# Типовий комунікаційний план у сфері кіберінцидентів під час виборів

## Для політичних партій та кампаній

## Міжнародне видання

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

ЗАХИСТ ЦИФРОВОЇ ДЕМОКРАТІЇ
ТРАВЕНЬ 2018

Адаптовано у партнерстві з

NDI IRI

**Проект «Захист цифрової демократії»**
Центр «Белфер» з науки та міжнародних відносин Гарвардської школи ім. Джона Ф. Кеннеді
вул. Дж.Ф. Кеннеді 79
Кембрідж, Масачусетс 02138

**www.belfercenter.org/D3P**

Партнер міжнародного видання

**Національний демократичний інститут**
www.ndi.org

**Міжнародний республіканський інститут**
www.iri.org



Дизайн та оформлення Ендрю Фасіні

Фото на обкладинці: Adobe Stock

# Типовий комунікаційний план у сфері кіберінцидентів під час виборів

## Для політичних партій та кампаній

## Зміст

# Вітальне слово

Ми створили **Проект із Захисту цифрової демократії** (D3P) у липні 2017 року з однією метою: допомогти забезпечити безпеку демократичних виборів від загроз кібербезпеки та інформаційних операцій. Існує декілька груп на передовій захисту демократії: (1) політичні кампанії; (2) політичні партії, (3) особи, відповідальні за організацію та проведення виборів, і (4) неурядові організації.

Ми поставили перед собою завдання протягом минулого року забезпечити кампанії, політичні партії, а також спеціалістів з питань виборів практичними керівництвами до найбільш вживаних передових практик у сфері кібербезпеки до проведення проміжних виборів у Сполучених Штатах у 2018 році. В листопаді 2017 року ми випустили «Стратегію забезпечення кібербезпеки під час кампанії» для спеціалістів із проведення кампаній. У лютому 2018 року ми випустили комплекс з трьох стратегій виборів США, розроблений для використання спільно з організаторами виборів в США, а саме: «Стратегія забезпечення кібербезпеки під час проведення загальнодержавних та місцевих виборів», «Керівництво з координації комунікування кіберінцидентів під час виборів» та «Типовий комунікаційний план у сфері кіберінцидентів під час виборів».
Після опублікування цих стратегій ми дізналися від міжнародних організацій про необхідність аналогічних розробок на глобальному рівні. Щоб задовольнити цю потребу, ми випускаємо «Типовий комунікаційний план у сфері кіберінцидентів під час виборів» для світової аудиторії. Де б не виникали інциденти у сфері кібербезпеки, політичні партії, кампанії та інші особи, які підтримують демократичні вибори, повинні мати засоби швидкої та ефективної комунікації з метою збереження довіри до демократичної виборчої системи.

D3P це двопартійна група експертів із кібербезпеки та політики з державного та приватного секторів, а також професіоналів з багатим досвідом проведення політичних кампаній. Ми співпрацювали з Міжнародним республіканським інститутом (MPI) та Національним демократичним інститутом (НДІ) з метою розробки стратегії у сфері комунікацій, адаптованої до умов виборів у міжнародному контексті.

Одна із суттєвих потреб, з якою ми зіткнулися, полягала в проханні про надання керівних вказівок щодо того, яким чином комунікувати під час кібер кризи, тому що для багатьох політичних партій, кампаній та інших організацій, які займаються проведенням демократичних виборів, питання кібербезпеки є незнайомими.

Цей типовий план насамперед призначений для використання політичними партіями або кампаніями як основи для розробки власних комунікаційних планів реагування, які включають передові практики, рекомендовані зовнішні процеси реагування, а також очікувані сценарії кіберінцидентів під час проведення виборів.

Сподіваємося, даний типовий план стане для політичних організацій в усіх країнах відправною точкою для підготовки заходів протидії кіберінцидентам під час проведення виборів.

На закінчення, ми би хотіли висловити подяку політичним партіям, особам, відповідальним за організацію та проведення виборів і організаціям, для яких ми писали цей Шаблон та інші шаблони цієї серії. Ви — передові захисники демократії. Сподіваємося, що ці зусилля допоможуть дещо полегшити таку колосальну відповідальність.

# Автори та дописувачі

Цей проект став результатом спільних зусиль D3P, MPI та НДІ. З часу їхнього створення в 1983 році відповідно до закону Конгресу, яким було засновано Національний фонд демократії, MPI та НДІ відповідали прагненням людей у всьому світі жити у демократичному суспільстві, яке захищає основні права людини. Непартійні Інститути працювали з політичними партіями, групами громадянського суспільства та парламентами у більш ніж 100 країнах з метою зміцнення демократичних інститутів, забезпечення безпеки виборчого процесу, сприяння залученню громадян, а також сприяння відкритому, підзвітному уряду.

Цей проект став можливий завдяки десяткам людей, які люб'язно приділили йому свій час. Особлива подяка Шивон Горман, Крісу Фарлі, а також Мередіт Девіс Тавера, яка склала план.  Також ми хочемо висловити подяку Сарі Моултон та Джесперу Франту з НДІ та Джону Томашевскі й Сему ЛаХуд з MPI за проведену роботу щодо інтернаціоналізації цього типового плану.

