути корисним для членів окружних (ОВК) та дільничних виборчих комісій (ДВК), а також для інших учасників виборчого процесу, що зацікавлені у вирішенні питань кібербезпеки, як-от урядові установи, політичні партії або громадянське суспільство.

## Кібербезпека виборів

Цифрова інформація та взаємозв'язок через Інтернет прискорили комунікації й уможливили існування масштабованої економіки, проте водночас створили нові загрози для критичної інфраструктури. Діджиталізація ускладнює інформаційні системи та створює нові, дедалі більш складні способи їхнього використання, водночас посилюючи потенціал недобросовісної чи зловмисної діяльності.

Виборчі системи не є винятком із цього правила, незалежно від того, чи бюлетені викидаються у скриньки та підраховуються вручну чи за допомогою машин. Навіть якщо ОАВ скептично ставляться до впровадження електронного голосування, більшість ОАВ у світі певною мірою поспівають цифровими системами під час проведення виборів: від реєстрації виборців та до електронної публікації результатів виборів.

У контексті президентських і парламентських виборів в Україні 2019 року кібератаки є реальною й наявною загрозою.

Якщо під час виборів виникають сумніви, що волю виборців було чесно відображено в мандатах обраних посадовців, на місці сумніву виникає глибока рана, яку важко зцілити. Кібератаки можуть потенційно не лише

скомпрометувати виборчий процес, але й викликати сумніви та невпевненість у цілісності та справедливості виборів. Це актуально й коли кібератаки стаються окремо, й особливо коли вони відбуваються в поєднанні з будь-якими іншими позірними порушеннями, суперечностями або спорами. Російська окупація Криму та конфлікт у Східній Україні мають чіткі характеристики гібридної війни, в якій традиційні методи ведення війни та кібертактики поєднуються з іншими методами. З наближенням президентських та парламентських виборів у 2019 році перспектива кібератак, які можуть уразити критичні системи, може мати серйозні наслідки для країни.

## ЦВК як критична інфраструктура

Відносно новий Закон «Про основні засади забезпечення кібербезпеки України» (чинний з травня 2018 року) надає урядові можливість визначати певну інфраструктуру як критичну. Попри те, що уряд ще не схвалив перелік об'єктів критичної інфраструктури, системи ЦВК є вже де факто об'єктами критичної інфраструктури. Досі усталена практика була такою, що Державна служба спеціального зв'язку та захисту інформації (Держспецзв'язок) та Служба безпеки України (СБУ) тісно співпрацювали з ЦВК упродовж кількох днів до і після дня виборів, щоб допомогти забезпечити як захист мережі, так і загальну інформаційну безпеку. ЦВК лише виграє від формалізації цього процесу, оскільки він у прозорий спосіб визначатиме, на які державні ресурси може покладатися ЦВК, що забезпечить її незалежність від інших установ, а також чітко визначить, хто за що відповідатиме.

**Рівні захисту з боку Держспецзв'язку:**  
Внутрішньо-державні системи (захищені CERT-UA)  
Інші державні органи (решта уряду)  
Критична інфраструктура в публічній власності (датчики)  
Критична інфраструктура в приватній власності (датчики)

## Хто несе відповідальність за захист виборів від зловмисників?

ОАВ в усьому світі відповідають за проведення справедливих, інклюзивних, демократичних виборів, які відображають волю людей. Попри те, що часто існує низка урядових структур, що відповідають за безпеку виборів і кібербезпеку зокрема, саме ОАВ найчастіше сприймаються

громадськістю як відповідальні за створення безпечного середовища для проведення виборів. В Україні, подібно до багатьох інших держав, вибори проводяться постійним, централізованим ОАВ, що очолює структуру окружних та місцевих виборчих комісій. ЦВК України є формально незалежним органом.

Окрім того, у випадках, коли ОАВ керує певними частинами виборчої інформаційної інфраструктури, як-от реєстром виборців, виникає згода в розумінні, що ОАВ також несе відповідальність за захист подібних даних. Незважаючи на те, що подібна роль може бути не закріплена на рівні прецедентного законодавства, застосування санкцій проти ОАВ на Філіппінах у 2016 році може бути показовим випадком щодо відповідальності ОАВ за кібербезпеку. У березні 2016 року Філіппінська комісія з виборів (COMELEC) зазнала хакерської атаки, вчиненої групою «Анонімні філіппінці». Хакери зламали веб-сайт COMELEC та злили назовні значну кількість інформації про виборців, зокрема відбитки пальців. Національна комісія з питань захисту персональних даних також рекомендувала запровадити кримінальну відповідальність щодо голови COMELEC Андреаса Баутіста за службову недбалість. Ця справа є переконливим прикладом того, що ОАВ та їхні члени можуть нести організаційну та особисту відповідальність за кібербезпеку на виборах. ЦВК України несе загальну відповідальність за ведення реєстрів виборців, а також за всі інші виборчі системи та заходи.

Національна система кібербезпеки України складається з Ради національної безпеки і оборони України, Держспецзв'язку, СБУ, Національної поліції, Міністерства оборони та Служби зовнішньої розвідки.

Незважаючи на те, що ЦВК несе як юридичну, так і фактичну відповідальність за належне гарантування кібербезпеки власних систем, під час проведення виборів діяльності комісії допомагають Держспецзв'язок, СБУ, Національна поліція, Рада національної безпеки та оборони України, Міністерство оборони та Служба зовнішньої розвідки. Зазвичай ця допомога полягає в наданні та експлуатації датчиків для оповіщень та попереджень, а також у координації зусиль на випадок інцидентів. Гарантування незалежності української ЦВК та попередження будь-якого негативного зовнішнього впливу, як реального, так і незримого, є критично важливим. Отже, для цілісності виборів і для довіри громадян до виборчого процесу надзвичайно важливо переконатися, що будь-яка допомога є прозорою, а офіційна міжвідомча співпраця спрямована на виявлення, запобігання та реагування на загрози.

## Комплексний підхід IFES до кібербезпеки на виборах (підхід HEAT)

Для захисту від кібератак необхідно застосовувати міждисциплінарний підхід та мати розуміння потенційних векторів загрози. Наприклад, злам облікового запису політика у Facebook може спричинити серйозні проблеми з, на перший погляд, не пов'язаними до цього питаннями, як-от зниженням довіри учасників виборчого процесу до цілісності ДРВ.

IFES розробили методику опису, зменшення наслідків та запобігання загрозам кібербезпеки за допомогою методу, що називається «Процес комплексного тестування вразливостей та адаптування систем» (HEAT, від англ. Holistic Exposure and Adaptation Testing). Метою підходу HEAT є визначити й усвідомити п'ять основних вразливостей до потенційних загроз: через використання технології, через кадровий/людський потенціал, через політичні, законодавчі та процедурні вразливості. Кожна з них розглядається окремо та узгоджено на основі використання п'ятирівневого функціонального підходу, що передбачає ідентифікацію, збір даних, виявлення вразливостей, випробування та адаптацію.

Більше інформації про методику HEAT, розроблену IFES, наведено у Додатку. Повний огляд доступний на веб-сайті IFES.

## Виборча інфраструктура в Україні

### Напередодні сезону виборів 2019 року

Сстійкі загрози в площині кібербезпеки в поєднанні з уразливостями виборчої системи створюватимуть значні ризики під час проведення майбутніх президентських і парламентських виборів, призначених на 31 березня і 27 жовтня 2019 року відповідно.

Захищеність системи виборів від кібератак стала темою до активного обговорення серед кіберспільноти в Україні, до того ж вже було докладено значних зусиль для підвищення безпеки об'єктів критичної інфраструктури. Після зухвалої кібератаки на цифрову інфраструктуру напередодні дострокових президентських виборів 22 травня 2014 року ЦВК вдалися до низки вдосконалень у царині кібербезпеки. Прагнучи посилити захист від кіберзагроз усередині організації, ЦВК відокремили офісну мережу (для виконання поточних робочих завдань) від критично важливих мереж та встановили сучасну й комплексну систему моніторингу мережі, почасти завдяки співпраці з державними органами безпеки. ЦВК також замінює застаріле обладнання для критично важливої мережі та модернізує основні компоненти апаратного й програмного забезпечення (публічні веб-сайти, сервери, мережеве обладнання). Працівники ЦВК також стали набагато більш обізнаними з ризиками, які кібератаки становлять для виборів, а всі працівники Секретаріату наприкінці 2018 року пройшли навчання з кібергігієни.

У цьому розділі ми спробували розглянути кібербезпеку виборів і необхідність захисту виборчого процесу та каналів передачі даних про результати виборів.



### ЦВК і її Секретаріат

Як незалежна інституція ЦВК має широкі повноваження для підготовки й контролю за проведенням президентських і парламентських виборів. Повноваження ЦВК на місцевих виборах є більш обмеженими. ЦВК складається з 17 членів, які призначаються Верховною Радою за поданням Президента після проведення консультацій із політичними фракціями й групами. Наразі одне з 17 місць у складі Комісії залишається вакантним; представлено всі парламентські партії, окрім однієї.

Оновлення складу ЦВК у жовтні 2018 року дало надію на вирішення деяких проблемних питань у галузі кібербезпеки, як-то брак прозорості в певних аспектах виборчого процесу.

Оновлений склад ЦВК вже продемонстрував серйозне ставлення до питання кібербезпеки виборів. Одного з членів Комісії було призначено опікуватися цією тематикою й брати безпосередню участь у низці заходів, зокрема в навчанні співробітників як ІТ-персоналу, так і працівників інших департаментів, що проводиться за підтримки IFES.

Секретаріат ЦВК є професійним органом і має штат висококваліфікованих адміністративних фахівців, які працюють у ЦВК на постійній основі – це близько 250 співробітників, які працюють у 15-ти департаментах. ОВК – це тимчасові органи, які створюються за 40 днів до дня голосування на президентських виборах і за 62 дні до голосування на парламентських виборах. Служба Державного реєстру виборців (ДРВ) є окремою організаційною одиницею у складі ЦВК і має чотири департаменти.

### Державний реєстр виборців (ДРВ)

#### Система реєстрації виборців в Україні

Списки виборців формуються на основі бази даних ДРВ, яка підтримується на центральному рівні фахівцями окремого підрозділу в межах ЦВК. Процес реєстрації є пасивним, а отже, за законом влада зобов'язана вносити до ДРВ усіх українських громадян, які мають право голосу.

Загалом в Україні зареєстровано близько 31 мільйона виборців. Як розпорядник ДРВ ЦВК укладає реєстр на підставі даних, отриманих від місцевих органів влади, що видають посвідчення особи громадян/паспорти та реєструють зміни місця постійного проживання та громадянського стану, як-от шлюб і смерть.

З погляду кібербезпеки, ДРВ не перебуває в зоні безпосередньої критичної загрози здебільшого через те, що на виборчих дільницях зберігається система використання паперових списків. Однак точність вихідних даних у списках виборців у день голосування є тим питанням, яке заслуговує на окрему увагу. Наприклад, муніципальна влада, яка відповідає за зняття з реєстрації та реєстрацію виборців на підставі місця постійного проживання, може не надати вчасно оновлену інформацію місцевим офісам у державній адміністрації, які, зі свого боку, не зможуть вчасно подати інформацію працівникам ДРВ для внесення змін до реєстру виборців.

#### Структура ДРВ

ДРВ оновлюється в електронному вигляді на основі даних, представлених 27 органами адміністрування реєстру (ОАР) і 761 органом ведення реєстру (ОВР) виборців, які контролюються ЦВК. ОВР є частиною державної адміністрації на районному рівні. Взаємодія зі всіма відповідними органами, розташованими в Автономній Республіці Крим і Севастополі (в цілому 33) наразі не можлива через окупацію Кримського півострова Росією. На сході країни через конфлікт на

Донбасі припинена взаємодія з 32 з 62 відповідних органів у Донецькій та з 19 з 34 відповідних органів у Луганській областях.

ДРВ оновлюється щомісяця. Державні та місцеві установи передають більшість даних до ОВР в електронному вигляді.

Служба ДРВ регулярно оновлює та чистить реєстр виборців на центральному рівні ЦВК, наприклад, шляхом видалення дублікатів записів (які виникають через повторну реєстрацію без зняття з попередньої). ЦВК є не лише розпорядником реєстру виборців, але й безпосередньо адмініструє базу ДРВ.

## Програмне забезпечення й конфігурація

База даних ДРВ і його користувацький інтерфейс, зокрема система введення даних для ОВР, розробляються безпосередньо командою Служби розпорядника ДРВ у ЦВК. Служба розпорядника ДРВ не укладає контрактів із зовнішніми підрядниками, а отже не має пов'язаних із цим ризиків, але цілком залежить від свого внутрішнього потенціалу для підтримки та технічного обслуговування системи.

Виділені лінії зв'язку під'єднано до кластера маршрутизаторів, які направляють трафік на сервер ДРВ.

## Доступ і звітність

У зв'язку з необхідністю забезпечити працівників ДРВ безперервним доступом і можливістю обробки даних, завжди є ризик випадкової (або потенційно навмисної) зміни даних, що може призвести до погіршення якості реєстру виборців. Наприклад, подібні випадки можливі при виявленні дублікату облікового запису виборця, адже передбачено, що Служба розпорядника ДРВ має видалити один із дублікатів шляхом зміни даних.

## Веб-сайт ДРВ

За інформацією Служби розпорядника ДРВ, починаючи з 2013 року близько 200 000 виборців перевірили дані про себе у ДРВ. Наразі процес онлайн перевірки статусу реєстрації вимагає від виборця попередньої реєстрації облікового запису (аккаунта). Такий обліковий запис можна створити за допомогою низки сервісів (Facebook, Google, BankID та ін.), однак активується він лише за 48 годин від моменту реєстрації. Це може стримувати виборців, які бажають перевірити дані про себе онлайн. Веб-сайт для перегляду детальних даних виборців має добре організований інтерфейс, тож користувачі можуть легко отримати доступ до інформації про виборчі дільниці.

Відповідно до провідних практик, обладнання, що під'єднане до мережі Інтернет, зокрема сервери, які дозволяють громадянам перевіряти дані про себе в реєстрі, відокремлено від основної мережі ДРВ. Тому злам веб-сайту в критичні періоди – до дня голосування, в період між публікацією попередніх і остаточних списків виборців – не зашкодить оригінальній базі даних ДРВ. Однак, якщо такі атаки виявляться успішними, вони можуть підірвати довіру до рівня захисту системи ДРВ, особливо якщо вони відбуватимуться разом із дезінформаційною кампанією, наголошуючи шкоду, яку такі атаки нібито можуть заподіяти. Зрештою довіра до цілісності списку виборців також може знизитися.

У серпні 2018 року хакер із відомої спільноти «Український кіберальянс» продемонстрував уразливість веб-сайту ДРВ і розмістив інформацію про це у Facebook. Хакер виявив незахищеність від XSS (міжсайтового скриптингу), що потенційно може поставити під загрозу користувачів із доступом до веб-сайту ЦВК (шкідливим наслідком такої атаки може бути, наприклад, крадіжка

особистого логіну члена ЦВК для авторизації доступу до електронної пошти). Крім того, хакер публічно підняв питання щодо належного захисту ДРВ. Статтю-відповідь на цю тему було опубліковано у вересні 2018 року.

Навіть попри пояснення ЦВК, що небезпека від атак XSS є перебільшеною, оскільки основна база даних ДРВ і веб-сайт є відокремленими системами, все ж не варто применшувати вплив подібних випадків на суспільне сприйняття.

## Друк і передача списків виборців

Друк та передача списків виборців на виборчі дільниці (списки виборців рівня ДВК) є критично важливим процесом, який потребує надійного захисту. Згідно з законом, попередні списки виборців передаються на виборчі дільниці в часовий проміжок від одного до трьох тижнів до дня голосування залежно від типу виборів, а уточнені списки виборців передаються не пізніше, ніж за два дні до дня голосування.

Якщо виникає затримка з передачею попередніх списків виборців на виборчі дільниці, це перешкоджатиме можливості виборців ознайомитися зі списками, дізнатися про місце голосування й переконатися, що їх включено до списку на відповідній виборчій дільниці. Якщо ж виникає затримка з передачею уточнених списків виборців, це може критично вплинути на виборчий процес, адже в день голосування реєстрація виборців на виборчих дільницях заборонена.

## Цілісність і точність ДРВ

ЦВК покладається на цілісність центральної бази даних ДРВ, яка забезпечує відсутність будь-якої втрати даних зареєстрованих виборців. У разі інцидентів порушення кібербезпеки або випадкової втрати даних ЦВК має бути в змозі діяти швидко й чітко. Необхідно регулярно створювати резервні копії даних онлайн та в автономному режимі (офлайн), аби в разі необхідності систему можна було відтворити з резервної копії. Відновлення значної частини втрачених даних – це складний процес, тому необхідно випрацювати та регулярно переглядати план аварійного відновлення, особливо для такої критично важливої бази даних, як ДРВ. Зважаючи на постійні зміни даних виборців, першорядного значення набуває практичний підхід, що включає додаткове й повне резервне копіювання бази даних онлайн та в автономному сховищі.

## Кадровий потенціал для обслуговування ДРВ

Оператори ДРВ в ОАР та в ОВРО є працівниками департаментів державних адміністрацій на місцевому рівні й отримують відповідну винагороду за свою роботу.

Рівень оплати праці в сфері IT/кібербезпеки в приватному секторі значно вищий, тому важко зберегти кваліфікований персонал у державному секторі. Дані за останні роки доводять ротацію майже третини всього IT-персоналу. ЦВК і представники урядових установ, які працюють у галузі безпеки, неодноразово підкреслювали, що брак достатніх людських ресурсів є давньою проблемою в усіх органах державної влади.

І навіть якщо звичайні оператори введення даних до ДРВ, особливо в ОВР, не повинні мати широкий спектр навичок із експлуатації і функціонування програмного забезпечення ДРВ, кібергігієна і дисципліноване суворе дотримання процедур безпеки, встановлених ЦВК, мають великий значення для запобігання можливим порушенням.

## Підключення до мережі

ОВР підключені безпосередньо до Служби розпорядника ДРВ у ЦВК волоконно-оптичним зв'язком, що надається підприємством «Укртелеком». Ризики, що виникають у зв'язку з цим, це

перш за все можливість фізичного пошкодження чи знищення основних вузлів мережі “Укртелекому”. Завдання забезпечити фізичний захист цих активів покладене урядом України на Національну поліцію.

## Система встановлення результатів виборів (СВРВ)

### Характеристики СВРВ

Процеси зведення та управління результатами під час виборів 2019 року будуть подібними до аналогічних процесів, які використовувалися на виборах у 2014 році. База даних СВРВ і програмне забезпечення розробляються наново для кожних виборів на основі попередньої системи. Схеми проектування та взаємозв'язок, а також включення й розташування окремих компонентів, оновлюються або змінюються.

Основним компонентом є головний сервер баз даних, до якого безпосередньо підключені ОВК.

Зважаючи на те, що ОВК є тимчасовими органами, система встановлення результатів на рівні виборчого округу не налаштовується до моменту створення ОВК безпосередньо перед кожними виборами.

Система передачі інформації про результати виборів (СПІРВ) є невід'ємною частиною СВРВ, але вона відокремлена від основної інфраструктури СВРВ. Ця система має бути доступною через Інтернет, щоб громадськість мала змогу переглядати результати виборів.

Дуже важливо усвідомлювати, що результати виборів, які публікуються на веб-сайті ЦВК протягом ночі після дня голосування, є попередніми. Офіційні результати зазначаються в підписаних підсумкових протоколах підрахунку голосів. Таким чином, навіть якщо із СВРВ трапляються інциденти, це не означає порушення цілісності результатів виборів. Паперовий звіт про результати голосування залишається на кожній виборчій дільниці (протокол ДВК про підрахунок голосів виборців на виборчій дільниці) і дозволяє забезпечити цілісність результатів. Усі електронні дані перевіряються на відповідність офіційним паперовим документам. Проте вдала атака на систему результатів, залежно від її ступеня складності, може негативно вплинути на виборчий процес, посиливши плутанину, невизначеність і сумнів серед учасників виборчого процесу щодо встановлених результатів.

ЦВК співпрацюватиме з Держспецзв'язком України над відпрацюванням вразливостей СВРВ, а також над тестами системи на проникнення (пен-тестами), як це вже відбувалося під час попередніх виборів.

### Введення даних про результати голосування на рівні ОВК

ЦВК не має спеціального обладнання для введення даних про результати голосування для ОВК, адже вони не є постійними органами Комісії. ОВК зазвичай використовують комп'ютери, отримані від місцевих державних адміністрацій. На попередніх виборах траплялися навіть випадки використання приватних комп'ютерів. Це може становити найбільшу кібервразливість для СВРВ.

Такі комп'ютери підключені до розподіленої захищеної мережі СВРВ, але не перебувають під повним контролем, тож цілком імовірно, що на них можливо встановити шкідливе програмне забезпечення або ж вони можуть лишитися без нагляду чи належного захисту.

## Система передачі інформації про результати виборів (СПІРВ)

СПІРВ – це розподілена система, фізичні носії якої розміщено в декількох місцях, таким чином однією з найбільш очевидних цілей системи для потенційних атак під час проведення виборів є пов'язаний з нею вебсайт.

Час «пікового» інтересу широкої громадськості до передачі інформації про результати виборів досить обмежений – цілком імовірно, це лише кілька годин протягом ночі дня голосування, особливо під час президентських виборів, коли встановлення результатів не потребує складних формул для підрахунку голосів.

Копії результатів (snapshots) з внутрішньої захищеної системи СВРВ копіюються на зовнішній веб-сервер, який використовується для розміщення результатів голосування й регулярно оновлюється.

Держспецзв'язок України займається моніторингом мережі й датчиками несанкціонованого втручання до веб-серверу ЦВК. Результати потрапляють на кілька сайтів-дзеркал у декількох місцях в Києві, що дозволяє протидіяти DDoS-атакам. Громадськість має вільний доступ до веб-сайту з прозорою переадресацією на відповідне дзеркало.

### Термін придатності апаратних засобів і програмного забезпечення

Застаріле обладнання стає проблемою кібербезпеки, коли виробники припиняють його обслуговування та забезпечення. Маршрутизатори, якими послуговувалися в ЦВК до кінця 2018 року, було визнано вразливими компанією-постачальником, яка припинила обслуговування цього обладнання. Зловмисники можуть використати їх для отримання неправомірного доступу до мереж ЦВК, що може загрожувати як СВРВ, так і ДРВ. Наразі ЦВК проводить закупівельні процедури для заміни й модернізації свого застарілого обладнання за підтримки IFES. Своєчасне встановлення та тестування цього обладнання буде критично важливим для захисту систем, які ЦВК використовуватиме на виборах у 2019 році.

## Антикризове планування, антикризове реагування

Створення плану реагування на кризові ситуації може здаватися занадто складним завданням для ОАВ, оскільки існує надто багато речей, які необхідно врахувати, при цьому працівникам ОАВ може здаватися, що вони не мають усієї необхідної підтримки.

Незважаючи на це, перед ОАВ стоїть завдання підготуватися до найгіршого варіанту розвитку подій, вважаючи, що зловмисники знайдуть спосіб зірвати виборчий процес. Це завдання є настільки ж важливим, як і створення системи захисту від кіберзагроз. Щоб запобігти такому розвитку подій, ОАВ повинні ретельно підготуватися та спланувати, що працівники ОАВ робитимуть у випадку настання кіберінциденту для подолання його наслідків як всередині організації, так й у взаємодії із громадськістю.

### 1. Комунікаційний план

Метою комунікаційного плану, а також метою діяльності відділу комунікацій в цілому під час та після кіберінциденту, є підтримка суспільної довіри до виборчого процесу.

ОАВ, особливо відділи комунікацій, повинні мати достатні знання про інцидент, щоб інформувати громадськість про його характер та наслідки.

Надалі ми ще розглянемо це питання, проте іноді може бути важко знайти баланс між тим, що можна повідомити суспільству, і тим, що необхідно зберегти у таємниці, щоб не дати можливості зловмисникам знайти шляхи загострення проблеми. Між тим, на основі попереднього досвіду можна зробити висновок, що все, що не містить безпосереднього ризику загострення проблеми, необхідно спокійно пояснювати суспільству.

Комунікаційний план має містити стратегію публікацій, визначати ролі й обов'язки представників відділу комунікацій та членів виборчої комісії. Подібний комунікаційний план має враховувати схему реагування на кіберінциденти, сформовані на досвіді попереднього врегулювання подібних кіберінцидентів та рекомендаціях IT-відділу.

Для того, щоб отримати більше інформації щодо підготовки координованої комунікації у випадку кіберінцидентів, зверніть увагу на шаблон комунікаційного плану при кіберінцидентах на виборах, що розміщено у додатку.<sup>1</sup>

For more information about the preparation of coordination of cyber incident communication, refer to the Election Cyber Incident Communications Plan Template<sup>1</sup>.

### 2. План дій у надзвичайних ситуаціях/План забезпечення безперервності операцій

План забезпечення безперервності операцій необхідний для того, щоб гарантувати, що критично важливі процеси, пов'язані з виборами, продовжуються в звичний спосіб, попри надзвичайну ситуацію або катастрофу. Попри те, що ми звертаємо основну увагу на можливі кіберінциденти, план дій під час надзвичайних ситуацій має також враховувати питання поза кібербезпекою, наприклад, імовірність виникнення пожежі або будь-якої іншої небезпеки, що може перешкодити звичайному перебігу виборчого процесу.

План забезпечення безперервності операцій передбачає вивчення організаційних загроз та встановлення переліку основних завдань, які необхідно виконувати для продовження основних операцій виборчого процесу з мінімальними відхиленнями від звичної практики у разі, якщо ці потенційні загрози реалізуються. Такий план може передбачати перехід до резервного центру обробки даних у разі, якщо на головний центр обробки даних буде здійснена атака, а також застосування ручного підрахунку голосів та фізичної передачі файлів у випадку, якщо мережа для обміну даними між ОВК та ЦВК буде порушена.

### 3. План відновлення

План відновлення, на відміну від плану забезпечення безперервності операцій, стосується створення умов для відновлення даних і програмного забезпечення, яке обслуговує виборчий процес, у разі збоїв у роботі, пошкодження або знищення центрів обробки даних, серверів або іншої ключової інфраструктури.

У плані відновлення після аварійної ситуації необхідно детально визначити розташування кожного резервного сховища й місця проведення резервного копіювання, а також описати необхідні для отримання резервної копії процеси. Ці процеси необхідно регулярно тестувати.

Важливим міркуванням під час розробки такого плану є час, необхідний для відновлення даних (час простою), оскільки він може суттєво вплинути на довіру суспільства до виборчого процесу.

Формат реагування на кризову ситуацію, означений в антикризовому плані, необхідно перевірити, пояснити та відпрацювати з усіма задіяними сторонами.

Технічна симуляція – це найкращий інструмент для забезпечення чіткого розуміння ланцюга команд та процесів обміну інформацією:

- ▶ на внутрішньому рівні до такої симуляції кризової ситуації слід залучити відділ комунікацій, IT-відділ (або ж агенцію, яка має технічні знання систем та інфраструктури), а також будь-які інші відповідні підрозділи ОАВ, які часто лишаються поза увагою, як-от юридичний та операційний відділи;
- ▶ на зовнішньому рівні за необхідності до ліквідації чи деескалації інциденту необхідно долучити партнерські організації, які надають послуги в галузі безпеки або ж групу реагування на надзвичайні ситуації у комп'ютерній мережі CERT; при цьому також варто залучати до цього ЗМІ, політичні партії, організації громадянського суспільства та інших суб'єктів, які можуть збільшити довіру громадськості до виборчого процесу.

ОАВ виграють найбільше, якщо повною мірою використовуватимуть усі зовнішні ресурси та внутрішній потенціал для виявлення, моніторингу та реагування на інциденти, які виходять за межі їхньої організаційної (інколи обмеженої) спроможності. Важливо залучати групи CERT та інші організації, які працюють у сфері кібербезпеки, до такого планування, щоб чітко визначити ролі та обов'язки всіх задіяних сторін, а також звертатися до них під час самого інциденту, коли міжвідомча взаємодія на високому рівні необхідна для успішного вирішення кризової ситуації. Симуляції дають можливість тестувати не тільки внутрішні можливості й готовність протистояти кризовим ситуаціям, але й перевіряти механізми спільної координації та реагування; по суті, це є єдиним способом виявлення вразливостей та відточення стратегій реагування на кризові явища, окрім власне реального інциденту в режимі реального часу.

<sup>1</sup> <https://www.belfercenter.org/publication/election-cyber-incident-communications-plan-template>

## Підготовка до наступних виборів – Десять найбільших ризиків у галузі кібербезпеки, які потребують уваги ЦВК

Цей розділ посібника присвячено огляду десяти найбільш актуальних для України кіберризиків під час виборів. Ризики та загрози, а також пропозиції до їхнього вирішення було описано та систематизовано таким чином, щоб цими рекомендаціями могли також скористатися розпорядники виборчих процесів і в інших державах.

Методика аналізу ризиків HEAT, розроблена IFES, використовується для мапування вразливостей і загроз, а також для визначення 10 найбільших ризиків, що мають значний вплив на вибори.

1. Кібергігієна, формування культури підвищеного рівня обізнаності в питаннях безпеки всередині та за межами організації
2. Підвищення суспільної довіри та поінформованості, комунікації та веб-сайт організації
3. Стійкість до шкідливого програмного забезпечення, регулярне оновлення апаратного та програмного забезпечення
4. Розбудова людського потенціалу, проблеми збереження та підготовки ключового персоналу
5. Журнали моніторингу мережі та роботи системи, важливість журналів («сліду») для кібераудиту
6. Важливість політики в галузі кібербезпеки, стандартних операційних процедур та кодексу поведінки в галузі ІТ
7. Міжвідомча взаємодія, створення команди з реагування на кризові ситуації на виборах
8. Доступ до цифрової інфраструктури, нагляд за всіма активними пристроями
9. Привілейований доступ та контроль доступу: знати хто, що і де робить у будь-який час
10. Фізичний захист цифрової інфраструктури, захист поза межами сфери виключно цифрових технологій

Більше інформації про методику HEAT наведено у Додатку 2 до цього інтерактивного посібника.

## 1. Кібергігієна, формування культури підвищеного рівня обізнаності в питаннях безпеки всередині й за межами організації

Люди роблять помилки. Згідно зі звітом із кібербезпеки компанії IBM за 2014 рік<sup>2</sup>, 95 відсотків усіх інцидентів у сфері безпеки трапляються через людські помилки. Дотримання правил кібергігієни дозволяє захистити та підтримати функціонування ІТ-систем і пристроїв, а також впровадити використання передового досвіду в царині кібербезпеки. Це найважливіший інструмент будь-якої організації для зменшення наслідків людських помилок у сфері кіберзахисту.

Кібергігієна – це онлайн-аналог особистої гігієни. Це повсякденні процедури, випадкові перевірки та загальні правила поведінки, дотримання яких забезпечує онлайн-здоров'я (безпеку) користувача в Інтернеті.

ЦВК вже розпочали тренінги із кібергігієни, розроблені IFES. ЦВК використовує комплексний та інтерактивний навчальний модуль із кібергігієни, частково заснований на методиці BRIDGE, а також адаптований до українських реалій. Представники ОБК також залучатимуться до навчання після створення комісій на місцях.

**Тренінг із кібергігієни охоплює наступні провідні практики:**

1. Виявлення та припинення спроб фішингу/спір-фішингу
2. Провідні практики у сфері використання паролів
3. Резервне копіювання та захист даних
4. Оновлення програмного забезпечення й антивірусних програм
5. Політика чистого столу й чистого екрану
6. Застереження при використанні USB-пристроїв
7. Небезпека Інтернету речей (IoT)
8. Соціальні мережі

**Інші учасники виборів, наприклад політичні партії або ОГС, мають інші потреби, і спеціально для них можливо також охопити такі додаткові питання:**

9. Адміністрування сторінок у соціальних медіа
10. Використання різних каналів для різних видів комунікацій
11. Використання хмарних обчислень, коли це має сенс

Тренінгів із кібергігієни загалом ніколи не може бути надто багато. Усі зацікавлені сторони, від політичних партій до ЗМІ, ОГС та всі учасники виборчого процесу повинні розглянути питання про відрядження їхніх працівників для проходження навчання з кібергігієни перед виборами, а також проводити курси підвищення кваліфікації перед кожною виборчою подією.

<sup>2</sup> <https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=77014377USEN>

## Рекомендації для ЦВК:



### ІДЕНТИФІКАЦІЯ І ЗБІР ДАНИХ:

- ▶ Регулярно переглядайте будь-які наявні функціональні можливості, операційні плани й плани організації заходів безпеки, виявляйте потенційні місця для людських помилок та включайте їх до програми навчання з кібергігієни.



### ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ:

- ▶ Нові працівники повинні проходити тренінги з кібергігієни, щойно вони вступають на роботу, задовго до початку фази підготовки до виборів.



### ВИПРОБУВАННЯ:

- ▶ Знайти правильний баланс між безпекою та придатністю до використання може виявитися складним завданням. ЦВК, як і всі організації, повинна вибрати, і якщо можливо, протестувати рекомендації із кібергігієни на невеликій вибірці користувачів, а також подбати про те, як досягти високого ступеня впливу на безпеку організації без створення великих незручностей для користувачів.



### АДАПТАЦІЯ:

- ▶ IT-відділ/відділ кібербезпеки має періодично переглядати вектори загроз, які виникають найчастіше, та оцінювати пов'язані з ними ризики, а також впроваджувати заходи з кібергігієни для зниження рівня цих ризиків. Це може бути, наприклад, періодична зміна паролів або багатофакторна автентифікація для доступу до електронної пошти.
- ▶ Зміст тренінгів із кібергігієни необхідно регулярно оновлювати, а також, коли це можливо, навчальні курси необхідно повторювати перед кожними виборами, таким чином, щоб дати достатню кількість часу користувачам для того, щоб зрозуміти, осмислити та адаптувати провідні практики в галузі кібербезпеки (листопад 2019 року та далі).
- ▶ Поедняйте тренінги з кібергігієни з інформаційними кампаніями з підвищення обізнаності в питаннях кібербезпеки, які пояснюють, як проводити внутрішні комунікації щодо ризиків у сфері кібербезпеки.

## Приклади вразливостей за параметрами:



**ТЕХНОЛОГІЧНІ:** Багато технологічних вразливостей є вкоріненими у людському параметрі. Широке використання піратського програмного забезпечення може стати причиною поширення шкідливого програмного забезпечення для викрадення персональних даних, поширення вірусних програм та створення додаткових «чорних входів» для проникнення в систему. Навіть якщо зрив виборчого процесу не є початковим наміром хакера, який ініціював розповсюдження шкідливого програмного забезпечення через піратські програми, проникнення у виборчу мережу може призвести до не запланованого заздалегідь злочину, коли хакери зрозуміють, до якої системи вони потрапили.



**КАДРОВІ/ЛЮДСЬКІ:** Заклопотані люди великою мірою стають жертвами зручності, особливо у період напружених останніх днів підготовки перед виборами. Випрацювання звичок, які можуть обмежити вплив зловмисників, як-от підозріле ставлення та

відповідне поводження з будь-якими небажаними електронними повідомленнями, навіть якщо вони отримані від близьких колег, вимагає дисципліни.

Помічники керівників або членів виборчих комісій, адміністратори, координатори міжвідомчої взаємодії та працівники відділу комунікацій можуть стати значно цікавішими «цільми» для кіберхакерів, ніж це може здаватися. Навіть досвідчені користувачі можуть стати жертвами, як правило, через те, що вони нехтують новими загрозами та недооцінюють їх, оскільки їхні попередні знання про кіберзагрози швидко стають застарілими. Наприклад, деякі досвідчені користувачі, особливо серед працівників IT-відділів, не встановлюють антивірусне програмне забезпечення, вважаючи, що робота антивірусу може дати додаткове навантаження на ефективність роботи перевіреного комп'ютера.



**ПОЛІТИЧНІ:** Належна кібергігієна є відповідальністю команди, вона поширюється на всі рівні організації. Дуже часто стається так, що IT-відділ може попереджати керівництво ОАВ про те, що на серверах не встановлювалися патчі, або ж що на серверах може використовуватися застаріла операційна система (ОС), яка вже не підтримується, але ОАВ може вирішити, що оновлення програмного забезпечення буде занадто дорогим, забере занадто багато часу або що поточний момент є надто наближеним до дати виборів. Виборча комісія запитує IT-відділ, чи можна провести вибори без серйозного оновлення та очікує, що відповідь буде «так».

Кількість атак, спрямованих проти допоміжних систем (систем, які безпосередньо не знаходяться під контролем ОАВ, але можуть мати значний вплив на виборчий процес), постійно зростала в усьому світі за останні 4 роки. Таким чином, це тільки підкреслює важливість кібергігієни та кібербезпеки в цілому, не лише для ОАВ, але й для всіх зацікавлених сторін. Найвідоміший випадок - це, мабуть, злам облікового запису персональної електронної пошти (за допомогою фішингу) керівника виборчої кампанії кандидата у президенти під час президентських виборів у США у 2016 році.

<sup>3</sup> [https://en.wikipedia.org/wiki/Podesta\\_emails](https://en.wikipedia.org/wiki/Podesta_emails)

## 2. Підвищення суспільної довіри й поінформованості, комунікації та веб-сайт організації

### Прозорість

Прозорість – це важливий принцип, що є запорукою проведення чесних виборів, а підтримка високого рівня довіри до виборчого процесу відповідає інтересам виборчих органів в цілому. Заходи кібербезпеки, які спрямовані на захист виборів, – це додатковий виклик для ОАВ: зазвичай буває досить важко визначитися з тим, яка інформація щодо заходів кібербезпеки має бути доступною для широкої громадськості, а яка має надаватися лише учасникам виборів або спостерігачам, лише членам комісії та лише IT-фахівцям із кібербезпеки, щоб забезпечити здоровий баланс між вимогами прозорості та необхідним рівнем конфіденційності.

### Стійкість веб-сайту

Окрім забезпечення прозорості, ОАВ повинні подбати також про те, щоби їхні зусилля з комунікацій із суспільством не були зведені нанівець через кібератаки на публічні веб-сайти ОАВ. Веб-сайти ОАВ зазвичай оновлюються та змінюються не надто часто, а отже швидко стають неактуальними, застарілими й незахищеними. Виборці в своєму повсякденному житті давно звикли до сучасних, функціональних і зручних для навігації веб-сайтів із багатим контентом, тож вони очікують такого ж стандарту для отримання інформації про вибори. Немає жодного способу запобігти потенційним DDoS-атакам – через відкриту природу Інтернету – але є способи послаблення пов'язаних із ними ризиків, наприклад, шляхом створення доступних для кінцевого користувача декількох потужних дзеркал або шляхом очищення трафіку через хмарний сервіс із високою пропускнуою здатністю.

### Стійкість комунікацій

Надзвичайно важливо, щоб ОАВ мав відкриті канали комунікацій із громадськістю, навіть коли веб-сайт стає об'єктом DDoS-атаки або його було зламано чи заблоковано. ОАВ повинні мати готові плани комунікацій для швидкого реагування у випадку найбільш передбачуваних інцидентів. Слід проводити тренування та «репетиції» виконання цих планів й переконатися, що всі учасники процесу чітко їх розуміють.

### Рекомендації для ЦВК:

Щодо прозорості, а також беручи до уваги проблемні питання, які виникли під час попередніх виборів, оновлена ЦВК має скористатися можливістю роз'яснити, яку інформацію можна оприлюднювати, а яку – ні. Загалом інформацію слід вважати непублічною, якщо у разі її оприлюднення зловмисники можуть використати її зі шкідливою метою.

Оскільки кібербезпека є питанням національної оборони, органи державної влади, які працюють у сфері безпеки, можуть на свій розсуд рекомендувати застосовувати більш строгий підхід до обмеження обміну інформацією з огляду на загрози, які виникають внаслідок витоку інформації через АРТ.



### ІДЕНТИФІКАЦІЯ І ЗБІР ДАНИХ:

- ▶ Створіть і згрупуйте разом плани комунікацій, в яких детально викладено протоколи комунікацій у кризових ситуаціях та повідомлення, які слід використовувати у разі атаки, оскільки, імовірно, що атака може статися в ході напруженого періоду виборів, коли час, необхідний для розробки таких протоколів або повідомлень, є дуже цінним і це може відвести увагу від інших критично важливих виборчих комунікацій.
- ▶ Створіть план комунікацій, орієнтований на успішну хакерську атаку на веб-сайт

для розміщення результатів виборів, у межах якого ЦВК може оприлюднити максимально можливу кількість інформації так, щоби це не вплинуло негативно на будь-яке розслідування інциденту або подальший захист системи.

- ▶ Перегляньте потреби відділу комунікацій ЦВК. Посильте їхні спроможності та необхідні ресурси для інформування учасників виборчого процесу про питання кібербезпеки.
- ▶ Постійно підтримуйте високі стандарти безпеки каналів зв'язку: систему управління наповненням сайту (CMS від англ. Content Management System), яка наразі використовується на веб-сайті, необхідно оновлювати за допомогою найновіших патчів; слід дотримуватися додаткових заходів обережності щодо запобігання зламу сторінок організації у соціальних медіа до та під час виборів.



### ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ І ВИПРОБУВАННЯ:



- ▶ Створіть платформу для обміну інформацією із зацікавленими сторонами, які працюють у сфері кібербезпеки та виборів.
- ▶ Проведіть тести на проникнення для веб-сайту ЦВК, веб-сайту ДРВ (джерело інформації для виборців) та для веб-сайту, на якому публікується інформація про результати виборів. У разі виявлення вразливостей усуньте їх та проведіть нові випробування.
- ▶ Підтримуйте свій веб-сайт за межами периметру вразливості, відокремлюйте його від інших. Веб-сайти ЦВК, ДРВ та веб-сайт для публікації результатів не повинні бути об'єднаними на єдиній платформі.
- ▶ Якщо це можливо і політично прийнятно, інституційні веб-сайти мають обслуговуватися спеціалізованими службами, які мають спеціальну групу безпеки й високий ступінь невразливості до DDoS-атак. У будь-якому разі ЦВК має готувати, оновлювати та регулярно перевіряти плани усунення наслідків DDoS-атак на всі веб-сайти, особливо в критично важливий період перед виборами.
- ▶ Змоделюйте ситуацію зі зломом веб-сайту ОАВ і продумайте, яким чином ОАВ має реагувати та усувати негативні наслідки інциденту. Комунікаційна стратегія на випадок інциденту, що є невід'ємною частиною комплексного плану відновлення, має бути чіткою, повідомлення – інформативними, а певні деталі необхідно зберегти в таємниці лише з метою захисту процесу розслідування або ж для уникнення небезпеки подальшої ескалації інциденту, якщо така небезпека насправді існує. Відділ комунікацій має мати всі необхідні можливості для обміну інформацією, а не отримувати окремий дозвіл на «розсекречення» кожної порції даних від керівництва ОАВ.



### АДАПТАЦІЯ:

- ▶ Посильте захист веб-сайту ЦВК та загальну спроможність ЦВК у сфері стратегічних комунікацій. Подбайте про те, щоб усередині ЦВК відділи ефективно взаємодіяли між собою, особливо відділ комунікацій та IT-відділ.
- ▶ Оцініть потенційні небезпеки приховування інформації від громадськості з міркувань безпеки; майте на увазі, що хакери могли вивчати систему ЦВК протягом декількох місяців і навряд чи поклалися в цьому на загальнодоступні дані.
- ▶ Інформуйте громадськість про резервне копіювання даних, про системи протидії кібератакам, а також про механізми аудиту введених даних для виявлення й виправлення помилок або зміни даних.
- ▶ Співпрацюйте із засобами масової інформації та НУО у сфері кібербезпеки й створюйте мережу прихильників, які матимуть можливість обмінюватися інформацією з ЦВК та громадськістю у випадку атаки, яка заблокує звичні канали комунікації.

- ▶ Перевірте власну стратегію зменшення потенційних ризиків за допомогою поширення інформації про вибори на місцевому рівні заздалегідь. Коли йдеться про результати виборів, це може бути реалізовано таким чином, що зацікавлені сторони (політичні партії, ЗМІ, групи спостерігачів за виборами та ін.) збирають результати виборів (сканкопії) на місцевому рівні. Їхні дані можна порівняти з офіційними опублікованими результатами, щоб переконатися у відсутності вторгнень до систем ЦВК. Це сприятиме підвищенню прозорості та стійкості виборчого процесу.

### Приклади вразливостей за параметрами:



**ТЕХНОЛОГІЧНІ:** ОАВ може вирішити залишити переважну більшість інформації про деталі системи таємною через побоювання, що розкриття інформації про елементи її архітектури буде грати на руку потенційним зловмисникам. Хоча такий підхід може бути цілком виправданим, він також призводить до виникнення певних проблем, адже «безпека через приховування» зазвичай не є ефективною практикою захисту. Через такий підхід ОАВ може вирішити, наприклад, не проводити тест-проникнення або ж не вдаватися до допомоги «білих хакерів», які можуть допомогти виявити вразливості, які насправді можуть використати зловмисники.



**КАДРОВІ/ЛЮДСЬКІ:** Є різні інструменти для створення веб-сайтів. Необхідно ретельно продумати вибір технології, слід керуватися міркуваннями безпеки, а не простоти конфігурації, та не надавати перевагу розробнику просто тому, що він вам знайомий. Працівники відділу комунікацій повинні бути дуже обережними у використанні цифрових пристроїв. Не слід мати доступ до всіх облікових записів з одного пристрою (Twitter, YouTube, Facebook та адміністрування веб-сайту), оскільки в разі викрадення та зламу цього пристрою ОАВ втратить контроль над усіма своїми каналами комунікації із громадськістю через лише єдину хакерську атаку.



**ПОЛІТИЧНІ:** IT-відділи ОАВ зазвичай приховують інформацію про те, які заходи кібербезпеки вони використовують та який ризик є для них прийнятним, щоб запобігти витоку даних про наявні вразливості. У більшості випадків аналітики, спостерігачі та інші зацікавлені сторони у виборчому процесі не матимуть можливостей проаналізувати будь-яку наявну документацію. Попри аргументи ОАВ щодо недоцільності розкриття внутрішньої інформації про наявні ризики, така заборона розголошення інформації не повинна поширюватися на параметри функціонування виборчих систем (наприклад, СВРВ або систему виборчих списків), якими цікавляться учасники виборчого процесу, маючи на те всі законні права. Політичний ризик, який виникає внаслідок розголошення інформації про здійснення успішної атаки на веб-сайт ОАВ, може також викликати обґрунтовані претензії (або безвідповідальні спекуляції з цього приводу) учасників виборчих процесів щодо здатності ОАВ забезпечити вибори від зовнішніх маніпуляцій.



**ПРАВОВІ:** Якщо виборче законодавство та/або будь-які закони, що регулюють кібербезпеку критичної інфраструктури, не містять чіткого визначення, які саме компоненти й документація повинні бути доступними та за яких обставин, ОАВ може просто занадто перестрахуватися й закрити доступ громадськості до більшості інформації, яка так чи інакше стосується кібербезпеки. Злам веб-сайту ОАВ зазвичай не означає ризику підміни справжніх даних, адже дані, які розміщені на веб-сайті, завжди є лише копією основних баз даних, розміщених деінде. Завжди є основні резервні копії тих даних, які були розмішені на сторінці. Однак у деяких випадках таке хакерське вторгнення може поставити під загрозу збереження конфіденційних даних виборців і таким чином може поставити під загрозу

можливість виконання закону про захист персональних даних, наприклад, у разі несанкціонованого доступу до інформації на веб-сайті, де розміщено інформацію про реєстрацію виборців.



**ПРОЦЕДУРНІ:** Наразі, коли кіберзагрози можуть викликати цілком виправдані сумніви в легітимності виборів, ОАВ повинні виходити за межі базової інформаційно-просвітницької кампанії серед виборців (як-от плакати, що заохочують до участі в голосуванні, відео, розміщені в Інтернеті та ін.). Ті ОАВ, які не готові надавати громадськості більше інформації, підсилюють недовіру до виборчого процесу загалом. Наприклад, якщо, ставши жертвою успішної кібератаки, ОАВ намагатиметься будь-якою ціною приховати сам факт атаки, щоб уникнути незручного становища або через хибну думку, що нерозголошення інформації відповідає національним інтересам, це може лише викликати страх, невпевненість і сумніви щодо легітимності виборчого процесу в суспільстві.

### 3. Стійкість до шкідливого програмного забезпечення, регулярне оновлення апаратного й програмного забезпечення

Шкідливе програмне забезпечення – це головний інструмент АРТ при проникненні в захищені мережі. Зловмисники намагаються впровадити функціональну частину вірусу, або payload (функціональна частина вірусу, або payload, – компонент комп’ютерного вірусу, який виконує шкідливу дію) та сховати його десь у системі. Під час реалізації атаки типу АРТ у промислових та комерційних системах хакери намагаються зберегти присутність шкідливого програмного забезпечення в цих системах упродовж тривалого часу з метою шпигунства та незаконного збору інформації. Однак, якщо хакерам вдається інсталиювати деструктивний програмний продукт в мережі ОАВ, вони, ймовірно, зможуть активувати його у той час, коли він буде здатний завдати найбільшої шкоди (наприклад, спробувати змінити результати виборів в Інтернеті, щоб вони не відповідали «паперовому сліду»).

Нове та інноваційне шкідливе програмне забезпечення створюється постійно, адже механізми виявлення та протидії такому програмному забезпеченню також постійно еволюціонують. Якщо організація зіткнулася з винахідливим супротивником, наприклад АРТ-кібезлочинцями, цілком імовірно, що вони вже знають, яке антивірусне програмне забезпечення використовується в цій організації; якщо шкідливе програмне забезпечення не є надто інноваційним, його може виявити будь-яке звичайне антивірусне програмне забезпечення під час рутинної перевірки.

Стійкість ОАВ щодо АРТ буде залежати від здатності відповідної організації підтримувати сучасне та здорове середовище як для апаратного, так і програмного забезпечення.

#### Рекомендації для ЦВК



##### ІДЕНТИФІКАЦІЯ І ЗБІР ДАНИХ:

- ▶ Періодично переглядайте архітектуру системи для виявлення застарілого програмного або апаратного забезпечення, яке необхідно замінити або оновити.
- ▶ Проводьте ретельні тести-проникнення як для СВРВ, так і потенційно для ДРВ перед кожними виборами. Розгляньте можливість проведення перевірки журналів активності з метою виявлення попередньо не помічених втручань у систему.



##### ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ:

- ▶ Періодично перевіряйте, які пристрої підключено до мережі та від’єднуйте всі нерозпізані пристрої.
- ▶ Виконайте перевірку та переконайтеся, що на жодному комп’ютері в організації не використовується неліцензійне програмне забезпечення.



##### ВИПРОБУВАННЯ:

- ▶ Працівники ІТ-відділу ОАВ повинні постійно вдосконалювати свої професійні знання та бути попереду трендів. Період між виборами – чудовий час для цього. IFES наразі співпрацює з ЦВК із метою забезпечити проведення навчання з кібербезпеки за поглибленою програмою, що не залежить від конкретного апаратного та програмного забезпечення.



##### АДАПТАЦІЯ:

- ▶ Плануйте будь-які суттєві зміни в системі, пов’язані з впровадженням нових апаратних засобів та програмного забезпечення задовго до виборів.
- ▶ Регулярно проводьте сегментацію мережі, так, щоб найбільш чутливі мережі не були доступні через Інтернет. Обов’язковою вимогою є розмежування (air-gapping, або фізичне розділення) найбільш чутливого обладнання, наприклад, серверу баз даних списків виборців або серверу СВРВ.
- ▶ Розгляньте можливість використання надійно захищених віртуальних систем на комп’ютерах, які підключено до критично важливої мережі. Надійно захищені віртуальні системи – це спеціально сконфігуровані версії ОС, що забезпечують захист від кіберзагроз.

#### Приклади вразливостей за параметрами:



**ТЕХНОЛОГІЧНІ:** Неможливість застосувати найновіші патчі з останніми оновленнями від постачальника обладнання/програмного забезпечення, необхідні для безпеки, призводить до виникнення технологічної вразливості, якою можуть скористатися зловмисники. Незважаючи на те, що основні проблеми можуть виникати через особливості людської поведінки, вони також можуть бути пов’язані з організаційними чи політичними проблемами, які фахівці з інформаційних технологій не можуть вирішити, наприклад, небажання керівництва виділяти ресурси на оновлення ОС, коли це необхідно. ОАВ, які зазвичай працюють в умовах недостатніх ресурсів або негнучких бюджетів, особливо часто стикаються з цією проблемою.

Якщо інформаційний потік не контролюється, він може потрапити під загрозу: будь-яка точка доступу до Інтернету або загалом доступ до будь-чого поза межами захищеного периметра, – це потенційна точка інфільтрації шкідливих програм. З погляду кібербезпеки, точки доступу, які не контролюються або не підпорядковуються ІТ-відділу ОАВ, є особливо вразливими. Слід уважно стежити та постійно перевіряти найбільш поширені канали проникнення в систему, зокрема електронну пошту та веб-доступ, а також зовнішні носії, наприклад USB-накопичувачі.



**КАДРОВІ/ЛЮДСЬКІ:** Застаріле та невиправлене (без патчів) апаратне та програмне забезпечення призводить до виникнення технологічних вразливостей. Проте важливо, щоб ІТ-відділи пильно стежили за появою нових вразливостей, які можуть становити загрозу для цілісності системи. Працівники ІТ-відділу ОАВ повинні оцінювати нові загрози з метою визначити, відбулося чи не відбулося пошкодження апаратного забезпечення, а також ліквідувати ці проблемні місця за допомогою патчів, у разі необхідності.



**ПОЛІТИЧНІ:** Навіть якщо ІТ-персонал усвідомлює весь спектр загроз, передача цієї інформації керівництву ОАВ може виявитися непростим завданням. Незалежно від розміру, з огляду на критично важливий характер виборів, ОАВ має виходити з припущення, що винахідливі супротивники будуть зацікавлені в розміщенні ретельно розробленого шкідливого програмного забезпечення у внутрішніх комп’ютерних мережах ОАВ.

## 4. Розбудова людського потенціалу, проблеми збереження й підготовки ключового персоналу

Незважаючи на те, що придбання апаратного забезпечення та налаштування необхідних конфігурацій систем безпеки вимагає значних часових і фінансових ресурсів, найбільш важливим є підвищення людського потенціалу. ОАВ зазвичай мають той самий рівень заробітної плати, що й інші державні установи, часто не конкурентний із рівнем заробітних плат у приватному секторі. Утримання висококваліфікованих кадрів – це велика проблема в багатьох країнах, і Україна не є винятком.

ІТ-спеціалісти мають розуміти, як працюють системи, що використовуються для захисту роботи інфраструктури, інакше ці системи не будуть ефективними для захисту від АРТ. Окрім того, ОАВ зазвичай не мають достатньо можливостей, щоб самостійно реагувати на загрози, тож для багатьох країн звичною є практика залучення зовнішніх підрядників або груп реагування на надзвичайні ситуації у комп'ютерній мережі типу CERT.

### Рекомендації для ЦВК:



#### АДАПТАЦІЯ:

- ▶ Спробуйте отримати спеціальний дозвіл від агентства з питань державної служби на оплату праці експертів із кібербезпеки та фахівців у галузі ІТ на рівні, вищому за рівень оплати праці в державному секторі.
- ▶ Стимулюйте утримання працівників за допомогою довгострокових навчальних програм.
- ▶ Працевлашуйте стажерів та молодих фахівців і пропонуйте довгострокові кар'єрні можливості для запобігання плинності кадрів.
- ▶ Перегляньте чинні практики працевлаштування задля посилення залучення персоналу з найвищим рівнем кваліфікації: фахівці з кібербезпеки в ОАВ повинні мати відповідну підготовку та освіту та/або відповідний досвід у галузі безпеки ІТ-систем.

### Приклади вразливостей за параметрами:



**КАДРОВІ/ЛЮДСЬКІ:** Деякі ОАВ можуть зіткнутися із серйозною проблемою утримання кваліфікованих ІТ-спеціалістів, адже у цій сфері спостерігається висока плинність кадрів. Ця проблема також посилюється тим, що більшість ОАВ не мають у своєму штаті фахівців із кібербезпеки, натомість покладаються на звичайних ІТ-фахівців у питаннях захисту від кіберзагроз.



**ПОЛІТИЧНІ:** Проблема потенційно неадекватної компенсації за роботу ІТ-спеціалістів ОАВ зазвичай пов'язана з проблемою низького рівня заробітної плати для ІТ-фахівців на державній службі в цілому, оскільки ОАВ є частиною державної структури. Тому вирішення цієї проблеми означає перегляд заробітної плати для працівників ІТ-служб та служб кібербезпеки у державному секторі або ж звернення з проханням про надання ОАВ виняткового права оплачувати працю фахівців у галузі кібербезпеки/ІТ за більш конкурентними тарифами.

## 5. Журнали моніторингу та роботи системи, важливість журналів діяльності («сліду») для кібераудиту

Контрольні журнали діяльності, або «слід» для кібераудиту, – це журнали, в яких фіксуються записи про діяльність у системі, що була ініційована через системні або прикладні процеси або через вхід користувачів до систем та додатків. У поєднанні з відповідними інструментами та процедурами контрольні журнали діяльності, або «сліди» для кібераудиту, можуть допомогти виявити порушення безпеки, проблеми з продуктивністю та недоліки у програмах.

Контрольні журнали діяльності, або «сліди» для кібераудиту, є незамінним інструментом для захисту цілісності мережі та виборів у цілому.

Наприклад, такий «слід» може допомогти реконструювати події, виявити втручання та проаналізувати такі проблеми, як низька продуктивність або неочікувана поведінка системи. Це також може сприяти належній поведінці та посиленню почуття відповідальності серед користувачів, якщо вони знатимуть, що їхні дії можна відстежити.

Питання моніторингу системи та мереж є не лише технічним. ІТ-відділ має налаштувати всі компоненти для реєстрації подій та трафіку, але також забезпечити ресурси для аналізу великої кількості новостворених даних у контрольних журналах діяльності.

### Рекомендації для ЦВК:



#### ІДЕНТИФІКАЦІЯ І ЗБІР ДАНИХ:

- ▶ Подбайте про те, щоб налагодити належним чином процес моніторингу всіх подій у системах та в мережах в межах SIEM (від англ. Security Information and Event Management — управління інформацією та подіями з безпеки). Періодично переглядайте всі процедури, політики та конфігурації, щоб переконаватися, що вони дозволяють зафіксувати всю інформацію, необхідну для комплексного аналізу кібербезпеки.



#### АДАПТАЦІЯ:

- ▶ Створіть протоколи, в яких детально описано, як реагувати на кожний тип критичних подій, які виявлено в системі. Дії з ліквідації проблеми або подальшого відновлення системи є настільки ж важливими, як і виявлення проблеми.
- ▶ Подбайте про те, щоб система фіксації даних та їхнього аналізу була протестована заздалегідь до виборів. Це дозволить адміністраторам побачити, як система працює в нормальних умовах та допоможе їм вчасно виявити потенційну аномалію.
- ▶ Систему управління подіями інформаційної безпеки слід використовувати комплексно, якщо це можливо, для реєстрації подій у мережі ДРВ, у мережі СВРВ та у внутрішній мережі ЦВК.
- ▶ Інсайдерським атакам можна запобігати опосередковано, але ефективно, через провадження ретельного моніторингу мережі та аналізу записів у контрольних журналах діяльності.

## Приклади вразливостей за параметрами:



**ТЕХНОЛОГІЧНІ:** Незалежно від кількості рівнів захисту критичної мережевої та серверної інфраструктури, ОАВ мають виявляти інциденти та реагувати на них, з'ясовуючи, чи йдеться про порушення кібербезпеки, чи про несправність апаратного забезпечення. Без контрольних журналів діяльності, або «сліду» для кібераудиту, ОАВ не можуть локалізувати та встановити походження проблеми.



**КАДРОВІ/ЛЮДСЬКІ:** Працівники ОАВ повинні повною мірою усвідомлювати, що зниження кібербезпекових ризиків та управління вразливістю потребують різних навичок: від вміння створити мережу для введення даних про результати до розробки бази даних реєстру виборців. IT-відділ ОАВ має або мати персонал, який, окрім інших навичок, обізнаний щодо провідних практик у галузі кібербезпеки, або найняти відповідних спеціалістів. Якщо працівники ОАВ не ознайомлені зі складними механізмами контролю над їхніми системами, це суттєво зменшує стійкість ОАВ до кібератак.



**ПРАВОВІ І ПРОЦЕДУРНІ:** Контрольні журнали діяльності, або «слід» для кібераудиту, необхідно захистити від зловмисників, які бажали би їх змінити, адже метою ведення таких журналів діяльності є запобігти незаконним діям та забезпечити існування відповідної системи стримування та протипаг. «Слід» для кібераудиту має важливе значення для ОАВ: його використовують, щоб довести, що відбувається і що не відбувається в периметрі безпеки, а отже, переконатися, що жодний критично важливий виборчий процес не зазнав несанкціонованого впливу. Такий «слід» може бути й вже був доказом при доведенні втручання в мережу в судових справах, пов'язаних із виборами.

## 6. Важливість політик у галузі кібербезпеки, стандартних операційних процедур і кодексу поведінки в галузі IT

Політика з кібербезпеки, перш за все, передбачає інформацію для операторів/виконавців щодо їхніх обов'язків із захисту технологічних та інформаційних активів ОАВ. Ці політики мають описувати засоби контролю та провідні практики, якими мають керуватися оператори/виконавці під час проведення виборчих операцій.

Компанії, особливо такі, що працюють у чітко законодавчо та процедурно врегульованих середовищах, наприклад, компанії фінансового сектора, вже давно запровадили певну політику та жорсткі операційні процедури для своїх працівників. Багато ОАВ мають, наприклад, чіткі процедури щодо процесу підрахунку голосів, але часто не мають настільки суворих процедур щодо управління даними та належного використання технологій. Жоден ОАВ наразі не може дозволити собі ігнорувати цю слабку ланку в системі.

Розробка програмного забезпечення є невід'ємною частиною стандартних операційних процедур, важливість якої не можна недооцінювати. Запровадження суворого контролю ланцюжка поставок і правил закупівель або ж протоколів для перевірки походження початкового коду під час встановлення нової версії програмного забезпечення допоможе переконатися в контролі й над цим процесом також.

### Рекомендації для ЦВК:



#### ІДЕНТИФІКАЦІЯ І ЗБІР ДАНИХ:

- ▶ Запровадьте стратегію кібербезпеки та систему зменшення ризиків на основі законодавства держави або міжнародно визнаних стандартів кібербезпеки, наприклад, стандартів кібербезпеки Національного Інституту стандартів та технологій (NIST) або з сім'ї ISO 27K.
- ▶ Запровадьте формалізовану систему моделювання загроз та управління ризиками при проектуванні та впровадженні системи, яка дозволить детально розглянути всі припущення щодо безпеки, а також плани дій щодо реагування та відновлення.
- ▶ Розробіть та попросіть працівників підписати кодекс поведінки, що визначатиме прийнятні стандарти використання професійних платформ та соціальних медіа. Працівники ЦВК та ОВК повинні утримуватися від активності в соціальних медіа протягом робочого часу в період виборів. Під час виконання службових обов'язків персонал не повинен «реєструватися» або ж поширювати інформацію про власне місцезнаходження або маршрути пересування.



#### ВИПРОБУВАННЯ:

- ▶ Періодично переглядайте та порівнюйте знімки даних, переглядайте кількість та тип змін у ДРВ для забезпечення цілісності даних. Докладайте до знімків даних звіти про діяльність у системі, які показують усі оновлення реєстру, забезпечуючи всі дані для повної перевірки усіх дій щодо внесення змін.
- ▶ Проводьте внутрішню і зовнішню перевірку початкових кодів після впровадження будь-яких змін (особливо значних змін) до системи ДРВ.
- ▶ Зробіть можливим створення різних версій початкового коду та подбайте про те, щоб можна було відслідковувати всі зміни за автором і датою модифікації.
- ▶ Обмежте весь доступ до бази даних із систем, що мають доступ до Інтернету, за

допомогою дотримання ретельно продуманих процедур збереження (SP) із використанням мінімально необхідної авторизації.



### АДАПТАЦІЯ:

- ▶ Розгляньте можливість виконання систематичної перевірки всіх процедур кібербезпеки за допомогою внутрішніх та потенційно зовнішніх процедур аудиту (щоб уникнути конфлікту інтересів під час розгортання та аудиту системи).
- ▶ Перегляньте плани створення резервних копій та відновлення ДРВ у разі виникнення аварійних ситуацій. Створіть системи, що дублюють одна одну, навіть на спрощеному апаратному забезпеченні, щоб мати можливість перехопити керування в разі відмови під час атаки або збою в основній системі.
- ▶ Створіть і протестуйте систему та план відновлення даних у разі їхньої втрати – це має бути запроваджено як політика в межах організації та інституційне зобов'язання.

### Приклади вразливостей за параметрами:



**КАДРОВІ/ЛЮДСЬКІ:** Чіткі процедури та політики гарантують, що співробітники ОАВ знатимуть, чого від них очікують. Наприклад, IT-відділ мусить мати чіткі інструкції, що не можна запускати в роботу жоден код, який не було перевірено належним чином.

За відсутності чіткого кодексу поведінки навіть відвідування певної конференції представниками ОАВ може бути використане як інструмент розвідки для подальшої розсилки спір-фішингового листа. Будь-яка реєстрація (зазначення геолокації) у місці, пов'язаному з діяльністю ОАВ під час виборів, може спричинити цілеспрямовані атаки на об'єкт із боку зловмисника, який прагне зірвати виборчі операції.

## 7. Міжвідомча взаємодія, створення команди реагування на кризові ситуації на виборах

Міжвідомча взаємодія є важливою складовою для підвищення рівня кіберзахисту кожної із залучених установ. Така взаємодія є цілком природним заходом, до якого вдаються урядові установи, проте ОАВ водночас мають при цьому подбати про збереження власної незалежності. Кібербезпека є однією з галузей, що потребують подібної співпраці, адже йдеться про питання національної безпеки і ОАВ зазвичай не мають достатньо ресурсів і забезпечення для того, щоб протистояти особливо складним загрозам самостійно.

ОАВ також мають регулярно співпрацювати з іншими учасниками виборчих процесів, зокрема політичними партіями, щоб виробити загальне розуміння важливих питань, пов'язаних із цілісністю виборчого процесу, що допоможе уникнути зайвих спекуляцій, які зазвичай виникають з огляду на брак інформації.

Розширення співпраці з НУО та засобами масової інформації – це ще один крок, до якого мають вдатися ОАВ, щоби покращити прозорість виборів, тим більше, що в багатьох країнах НУО, які займаються питаннями виборів, виявляють підвищений інтерес до кібербезпеки.

### Рекомендації для ЦВК:



#### ІДЕНТИФІКАЦІЯ І ЗБІР ДАНИХ:

- ▶ Подбайте про те, щоб співпраця з урядовими установами, зокрема Держспецзв'язком та СБУ, була формалізованою, публічною та прозорою, щоб підтримувати впевненість громадськості в незалежності ЦВК. Повноваження кожного члена групи CERT, яких залучено до виборів, повинні бути чітко зрозумілі для всіх зацікавлених сторін.



#### ВІЯВЛЕННЯ ВРАЗЛИВОСТЕЙ І ВИПРОБУВАННЯ:

- ▶ Міжвідомчу взаємодію необхідно ретельно обдумати та вписати у більш широкий контекст плану забезпечення безперервності операцій, якщо такий план існує, або аналогічного плану заходів із кібербезпеки. Спираючись на цей план, міжвідомча робоча група має швидко реагувати й вживати відповідних заходів, які стануть належною відповіддю на кризову ситуацію у сфері кібербезпеки.



#### АДАПТАЦІЯ:

- ▶ Вимагайте періодичного перегляду рівня захисту наявних систем та моніторингу будь-яких пов'язаних із ними ризиків для відповідних установ, враховуючи залежність від зовнішніх мереж для передачі інформації, пов'язаної з виборами, зокрема даних реєстру виборців.
- ▶ Співпрацюйте з Держспецзв'язком, щоб отримати достатні ресурси для виконання ретельних тестів-проникнень з огляду на характер АРТ. Вимагайте проведення тестів-проникнень на ранніх стадіях, щоб забезпечити можливість зниження рівня ризиків від нововиявлених вразливостей, а також, якщо буде потреба, повторіть ці тести.

## Приклади вразливостей за параметрами:



**ТЕХНОЛОГІЧНІ:** У взаємодії команди ОАВ зі спеціалістами CERT однаково важливими є як співпраця та комунікація, так й інформація з системних та мережевих датчиків моніторингу. Недостатня співпраця на робочому рівні з використанням усталених процедур обміну інформацією може призвести до неефективності та існування невиявлених загроз.



**КАДРОВІ/ЛЮДСЬКІ І ПОЛІТИЧНІ:** Якщо вжиті спільні зусилля слугують лише бюрократичним цілям і не мають практичної цінності, ОАВ взагалі не отримає переваг від такої співпраці. Навпаки, така обмежена або слабка співпраця може завадити ОАВ у пошуках важливої технічної допомоги з інших джерел та призвести до того, що вони будуть змушені взяти на себе відповідальність за неліквідовані вразливості.



**ПРАВОВІ:** Як реальна, так і позірنا незалежність ОАВ від втручання з боку урядових установ може мати значний вплив на впевненість виборців у тому, що вибори проводяться на рівних для всіх умовах. Якщо характер співпраці з урядовими установами не є обґрунтованим та прозорим, це може перешкоджати спроможності ОАВ як незалежної виборчої комісії адмініструвати вибори. Потрібно уникати ситуації, коли міжвідомча співпраця призводить до реального або уявного конфлікту інтересів, в якому Секретаріат ОАВ сприймається як продовження уряду, а не як структура, що є підзвітною незалежному ОАВ.



**ПРОЦЕДУРНІ:** ОАВ можуть взаємодіяти з урядовими установами в робочому порядку, проте в деяких випадках немає процедури, яка би визначала найкращі шляхи для такої взаємодії, особливо якщо йдеться про реагування на інцидент у сфері кібербезпеки. Внаслідок цього можливі імпровізації або хаотичні поспішні рішення, що будуть затверджуватися протягом достатньо напруженого виборчого періоду.

## 8. Доступ до цифрової інфраструктури

Обладнання без належного нагляду або недостатньо захищене обладнання є чудовою цілью для зловмисника.

Одна з кращих практик полягає в тому, щоби переконатися, що всі комп'ютери блокуються після відносно короткого періоду бездіяльності, а також чітко визначити, хто нестиме особисту відповідальність за кожний критично важливий компонент обладнання.

### Рекомендації для ЦВК:



#### ІДЕНТИФІКАЦІЯ І ЗБІР ДАНИХ:

- ▶ Увесь доступ до найбільш чутливого обладнання, як-то сервербази даних реєстру виборців, необхідно реєструвати двічі, тобто електронним способом і на папері. Доступ до зовнішніх портів серверів і робочих станцій, що використовуються для підключення до критично важливих систем, має бути суворо заборонений.
- ▶ Визначте, хто має право доступу до відповідного обладнання. Наприклад, позбавте доступу колишніх працівників, як тільки вони полишають службу.
- ▶ За допомогою перегляду структури системи та періодичних перевірок подбайте про те, щоб усі критично важливі компоненти та внутрішні мережі виборчих систем були сегментовані або відокремлені (фізично ізольовані) від решти мереж та Інтернету. Комп'ютери, які використовують для обробки електронних листів та загальної мережевої навігації, не мають жодним чином бути під'єднані до мережі, де зберігаються конфіденційні дані про вибори.



#### ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ І ВИПРОБУВАННЯ:

- ▶ Ознайомте керівництво з процедурами доступу. Керівництво має переглянути та схвалити їх. Для ЦВК було би доцільним розглянути офіційне оформлення цих процедур та прийняти рішення про те, чи варто викласти їх лише у внутрішньому документі, залежно від рівня деталізації описів у такій документації.



#### АДАПТАЦІЯ:

- ▶ Не надавайте повний доступ до серверів та конфігурацій інших пристроїв лише одній особі, завжди робіть це парно з метою забезпечити перехресні перевірки безпеки.
- ▶ Встановіть систему відеоспостереження над точками входу/виходу в тому місці, де розташована чутлива апаратура. Проте уникайте наведення камер на термінали, підключені до серверів, із метою уникнення можливості зйомки введення облікових записів для входу в систему.
- ▶ Застосовуйте підхід дуже обмеженого доступу: фізичний доступ до вразливої апаратури необхідно узгоджувати та/або дозволяти лише за особливих обставин, що підлягають контролю. Проте слід обов'язково передбачити можливість вільного доступу для зареєстрованих спостерігачів та аудиторів протягом періоду виборів, щоб вони могли переконатися в застосуванні необхідних заходів безпеки.
- ▶ Подбайте про відключення бездротового з'єднання на системному рівні на будь-якому об'єкті критичної виборчої системи, яка його не потребує. Усі фізичні порти та термінали, підключені до серверів, необхідно опломбувати, а фізичне з'єднання з будь-якими пристроями має виконуватися лише з дуже вагомих причин і бути задокументовано.

## Приклади вразливостей за параметрами:



**ТЕХНОЛОГІЧНІ:** Критично важливе обладнання може опинитися під загрозою навіть із боку ІТ-фахівців, які вважаються довіреними співробітниками. Загроза може бути пов'язана з тим, як саме отримують доступ до серверів та якою є динаміка доступу до серверів у спеціально захищеному середовищі. Загроза також може бути пов'язана з набагато простішою, але потенційно фатальною помилкою, коли незаблокований ноутбук залишають без нагляду. Ніколи не слід надавати доступ до критично важливих мереж через бездротові з'єднання. На всіх критично важливих пристроях слід використовувати опечатувальні стрічки для контролю незаконного проникнення, що наліплюються на USB та інші порти з метою попередити навмисне або випадкове завантаження до системи шкідливого програмного забезпечення.



**КАДРОВІ/ЛЮДСЬКІ:** Вхід до серверної кімнати слід розглядати як потенційне порушення безпеки. Небезпека атаки зсередини організації в Україні є значною і може мати вигляд несанкціонованого доступу до робочих станцій, приватних комп'ютерів, маршрутизаторів та серверів даних. У разі внутрішньої атаки, наприклад завантаження шкідливого програмного забезпечення через незареєстрований доступ до робочої станції, колеги без нагляду є одним із можливих способів атаки, який не потребує від інсайдера спеціальних знань з інформаційних технологій.



**ПОЛІТИЧНІ:** Надмірна залежність від зовнішніх організацій, які не несуть безпосередньої відповідальності за виборчий процес, зокрема від постачальників, підрядників чи навіть урядових установ, може стати причиною додаткової кадрової вразливості та потенційних порушень безпеки.



**ПРОЦЕДУРНІ:** У разі відсутності відповідних інструкцій щодо доступу, політика розширеного доступу, наприклад, у період між виборами, коли менше уваги приділяється питанням безпеки, потенційно може призвести до виникнення додаткової кадрової та технічної вразливості.

## 9. Привілейовані права доступу й неадекватний контроль

Лише фізичного доступу зазвичай недостатньо для того, щоб втрутитися в роботу системи через термінал. Проте за наявності з'єднання більшість комп'ютерів можна атакувати віддалено. Правильним припущенням кібербезпеки є таке: якщо комп'ютер фізично не від'єднано від мережі, теоретично, доступ до нього можна отримати віддалено, незалежно від будь-яких заяв, що заперечують подібну ймовірність.

Великі організації загалом запроваджують ретельне управління системою ідентифікації та доступу (IAM, від *англ.* Identity and Access Management). Наприклад, голова ОАВ може попросити ІТ-адміністратора надати їй права адміністрування на ноутбуці, щоб вона могла вільно та конфіденційно встановлювати програмне забезпечення, яке вона забажає. Це може бути зручно для голови особисто, але, безумовно, не є доцільним з погляду кібербезпеки. ІТ-адміністраторові (який в ОАВ невеликого розміру може також виконувати функції спеціаліста з кібербезпеки) може бути важко відмовити голові, проте виконавши подібне прохання, він вже більше не буде знати, яке саме програмне забезпечення встановлено на її ноутбуці.

Важливо, щоб усі користувачі дотримувалися встановлених правил. Безпека будь-якої системи є настільки міцною, наскільки міцна її найслабша ланка, і це також стосується кібербезпеки виборчих систем.

### Рекомендації для ЦВК:



#### ІДЕНТИФІКАЦІЯ І ЗБІР ДАНИХ:

- ▶ Періодично переглядайте політику доступу для всіх працівників. Розгляньте правила доступу учасників виборчого процесу до даних про вибори: слід знати, чи користувачі, особливо працівники ОАВ, розуміють, що і де знаходиться в системі, а також що є прийнятним використанням інформації, а що ні.
- ▶ Перегляньте політику щодо доступу через бек-енд до реальних даних, пов'язаних із виборами, як для ДРВ, так і для СВРВ, щоб гарантувати, що неправильні оновлення та несанкціоновані зміни не робляться випадково чи навмисно.



#### ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ І ВИПРОБУВАННЯ:

- ▶ Перевіряйте, чи політики застосовуються насправді: наприклад, перевіряйте час від часу, чи неактивні облікові записи було деактивовано, чи оновлення системи взаємозв'язування компонентів потребує перевірки за білим (або чорним) списком.
- ▶ Чітко розподіліть відповідальність і складіть робочий план, який визначає процедури безпеки, наприклад, стосовно доступу до серверів. Це надзвичайно важливо для зниження рівня ризику інсайдерської атаки.



#### АДАПТАЦІЯ:



- ▶ Підтримуйте розмежування обов'язків між системними адміністраторами, які налаштовують ОС та встановлюють необхідне програмне забезпечення, і адміністраторами безпеки, які переглядають зміни у файлах та журналах конфігурації і не мають доступу та права обробляти будь-які чутливі (виборчі) дані. У будь-якому разі необхідно суворо обмежити кількість спеціалістів з інформаційних технологій, які мають право доступу адміністратора до основних компонентів системи.

- ▶ Розгляньте питання про залучення аудитора захисту доступу, як на тимчасовій, так і на постійній основі, з метою виконання періодичних перевірок, виявлення слабких місць та забезпечення реалізації політики у сфері контролю доступу.
- ▶ Розгляньте можливість додаткової перевірки персоналу для доступу до конфіденційної інформації, коли і якщо це можливо.

### Приклади вразливостей за параметрами:



**ТЕХНОЛОГІЧНІ:** Вибір ОС може визначати певні аспекти того, як надаються права доступу. Усі сучасні ОС мають складні інструменти для управління правами користувачів, але адміністратори мають добре знатися на можливих наслідках різних конфігурацій, щоб забезпечити належний функціональний доступ, одночасно запобігаючи наданню повноважень, які користувачам не потрібні. Наприклад, немає жодних підстав для того, щоб один із членів ЦВК мав привілейований доступ до бази даних реєстру виборців. З іншого боку, причини, з яких член ЦВК хотів би мати такий доступ, можуть викликати підозри в тому, наприклад, що він бажає скопіювати базу даних реєстру виборців та винести її за межі контрольованого середовища для отримання політичних переваг.



**КАДРОВІ/ЛЮДСЬКІ:** Брак підготовки адміністраторів з управління правами користувача, як у відповідних ОС, так і в ОС-нейтральних ситуаціях, може значно підвищити рівень технологічних вразливостей. Керівництво організації може бути надто слабким і дозволити нівелювання політики прав доступу виключно тому, що так зручно користувачам.

Створення неперсоналізованих облікових записів користувачів може зменшити відповідальність індивідуальних користувачів виборчих систем. Як правило, такого підходу слід уникати. Іншими словами, слід мати можливість відстежити будь-який випадок зареєстрованого доступу і атрибутувати його до конкретного користувача.



**ПОЛІТИЧНІ І ПРАВОВІ:** Жорстка політика щодо надання права доступу може призвести до зменшення прозорості виборів у випадку, якщо така політика не буде добре зважена. Наприклад, адміністратори мають дослідити, які дії можливо виконувати в системі без потреби ідентифікації користувачів. Відсутність доступу учасників виборчого процесу, як-от політичних партій та громадянського суспільства, до даних, які не є конфіденційними, може зменшити підзвітність та прозорість ОАВ. Водночас загальнодоступні системи та системи обмеженого доступу повинні бути ізольовані одна від одної, щоб виключити можливість випадкового доступу неавторизованих користувачів до конфіденційної інформації.



**ПРОЦЕДУРНІ:** Брак процедур для надання прав доступу може призвести до плутанини та хиткого організаційного підходу. Відсутність всеохопної документації, в якій детально описано привілейований доступ, може призвести до виникнення прихованих проблем. Весь персонал необхідно письмово поінформувати щодо процедур надання прав доступу та підтвердити ознайомлення й усвідомлення цієї політики.

## 10. Фізичний захист цифрової інфраструктури

Україна зіткнулася із супротивником, який вдається до всіх методів ведення гібридної війни та не цурається жодних засобів агресії. Фізичні атаки на інфраструктуру можуть використовуватися для того, щоб посягти страх, непокору й створити плутанину, а також із метою знищення IT-інфраструктури.

### Рекомендації для ЦВК:



#### ІДЕНТИФІКАЦІЯ І ЗБІР ДАНИХ:

- ▶ Проведіть координаційні та/або робочі зустрічі з державними/місцевими органами, які мають юридичні повноваження для забезпечення фізичної безпеки. Оцініть, чи достатня увага приділяється захисту цифрових активів.
- ▶ Перевірте планування периметрів фізичної безпеки та з'ясуйте розклад змін охоронців і плани посилення заходів безпеки під час виборів.
- ▶ Дослідіть історію попередніх інцидентів у сфері безпеки, встановіть деталі таких інцидентів: мета, жертви та зловмисники, обсяги шкоди.
- ▶ Складіть список критично важливого обладнання та матеріалів, визначте потенційних постачальників обладнання та послуг, які можуть негайно надавати підтримку у випадку надзвичайних ситуацій.
- ▶ Оцініть та опишіть потенційну шкоду, якої можна завдати виборчим процесам у випадку фізичного саботажу; при цьому використовуйте календар виборів, послідовність робочого процесу та схеми периметрів безпеки.



#### ВІЯВЛЕННЯ ВРАЗЛИВОСТЕЙ І ВИПРОБУВАННЯ:

- ▶ Встановіть, які ризики фізичної безпеки є прийнятними, та виконайте повторну оцінку необхідності їхнього зниження.
- ▶ Знайдіть головні точки вразливості та перелічіть їх. Перевірте, чи є якісь організаційні моменти щодо безпеки, які не було сплановано належним чином.
- ▶ Проведіть симуляцію дій у день виборів та планів дій у надзвичайних ситуаціях.



#### АДАПТАЦІЯ:

- ▶ Створіть ретельний план заходів безпеки або перегляньте наявні плани, використовуючи підхід «здобутих уроків» на етапі планування.
- ▶ Підготуйте ретельний план екстрених заходів із метою відновлення виборчих операцій у разі настання інциденту.
- ▶ Періодично та перед кожними виборами проводьте та повторюйте симуляції кризових ситуацій на основі оновленого плану заходів безпеки.

### Приклади вразливостей за параметрами:



**ПРОЦЕДУРНІ:** Добре сплановані та скоординовані атаки можуть спрямовуватися на сервери, телекомунікаційні вузли й інше критично важливе обладнання. У найбільш напружені періоди виборів, наприклад із наближенням законодавчо визначених кінцевих термінів або власне у день виборів, фізичні атаки можуть бути дуже ефективним руйнівним інструментом. Наприклад, супротивник може спробувати втрутитися в процес підрахунку результатів виборів у достатньо великій кількості округів із метою затримати публікацію результатів або ж посягти сумніви в результатах виборів.

## Додаток 1 – Історія найбільш значних кібератак на об'єкти критичної інфраструктури в Україні

### Травень 2014 року – кібератака на ЦВК

За три дні до дня голосування на позачергових виборах Президента України, о 3 годині ранку, група хакерів активувала попередньо встановлене вірусне програмне забезпечення та знищила компоненти СВРВ, а також усі резервні копії цієї системи. На відновлення системи за допомогою офлайн резервних копій (збережених в автономному режимі), ЦВК знадобилося майже три дні; система була повністю готова до роботи лише за годину до початку голосування.

Досі залишається незрозумілим, як саме було встановлено вірусне програмне забезпечення. Хоча відповідальність за акцію взяла на себе проросійська група «Кіберберкут», є підозри, що насправді за кібератакою стояла група АРТ28, оскільки одразу після цього сталася DDoS-атака та невдала спроба розміщення сфальсифікованих результатів голосування на веб-сайті ЦВК.

### Жовтень 2015 року – атаки на ЗМІ («БлекЕнерджі»)

Хоча про існування троянського вірусу «БлекЕнерджі» було відомо ще у 2007 році, модифіковані варіанти цього шкідливого програмного забезпечення (відомі також під назвами «БлекЕнерджі»-2 та «БлекЕнерджі»-3) було виявлено в Україні в середині 2015 року – їх було вбудовано в документи Microsoft Excel та Word під виглядом макросів. Існує інформація про те, що ці типи шкідливих програм існували в Україні також і в 2014 році.

Наприкінці 2015 року антивірусна компанія ESET виявила, що троянський вірус «БлекЕнерджі» використовували для несанкціонованого віддаленого доступу (так званий backdoor) для встановлення надзвичайно шкідливої програми знищення даних на жорстких дисках (KillDisk) та для здійснення атак на деякі українські ЗМІ під час проведення місцевих виборів у жовтні 2015 року. Використання цієї програми (тобто, програми, що знищувала інформацію на жорстких дисках) було вперше зафіксовано спеціалізованим структурним підрозділом Держспецзв'язку, групою реагування на надзвичайні ситуації у комп'ютерній мережі під назвою CERT-UA. Метою атаки було знищити конкретні типи файлів у ЗМІ (як-от аудіовізуальні файли), і внаслідок цього завдати таким ЗМІ особливо відчутної шкоди.

### Грудень 2015 року – атаки на енергорозподільні компанії («БлекЕнерджі»)

Український енергетичний сектор став одним із головних об'єктів кібератак, здійснених за типом АРТ ще у 2015 році. Кібератака на енергорозподільні компанії із використанням вірусу «БлекЕнерджі» у грудні 2015 року стала найбільш успішною кібератакою в енергетичному секторі в історії. Наслідком атаки стало відключення на декілька годин електроенергії у трьох різних областях України, що завдало шкоди майже 300 000 українських громадян. Багато хто вважає, що за цими атаками стоїть група хакерів АРТ «Sandworm» (АРТ28).

Проникнення троянського вірусу до комп'ютерних мереж енергорозподільних компаній відбулося через розсилку фішингових електронних листів, які несанкціоновано встановлювали шкідливе програмне забезпечення для віддаленого доступу до мереж цих компаній. Хакерам вдалося встановити контроль над системами диспетчерського управління й збору даних, вимкнути енергопостачання та зрештою знищити дані на серверах, щоб запобігти виявленню джерел втручання в роботу автоматизованих систем.

### Січень 2016 року – Кібератака на міжнародний аеропорт «Бориспіль» («БлекЕнерджі»)

Іншим прикладом атаки на об'єкти критичної інфраструктури у цей самий період було виявлення зразків шкідливого програмного забезпечення типу «БлекЕнерджі» на комп'ютерах у Міжнародному аеропорту «Бориспіль». Хоча кібератаку так і не було проведено, імовірність серйозної шкоди через використання відповідної вірусної програми змусила органи влади в Україні посилити кібербезпеку на об'єктах критичної інфраструктури.

### Грудень 2016 року – Кібератака на Міністерство фінансів України та Державну казначейську службу

Хакерська АРТ група, яка використовувала невідомі інструменти для завантаження функціональної частини вірусу, спромоглася проникнути в автоматизовані системи Міністерства фінансів та Державної казначейської служби й знищити головні бази даних на серверах цих органів за допомогою вірусної програми знищення даних на жорстких дисках під назвою KillDisk.

Метою хакерів було повне виведення з ладу державної фінансової системи наприкінці року, тобто у період, коли з Державного бюджету здійснюються масові платежі. Хакери спромоглися зірвати велику кількість платіжних операцій на сотні мільйонів гривень.

### Грудень 2016 року – кібератака на Київенерго («Індустройер»)

За результатами другої успішної атаки на системи енергорозподільних компаній окремі райони міста Києва залишилися без світла на одну годину. Новою рисою цієї атаки стало використання шкідливого програмного забезпечення, створеного для систем контролю в промисловості, які не працюють зі звичайними комп'ютерними мережами (IP-протоколами передачі даних) для обміну інформацією.

Було встановлено, що шкідливим програмним забезпеченням був «Індустройер», відомий також під назвою «Крешоверрайд». Це модульне програмне забезпечення, до складу якого входить компонент для несанкціонованого віддаленого доступу, елемент запуску програми, чотири різні функціональні частини вірусу та програма знищення інформації.

### Грудень 2016 року – Кібератака на ІТ-системи «Укрзалізниці»

Помітним інцидентом у галузі кібербезпеки стало встановлення контролю над електронними системами найбільшої української компанії – «Укрзалізниці». Хоча у відкритому доступі наявна лише обмежена інформація щодо цього інциденту, повідомлялося, що за допомогою шкідливого програмного забезпечення та віддаленого доступу до мережі компанії хакери спромоглися вивести з ладу вебсайт «Укрзалізниці» та окремих транспортних систем, що призвело до серйозних затримок у розкладі руху потягів.

### Червень 2017 року – Кібератака на українські компанії (вірус «(Не)Петя»)

Кібератака з використанням вірусу «(Не)Петя» вважається наразі найбільшим глобальним інцидентом у сфері кібербезпеки. Проникнення шкідливого програмного забезпечення до систем великої кількості компаній відбулося разом з оновленням популярного фінансового програмного забезпечення M.E.Doc.

Атака, яку згодом почали приписувати хакерській групі АРТ «Піщаний хробак» (також відомій як

група АРТ28), спочатку передбачала проникнення до систем головного офісу М.Е.Дос та злам місцевого сервера з оновленням, який на той час працював на базі застарілої та незахищеної операційної системи.

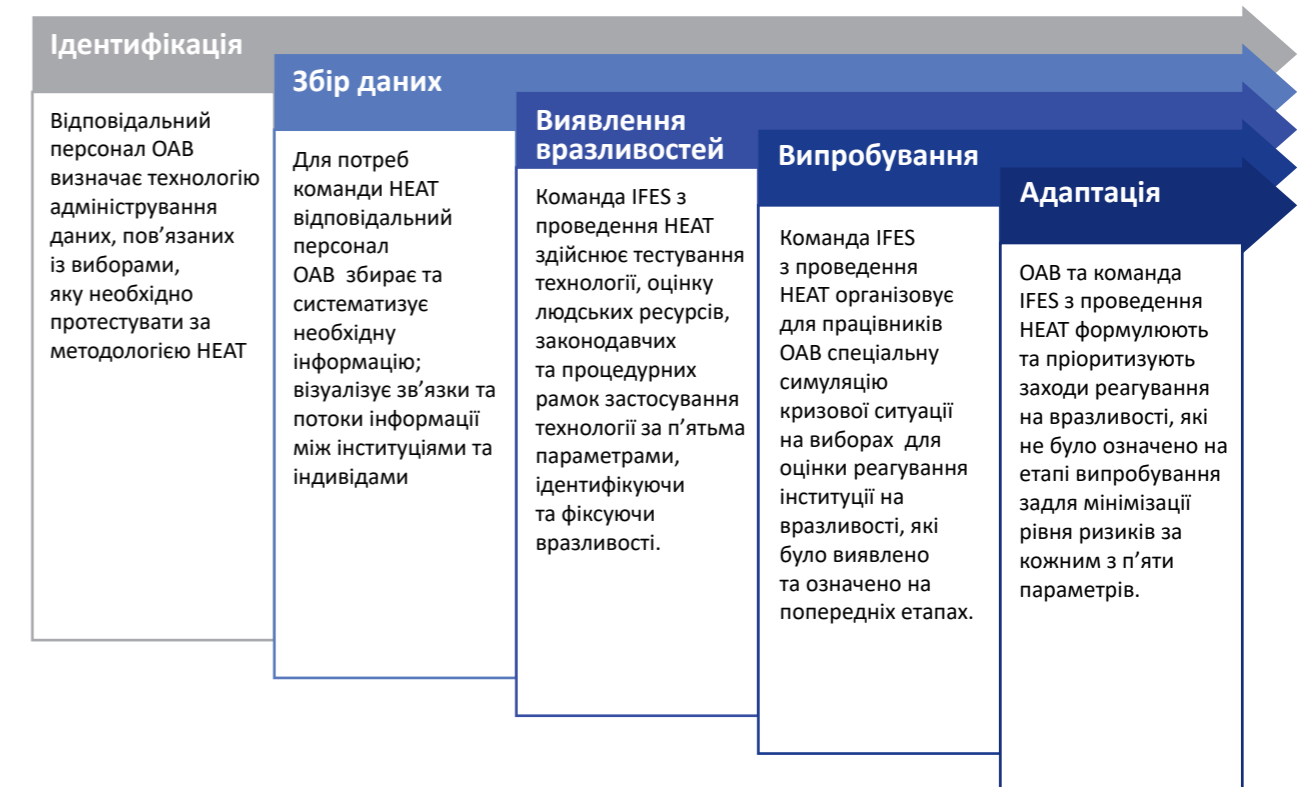
Шкідлива програма зашифрувала дані жорстких дисків інфікованих комп'ютерів і вимагала сплати грошового еквіваленту 300 американських доларів у криптовалюти за декодування. Насправді вірусне програмне забезпечення лише прикидалося програмою-шантажистом, адже користувачам, які сплатили викуп, не було надіслано жодних ключів для дешифрування даних.

Вірус «(Не)Петя» завдав значних збитків не лише українським, але й значній кількості міжнародних компаній.

### 📅 Жовтень 2017 року – кібератака на Київський метрополітен та Одеський аеропорт («БедРеббіт»)

Менш масштабною, але не менш серйозною була кібератака за допомогою програми-вимагача проти транспортних компаній, до яких належать Одеський міжнародний аеропорт та Київський метрополітен. Як і у випадку з вірусом «(Не)Петя», програма «БедРеббіт» здійснювала шифрування даних на жорстких дисках для отримання викупу за дешифрування. Наразі невідомо (або не розголошується), хто здійснив цю атаку в Україні.

## Додаток 2 – Процес комплексного тестування вразливостей та адаптування систем (HEAT)



Процес HEAT – це процес одночасної ідентифікації та тестування потенційного використання вразливостей у технології адміністрування даних, пов'язаних із виборами. HEAT передбачає тестування як самої технології, так і операційних рамок та законодавства, у межах яких ця технологія застосовується. На відміну від сертифікації технології або базового процесу тестування, процес HEAT – це комплексний підхід, що дозволяє дослідити вразливості й забезпечити їхнє виправлення, а також забезпечити інформування про них та їхнє усунення. Наприклад, в межах традиційного процесу сертифікації може проводитися тестування певної технологічної платформи з метою гарантування безпеки даних. Водночас, процес сертифікації не підготує ОАВ до ситуації звичайного блокування доступу до веб-сайту внаслідок кібератаки, що може серйозно знизити рівень довіри до інституції з боку пересічних громадян, незалежно від того, чи зазнали пов'язані з виборами дані тих чи інших пошкоджень або втручань, чи ні.

На основі тематики, трендів та підходів, відображених в літературі, IFES визначили п'ять різних параметрів, які має враховувати ОАВ при використанні технологічних платформ адміністрування даних, пов'язаних із виборами: технологічні, кадрові/людські, політичні, правові та процедурні. Саме на основі цих різних параметрів і тримається розвиток процесу HEAT. Завданням IFES є інкорпорація елементів наявних процесів тестування в зрозумілий і комплексний процес тестування, який би допоміг ОАВ усунути вразливості в кожному з п'яти напрямів, які можуть призводити до маніпуляцій із виборчими даними (як відомих, так і невідомих), припинення функціонування систем або законодавчих викликів у майбутньому. Процес HEAT не передбачає прийняття або відхилення рішень щодо використання тієї чи іншої технології, відбору того чи іншого постачальника. Водночас він дозволяє забезпечити ефективні відносини з постачальником, напрацювати стратегію реагування на ризики, що виникають у процесі постачання кібертехнологічного обладнання, налагодити взаємодію між різними технологічними платформами, які використо-

вуються на різних етапах виборчого процесу. Процес HEAT також дозволяє ОАВ підготувати ресурси та пристосувати процеси до ситуацій, пов'язаних із відмовою систем і несанкціонованим втручанням у їхню роботу, а також оскарженням рішення про застосування систем у судовому порядку. Останнє має особливе значення в контексті типу доказів, які є законними й допустимими у сфері використання технологій, формування доказової бази для врегулювання відповідних судових спорів у майбутньому. Реагування на такі виклики потребує тісної взаємодії ІТ-спеціалістів та юристів, які працюють у штаті ОАВ.

Як і в усіх інших аспектах виборчого процесу, позитивне суспільне сприйняття та громадська довіра є головними елементами довіри до виборів і визнання їхніх результатів. Процес HEAT має на меті запропонувати політикам та громадськості у цілому засоби мінімізації ризиків, необхідні для належного використання технологій у виборчому процесі, а також підкреслити важливість розробки планів дій у надзвичайних ситуаціях. Кінцевою метою процесу HEAT є підвищення рівня довіри суспільства до виборчого процесу, а також надання ОАВ допомоги у впровадженні та документуванні комплексної перевірки систем. Водночас, оскільки процес HEAT зосереджується на виявленні вразливостей, він має належним чином адмініструватися й доводитися до відома загалом з тим, щоб посилити (а не зруйнувати) довіру до ОАВ та технологій, які використовуються у виборчому процесі. Відповідно, ОАВ мають оперувати достатніми часовими та іншими ресурсами, які б дозволяли вирішувати виявлені проблеми, бо ж інакше відповідні вразливості можуть бути використані для того, щоб поставити під сумнів різні аспекти виборчого процесу, починаючи від достовірності відомостей реєстру виборців і закінчуючи легітимністю результатів виборів.

Процес HEAT включає п'ять кроків, які більш детально розглянуто нижче: ідентифікація (ОАВ визначає технологію, тестування якої проводиться); збір даних (IFES у взаємодії з ОАВ збирає необхідну інформацію, зокрема проводить візуалізацію компонентів систем); виявлення вразливостей (при цьому використовуються п'ять параметрів, що згадувалися раніше, IFES проводить роботу з виявлення вразливостей технології у межах кожного параметру); випробування (IFES спільно з ОАВ проводить симуляцію кризової ситуації, враховуючи при цьому вразливості, виявлені під час двох попередніх кроків); адаптація (ОАВ спільно з IFES визначають першочергові кроки, необхідні для захисту технологій у виборчому процесі від виявлених вразливостей).

*Короткий зміст процесу комплексного тестування вразливостей та адаптування систем*

## Ідентифікація

Процес HEAT побудовано таким чином, що головну роль у його проведенні має відігравати ОАВ, загалом процес спрямовано на посилення спроможності ОАВ (що відрізняє його від зовнішнього оцінювання). Власне, перший крок в межах HEAT виконує безпосередньо ОАВ (у разі необхідності – із залученням технічної допомоги), і передбачає від ОАВ визначити технологію/технології адміністрування даних, пов'язаних з виборами, яку необхідно випробувати за допомогою HEAT. Процес HEAT головним чином фокусується на електронних системах або платформах, пов'язаних з організацією виборчого процесу, які містять будь-які форми автоматизації або цифрової обробки даних, як-от реєстрація виборців, їхня ідентифікація, голосування, підрахунок голосів, передача даних щодо результатів голосування, встановлення підсумків голосування/результатів виборів. Залежно від того, наскільки складною або комплексною є система адміністрування, вона також може включати електронні системи реєстрації кандидатів, визначення формату виборчого бюлетеня (на складних виборах, зокрема на місцевих), а також друк виборчих бюлетенів. Тестувати можна як одну, так і декілька систем, залежно від конкретної країни, адже HEAT безпосередньо націлено на роботу із системами та процесами. Водночас, залежно від сфери компетенції ОАВ та особливостей відповідної країни, ОАВ може висловити бажання протестувати й інші системи або платформи адміністрування даних, зокрема бази даних реєстрації політичних партій, системи, пов'язані з фінансуванням передвиборної агітації та звітністю щодо такого фінансування, системи визначення меж виборчих округів, дільниць, місцезнаходження дільничних виборчих комісій, системи публічних закупівель та інвентаризації, бази даних кадрів і фінансів, веб-сайти та платформи соціальних медіа, системи адміністрування розгляду справ за скаргами суб'єктів виборчого процесу.

Кібербезпека – це комплекс заходів і дій, до яких вдаються для виявлення загроз цифровим мережам та захищеній інформації, захисту активів цифрової інформації (і пов'язаних із ними фізичних активів) від крадіжки, розкриття, знищення або зміни, виявлення того, що інцидент стався всередині системного домену, а також реагування на атаку й швидкого відновлення після завданого порушення.

Окрім визначення активів, що потребують захисту, ОАВ мають також бути готовими виконати оцінку ймовірності кіберінцидентів, як DDoS-атаки чи інсайдерські атаки, спір-фішинг та встановлення шкідливого програмного забезпечення. Ідентифікація всіх можливих кіберзагроз і ступеня їхнього впливу дозволяє підготуватися до наступних кроків у рамках процесу HEAT.

## Збір даних

Після ідентифікації конкретної технології адміністрування даних, пов'язаних із виборами, яка підлягатиме тестуванню в межах HEAT, відповідні працівники ОАВ мають зібрати та систематизувати всю необхідну інформацію, яка буде використовуватися командою HEAT. До цієї інформації належать закони, правила, процедури, посібники, навчальні матеріали, офіційні стратегії (якщо такі є) – з одного боку, а з іншого – технічна інформація щодо структури системи (у вигляді схеми), політики у сфері безпеки даних, скрипти налаштування та конфігурації системи, програмні початкові коди, інші пов'язані з цим матеріали тощо. Дуже важливо зібрати всі наявні закони й правила для того, щоб команда з проведення HEAT могла чітко визначити положення в законодавчих актах, які можуть зумовити сумніви в легітимності застосовуваної технології та в процесах адміністрування даних під час майбутніх виборів, переконатися в наявності ефективного регулювання та політик у сфері технології адміністрування даних, наявності чіткого розподілу ролей та відповідальності (особливо між ОАВ і постачальниками та користувачами), а також розробити плани дій у випадку надзвичайних ситуацій. До переліку таких законів і правил можуть входити Конституція відповідної держави, закони про вибори, акти ОАВ, інші суміжні закони та правила адміністрування даних, захисту інформації в автоматизованих системах, полі-

тика в галузі кібербезпеки, закони та правила, що регулюють цивільний процес та збір доказів, а також відповідне національне прецедентне право (за наявності). Окрім різноманітних законодавчих актів, ОАВ також має зібрати всі пов'язані (повністю або частково) із застосуванням відповідної технології політики, процедури, стратегії, операційні плани, керівні роз'яснення, посібники та навчальні матеріали, які використовуються в ході виборчого процесу.

На етапі збору даних ОАВ також має підготувати схему застосування відповідної технології, яка б візуалізувала компоненти системи, яку тестуватиме HEAT, а також зв'язки та потоки даних між інституціями й індивідами. Підготовка такої схеми може бути складовою процесу більш масштабного дослідження систем, яке оприявлюватиме зв'язки між ключовими суб'єктами. Дуже часто зв'язки між індивідами та інституціями (або брак таких зв'язків) може мати вплив на виборчий процес. Зв'язки, які ОАВ підтримує з іншими органами влади всередині країни, зокрема незалежними інституціями та органами виконавчої влади, залученими до процесу забезпечення захисту даних, мають бути чітко визначені саме на цьому етапі. Кіберспільнота є одноставною в тому, що обмін інформацією у сфері кібербезпеки є критично важливим для належного захисту даних і стійкості систем у цілому, і виборчий процес не є винятком. Незважаючи на це, винятковою рисою виборчого процесу є те, що він передбачає гарантування незалежності ОАВ та при цьому немає значення, якою є взаємодія цього органу з іншими інституціями й індивідами. Команда IFES із проведення HEAT надаватиме інструкції і зразки для візуалізації системи або ж може надавати пряму допомогу ОАВ у створенні такої візуалізації. Підготована схема буде частиною процесу випробування системи на вразливості командою HEAT, що проводиться на третьому етапі тестування.

## Виявлення вразливостей

На третьому етапі передбачається, що команда HEAT проводить колегіальний аналіз відповідних матеріалів, наданих ОАВ, а також візуалізації системи з метою виявлення вразливостей за п'ятьма параметрами – технологічним, кадровим/людським, політичним, правовим та процедурним. Оскільки в межах цього процесу всі п'ять параметрів вразливостей досліджуються в комплексі, до складу команди HEAT за загальним правилом входить експерт із питань технологій, юрист та експерт із питань виборів. Перший етап процесу HEAT використовується для визначення складу команди HEAT із позиції конкретної технології або технологій, які тестуються. Головне питання – хто є достатньою мірою кваліфікованим, щоб допомогти протестувати й оцінити виборчу технологію та рамки/контекст, в яких ця технологія застосовується? Як тільки буде надано відповідь на це питання, на цьому етапі тестування команда HEAT зможе визначити й зафіксувати вразливості, з якими стикається ОАВ в процесі використання специфічної технології, що тестується, і які групуються за кожним параметром, а також визначити попередній перелік можливих кроків, які би дозволяли усунути чи мінімізувати небезпеку цих вразливостей<sup>3</sup>. Крім того, команда з проведення HEAT має також проаналізувати зовнішні елементи, які можуть суттєво вплинути на виборчий процес, особливо в контексті можливого негативного впливу чи дезінформаційних кампаній проти ОАВ або інших зацікавлених сторін, а також вивчити наявні комунікаційні стратегії ОАВ.

## Випробування

З урахуванням специфічних вразливостей, визначених на етапах 2 та 3, команда HEAT організовує та проводить для відповідальних працівників ОАВ симуляцію кризової ситуації для визначення механізмів реагування ОАВ на специфічні типи інцидентів. Симуляція кризової ситуації – це навчання, яке проводиться в режимі моделювання реальних життєвих ситуацій в умовах

<sup>3</sup> Планується, що у майбутньому IFES підготує глобальну базу вразливостей та рекомендацій, оскільки процес HEAT проводиться у взаємодії із місцевими партнерами. Ця база зможе використовуватися як ОАВ, так і проектами технічної допомоги.

обмеженого часу на реагування, щоб імітувати тиск на учасників вправи, як в реальному житті. Симуляція кризової ситуації передбачає закріплення за кожним учасником конкретної ролі та відповідних обов'язків, а також дозволяє учасникам отримувати інформацію, приймати рішення та виконувати плани. Вона є дуже подібною до вправи «червоні команди», яка практикується Департаментом оборони США «для виявлення вразливості операційних концепцій до того, як такі вразливості будуть знайдені реальними суперниками»<sup>4</sup>. Для тестування реакцій учасників команда HEAT використовує вразливості, визначені на третьому етапі проведення тестування HEAT, та оцінює механізми реагування учасників на атаки, що стають можливими завдяки цим вразливостям, поява та розвиток яких моделюється в симульованих умовах. Цей етап має виконати два основних завдання – з'ясувати наявну спроможність і способи реагування на ситуації посадовців ОАВ, а також виступити в якості механізму ефективного навчання для посадовців, відповідальних за впровадження необхідних змін із метою зменшення ризиків кіберзагроз, з якими стикається ОАВ. Члени виборчих комісій нижчого рівня загалом потребують більш змістовного навчання з питань організації виборчого процесу, і кібербезпека у цьому контексті не є винятком.

Симуляція кризової ситуації дозволяє виявити та акцентувати для посадовців ОАВ конкретні потреби в навчанні для різних категорій персоналу ОАВ, зокрема пов'язані з кібергігієною та запобіганням спір-фішингу. Симуляція кризової ситуації має бути адаптована до вразливостей, виявлених під час проведення HEAT й у більш широкому виборчому контексті, в якому ОАВ застосовуватиме відповідну технологію. Симуляція кризової ситуації завершується підбиттям підсумків, під час якого обговорюються засвоєні уроки та формулюються способи реагування на решту вразливостей, що дозволяє ОАВ та IFES напрацювати план заходів на наступному та фінальному етапі тестування.

## Адаптація

Останнім кроком процесу HEAT є спільна підсумкова вправа та стратегічна сесія за участі відповідних посадовців ОАВ. Під час цієї сесії формулюються та пріоритизуються кроки, спрямовані на усунення вразливостей, які не було задовільним чином нейтралізовано на етапі випробування. Кінцевою метою цієї сесії є мінімізація рівня загроз за п'ятьма параметрами. Під час неї з'ясується, хто саме є відповідальним за виправлення або усунення вразливостей, короткострокові та довгострокові фінансові плани, протягом яких термінів мають здійснюватись відповідні заходи та яким чином має забезпечуватися прозорість та комунікація.

З точки зору технологічного параметру вразливостей основними інструментами, які ОАВ може розглянути для запобігання зламам системи, є такі: ретельне проектування самої системи, тестування, налаштування, пілотне провадження, перевірка, складання плану дій у надзвичайних ситуаціях. ОАВ повинні мати резервні плани підтримки функціонування нових систем, зокрема можливість запуску в роботу попередньої системи у випадку виникнення кризової ситуації. Наприклад, якщо система розподілу місць є доволі складною, комісія, яка несе за це відповідальність, може вирішити не покладатися виключно на програмне забезпечення, яке використовується вперше, навіть якщо попередньо проводилися заходи з тестування такого програмного забезпечення<sup>5</sup>. ОАВ повинні мати посилену спроможність для здійснення моніторингу роботи систем для того, щоб із високою часткою впевненості визначити природу подій, які відбуваються в системах. За умови наявності відповідної стратегії ОАВ зможуть реагувати на ситуації оперативного реагування, застосовувати план дій у надзвичайних ситуаціях та поновлювати систему на основі використання резервних копій.

<sup>4</sup> Наукова робоча група з питань оборони, Роль та статус діяльності в рамках «Червоних команд», Департамент оборони США, вересень 2003 року, <https://fas.org/irp/agency/dod/dsb/redteam.pdf>.

<sup>5</sup> У Данії під час виборів до Європейського парламенту у 2009 році Департамент статистики Данії використовував програмне забезпечення для розподілу місць за кількістю голосів, але також неофіційно використовував таблиці MS Excel як додатковий інструмент для перевірки правильності такого розподілу.

З точки зору кадрового/людського параметру вразливостей цілком очевидною може бути потреба вжити заходи, спрямовані на протидію інсайдерським атакам (наприклад, шляхом моніторингу фізичного доступу до серверів). Водночас інколи існує потреба й у додаткових заходах. Це може передбачати одночасний доступ двох ІТ-спеціалістів до «чутливих» серверів, відмову від використання бездротових технологій з'єднання з чутливими мережами для запобігання кібератак із використанням підробленого Wi-Fi доступу (так звана атака типу «злий двійник»). Мають бути впроваджені системи контролю за дотриманням рівнів допуску до систем, створення журналів фіксації входів до систем; всі входи до системи мають регулярно переглядатися уповноваженими спеціалістами з відділу ІКТ для гарантування дотримання режиму доступу та запобігання зловживанням. Перевірка персоналу на етапі влаштування на роботу є позитивною практикою, але вона має проводитися у спосіб, який би запобігав непотизму або дискримінації чи виникненню нових проблем, зокрема, потенційної бюрократичної тяганини. Прогресивні ОАВ мають впроваджувати стратегії захисту безпеки даних для підвищення ефективності адміністрування даних, щоб вона не знижувалася за рахунок використання застарілих, вразливих та нечинних на практиці систем.

З точки зору політичних вразливостей, ОАВ мають уважно планувати та проводити процеси закупівлі технологій для проведення виборів, а також напрацювати ефективні механізми консультацій і комунікацій з питань кібербезпеки. З метою посилення юридичної та фактичної незалежності ОАВ та його керівництва можна вживати особливі заходи. Водночас, залежно від природи кіберзагроз може існувати потреба в більш тісній взаємодії ОАВ із працівниками правоохоронних органів, служб розвідки. Така взаємодія має здійснюватись обережно, при цьому слід враховувати необхідність збереження незалежності ОАВ – як на практиці, так і з точки зору суспільного сприйняття цієї інституції. З точки зору правового та процедурного параметру вразливостей може існувати потреба у внесенні змін до законодавства або регуляторних актів – так само, як і в розробці або вдосконаленні стратегічних документів, операційних планів, навчальних матеріалів, посібників та керівних принципів.

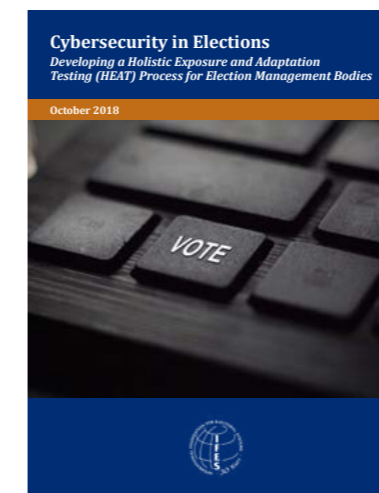
ОАВ часом насправді мають певні практики кібербезпеки, однак вони, розпорошені між різними документами, містяться в неофіційних файлах ІТ-спеціалістів або навіть не існують у паперовому вигляді, а лише використовуються на практиці. Команда HEAT має заохочувати ОАВ до об'єднання та викладу практичних настанов із питань кібербезпеки в одному документі. Це дозволить забезпечити більшу доступність та прозорість відповідних практик і припущень для самого ОАВ, а також надасть можливість оперативного коригування таких практик (наприклад, якщо система не передбачає жодних обмежень щодо довжини та структури паролів, це може бути вкрай проблематичним). Якщо такі практики формалізовані, вони можуть стати стратегією забезпечення кібербезпеки ОАВ. Впровадження подібної стратегії дозволить посилити ступінь готовності ОАВ до протидії кіберзагрозам.

Конкретні рекомендації та кроки, напрацьовані на цьому фінальному етапі, залежать від інформації, отриманої під час виконання попередніх кроків. Приклади кроків, визначених на етапі адаптації, – це курси кібергігієни для працівників ОАВ, інтерактивний посібник із кібербезпеки, спеціально розроблений для ОАВ, надання допомоги під час закупівлі нових технологій. Врешті-решт, метою процесу HEAT є комплексне оцінювання специфічних виборчих технологічних систем та їхніх вразливостей, пряме залучення відповідних посадовців ОАВ до процесу тестування задля того, щоби цей процес міг слугувати інструментом розвитку спроможності, а також визначення змін, які можуть бути впроваджені під егідою ОАВ із метою зменшення ризиків кіберзагроз.

## Додаток 3 – Література з кібербезпеки на виборах

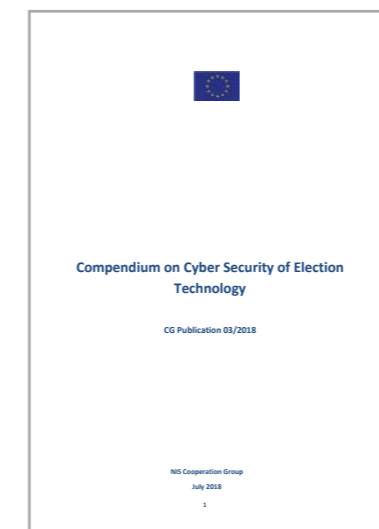
Інформаційно-ресурсна база щодо кібербезпеки на виборах швидко розвивається.

Тут наведено список із п'яти рекомендованих публікацій, які вийшли 2018 року, що безпосередньо стосуються кібербезпеки у виборчих процесах або пов'язаних із ними технологіях, складений за датою публікації:



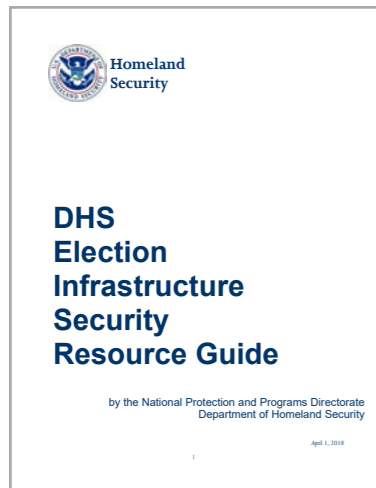
**Cybersecurity in Elections: Developing a Holistic Exposure and Adaptation Testing (HEAT) Process for Election Management Bodies [Кібербезпека на виборах: розробка процесу комплексного тестування вразливостей та адаптації систем (HEAT) для органів адміністрування виборів] (IFES, жовтень 2018 року)**

У цій публікації IFES запропонувала нову методикку для оцінки загроз кібербезпеки та спроби їхнього усунення на основі використання комплексного підходу. У цьому інтерактивному посібнику використовується варіант методики HEAT; більше деталей наведено у Додатку 2.



**NIS CG Compendium of Cyber Security on Election Technology [Компендіум із кібербезпеки виборчих технологій, укладено Групою співробітництва з мережевої та інформаційної безпеки] (липень 2018 року)**

Група співробітництва у сфері мережевої та інформаційної безпеки, до якої увійшли представники Європейської комісії, ENISA та країн-членів ЄС, підготувала комплексний компендіум загроз кібербезпеки на європейських виборах, охоплюючи, серед іншого, майбутні вибори до Європейського парламенту, які заплановано на травень 2019 року. Розглядаються конкретні технічні заходи для захисту виборів, пов'язані з цілісністю даних та моніторингом мережі, а також такі важливі поняття, як підзвітність, довіра та прозорість. У розділі, присвяченому тематичним дослідженням (кейс-стаді), пропонуються різноманітні приклади, зокрема реальні інциденти з практики.



### Election Infrastructure Security Resource Guide [Керівні принципи використання ресурсів для гарантування безпеки виборчої інфраструктури] (створено DHS, квітень 2018 року)

У цій публікації Департаменту національної безпеки США пояснюється, які ресурси доступні посадовцям виборчих адміністрацій у США. Це підсумок роботи, розпочатої ще на початку 2017 року. Департамент національної безпеки США пропонує різноманітні послуги та консультації, пов'язані з виборами, такі як оцінка кібербезпеки базових систем, виявлення загроз та запобігання інцидентам, обмін інформацією для поліпшення взаємодії та навчання персоналу.

### A Handbook for Elections Infrastructure Security [Довідник із безпеки інфраструктури виборів] (укладено Центру інтернет-безпеки, лютий 2018 року)

Центр Інтернет-безпеки (CIS) – це провідна американська неприбуткова організація, яка активно пропонує ресурси, необхідні для гарантування кібербезпеки як приватним, так і державним організаціям. У їхньому посібнику надається огляд ризиків, пов'язаних із різними виборчими системами. Попри те, що посібник розглядає виборчі системи, які є специфічними для США, найцінніші рекомендації із публікації CIS можна використати в будь-якій виборчій системі світу. Слід зазначити, що ці рекомендації є дуже точними та базуються на основі різних детальних стандартів, серед яких – стандарти NIST та Керівні принципи системи добровільного голосування Комісії зі сприяння у проведенні виборів (EAC) (VVSG).

### Cybersecurity Playbook for Election Officials [Інтерактивний посібник із кібербезпеки для посадовців органів адміністрування виборів] (укладено Белферським центром, лютий 2018 року)

Белферський центр науки й міжнародних зв'язків «Школи державного управління імені Джона Ф. Кеннеді» Гарвардського університету створив проект D3P ще в липні 2017 року з безпосередньою метою допомогти захистити демократичні вибори від кібератак та кіберзагроз. У цьому інтерактивному посібнику розглядаються аспекти кібербезпеки, які застосовуються до юрисдикцій виборчих округів у США, з урахуванням 10 провідних практик, які може застосувати будь-яка виборча комісія. Окрім того, наведені технічні рекомендації стосуються конкретних компонентів виборів, як-от бази даних реєстрації виборців та реєстри для електронного голосування, електронне обладнання для голосування та системи звітності про результати. Багато рекомендацій, що містяться у цьому посібнику, так само як і в «Довіднику з безпеки інфраструктури виборів», опублікованому CIS, є універсальними.



## Додаток 4 - Скорочення

Держспецзв'язок – Державна служба спеціального зв'язку та захисту інформації

ДВК – Дільнична виборча комісія

ДРВ – Державний реєстр виборців

ЄС – Європейський Союз

ІКТ – Інформаційно-комунікаційні технології

ІТ – Інформаційні технології

МВС – Міністерство внутрішніх справ

НАТО – Організація Північноатлантичного договору

НУО – Неурядова організація

ОАВ – Орган адміністрування виборів

ОАР – Орган адміністрування реєстру

ОВК – Округна виборча комісія

ОВР – Орган ведення реєстру

ОС – Операційна система

СБУ – Служба безпеки України

США – Сполучені Штати Америки

ЦВК – Центральна виборча комісія

APT – *англ.* Advanced Persistent Threat – Ускладнені сталі загрози

BDS – *англ.* Breach Detection System – Система виявлення зламів

BRIDGE – *англ.* Building Resources in Democracy, Governance and Elections – Розбудова ресурсів у сфері зміцнення демократії, врядування та виборів

BRP – *англ.* Business Recovery Plan – План відновлення після інцидентів

CERT – *англ.* Computer Emergency Response Team – Група реагування на надзвичайні ситуації у комп'ютерній мережі;

CERT-UA – Спеціалізований структурний підрозділ Державного центру кіберзахисту та протидії кіберзагрозам

CIS – *англ.* Center for Internet Security – Центр Інтернет-безпеки

CMS – *англ.* Content Management System – Система управління контентом

CSIRT – *англ.* Computer Security Incident Response Team – Група реагування на інциденти в сфері комп'ютерної безпеки

D3P – *англ.* Defending Digital Democracy Project – Проект захисту цифрової демократії

DDoS – *англ.* Distributed Denial-of-Service – Розподілена відмова в обслуговуванні

DHS – *англ.* Department of Homeland Security – Департамент національної безпеки

DMZ – *англ.* Demilitarized Zone – Демілітаризована зона

DPI – *англ.* Deep Packet Inspection – Глибинна перевірка пакетів – технологія перевірки та фільтрації пакетів за змістом. DPI здатен виявляти і блокувати віруси, фільтрувати інформацію відповідно до заданих критеріїв.

EAC – *англ.* Election Assistance Commission – Комісія зі сприяння у проведенні виборів

EDR – *англ.* Endpoint Detection and Response – Система виявлення загроз на кінцевих точках

ENISA – *англ.* European Network and Information Security Agency – Європейське агентство з питань безпеки мереж та інформації

GOTV – *англ.* Get Out to Vote – Заохочення до участі в голосуванні

HEAT – *англ.* Holistic Exposure and Adaptation Testing – Процес комплексного тестування вразливостей та адаптації систем

HNEC – *англ.* High National Election Commission – Вища національна виборча комісія

IAM – *англ.* Identity and Access Management – Управління ідентифікацією та доступом

IFES – *англ.* International Foundation for Electoral Systems – Міжнародна фундація виборчих систем

IPS – *англ.* Intrusion Prevention System – Система запобігання вторгненням

LAN – *англ.* Local Area Network – Локальна (закрита) мережа

MAC – *англ.* Media Access Control – Управління доступом до середовища. Для забезпечення можливості передачі певної інформації необхідно, щоб кожен мережевий інтерфейс мав власну унікальну адресу в мережі Ethernet. Вона називається MAC-адресою (MAC = Media Access Control).

MITM – *англ.* Man-In-The-Middle (attack) – Несанкціоноване підключення «посередника» при передачі даних

MPLS – *англ.* Multiprotocol Label Switching – Багатопротокольна комутація з використанням міток

NIC – *англ.* Network Interface Card – Карта мережевого інтерфейсу

NIS CG – *англ.* Network and Information Security Cooperation Group – Керівна група з питань мережевої та інформаційної безпеки

NIST – *англ.* National Institute of Standards and Technology – Національний інститут стандартів і технології

OWASP – *англ.* Open Web Application Security Project – Замінить на Відкритий проект із безпеки веб-додатків

PAM – *англ.* Privileged Access Management – Система управління привілейованим доступом

RMS – *англ.* Results Management System – Система встановлення результатів виборів (СРРВ)

RRS – *англ.* Results Reporting System – Система передачі інформації про результати виборів (СРІРВ)

SCADA – *англ.* Supervisory Control and Data Acquisition (control system) - Система управління, контролю та збору даних (система контролю)

SIEM – *англ.* Security Information and Event Management – Управління подіями інформаційної безпеки (від об'єднання двох термінів, що позначають сферу застосування ПО: SIM – *англ.* Security Information Management – Управління інформаційною безпекою, а також SEM – *англ.* Security Event Management – Управління подіями безпеки)

SOC – *англ.* Security Operations Center – Центр керування кібербезпекою

SP – *англ.* Stored Procedures – Збережені процедури

SPOF – *англ.* Single Point of Failure – Єдина точка відмови (компонент, відмова якого призводить до відмови всієї системи)

SQL – *англ.* Structured Query Language – Мова структурованих запитів (міжнародна стандартна мова для визначення і доступу до реляційних баз даних)

TCP/IP – *англ.* Transport Control Protocol / Internet Protocol – Набір мережевих протоколів передачі даних

TTX – *англ.* Table Top Exercise – Симуляція кризової ситуації

USB – *англ.* Universal Serial Bus – Універсальна послідовна шина, USB

VLAN – *англ.* Virtual Local Area Network – Віртуальна локальна мережа

VPN – *англ.* Virtual Private Network – Віртуальна приватна мережа

VVSG – *англ.* Voluntary Voting System Guidelines – Сертифікація пристроїв електронного голосування

WAF – *англ.* Web Application Firewall – Міжмережевий екран рівня веб-додатків

XSS – *англ.* Cross-site Scripting – «Міжсайтовий скриптинг», тип вразливості інтерактивних інформаційних систем у вебі.