Ми також у боргу перед зазначеними нижче людьми, які витратили незчисленні години на перегляд чорнових варіантів та розробку власного внеску.

ЗАХИСТ ЦИФРОВОЇ ДЕМОКРАТІЇ

**Ерік Розенбах**, (Eric Rosenbach), співдиректор Центру «Белфер»; Директор Проекту «Захист цифрової демократії»

**Роббі Мук** (Robby Mook), співдиректор D3P

**Метт Роудз** (Matt Rhoades), співдиректор D3P

**Кейтлін Конлі** (Caitlin Conley), виконавчий директор D3P

**Мередіт Девіс Тавера (Meredith Davis Tavera)**, D3P, Школа управління ім. Джона Ф. Кеннеді, Гарвард

**Мері Дуґас** (Mari Dugas), координаторка проекту, D3P, Школа управління ім. Джона Ф. Кеннеді, Гарвард, центр «Белфер»

**Кріс Фарлі** (Chris Farley), адвокат, Albright Stonebridge Group

**Шивон Горман** (Siobhan Gorman), партнер, «Brunswick Group», консультативна група D3P високого рівня

ДОДАТКОВІ АВТОРИ ТА ДОПИСУВАЧІ

**Стів ДіПангразіо (Steve DiPangrazio)**, Міжнародний республіканський інститут

**Джеспер Франк (Jesper Frank)**, Національний

демократичний інститут

**Сем ЛаХуд (Sam LaHood)**, Міжнародний

республіканський інститут

**Сара Моултон (Sarah Moulton)** , Національний

демократичний інститут

**Джон Томашевскі (John Tomaszewski)** , Міжнародний республіканський інститут

**Френк Уайт**, незалежний консультант з питань комунікації

ГРУПА ВЕБ-РОЗРОБНИКІВ ТА ДИЗАЙНЕРІВ ЦЕНТРУ «БЕЛФЕР»

**Аріель Дворкін** (Arielle Dworkin), менеджер з цифрових комунікацій, Школа управління ім. Джона Ф. Кеннеді, Гарвард, центр «Белфер»

**Ендрю Фасіні** (Andrew Facini), координатор з питань друку та дизайну, Школа управління ім. Джона Ф. Кеннеді, Гарвард,центр «Белфер»

# Короткий зміст та ціль

За останні декілька років загрози втручання у вибори за допомогою кібер-засобів значно зросли та стали більш різноманітними і потенційно руйнівними для виборчого процесу. Пов'язаний з виборами кіберінцидент може охоплювати широкий спектр зловмисної діяльності в кіберпросторі. Протягом політичної кампанії він може варіюватися від крадіжки даних кампанії або зловмисників, які зламують веб-сайт партії або кандидата, до розповсюдження дезінформації, щоб розхитати вибори. Найчастіше мета полягає у підриві довіри та підтримки демократичних інститутів.

З урахуванням щораз більшої кількості кібер-загроз, які виникають перед виборами у всьому світі, політичні партії та кампанії займаються підготовкою шляхів реагування на кіберінциденти на усіх напрямках, включаючи зовнішні комунікації. Ефективні комунікації під час кіберінциденту, які демонструють, що постраждала організація займається управлінням інциденту для збереження цілісності виборів, мають вирішальне значення для підтримання довіри до демократичних систем.

**Головне завдання цього документу полягає у тому, щоб забезпечити можливість політичних партій та кампаній зберегти довіру громадськості до цілісності їхньої демократичної виборчої системи у випадку кіберінциденту.** Даний документ надає шаблон та рекомендації для політичних партій та кампаній щодо розробки власних комунікаційних планів для управління інцидентами у сфері кібербезпеки під час виборів. Він включає набір передових практик та містить структуру комунікаційної стратегії реагування, яку політичні партії згодом зможуть розбудувати та пристосувати до своєї країни та конкретних обставин.

Головною складовою збереження довіри є надання громадськості своєчасної та точної інформації. Не менш важливе значення має максимально швидке спростування недостовірної інформації, особливо у нинішньому замкнутому колі традиційних та соціальних засобів масової інформації. Найбільш ефективний спосіб підтримання довіри полягає у тому, щоб партійне керівництво – в усіх асоціаціях та юрисдикціях – виявлено єдність позицій.

Можливість виникнення кіберінцидентів, пов'язаних з інфраструктурою кампанії, зокрема веб-сайтами, базами даних донорів та членів партії, а також обліковими записами в соціальних мережах є сумними реаліями нашого часу. Зростає зацікавленість у використанні кібер-засобів для шпигування або зриву виборів у США, починаючи щонайменше з 2008 року та завершуючи резонансними кіберінцидентами 2016 року.

Водночас державні чиновники та громадські лідери на всій території Європи приділяють особливу увагу кіберінцидентам, що направлені проти важливих демократичних інститутів, принаймні з моменту надання широкого розголосу втручанню в системи Федерального

парламенту Німеччини (Бундестагу) у 2015 році. Занепокоєння викликав 2017 рік важливих виборів, протягом якого Нідерланди та Норвегія вирішили провести національні підрахунки голосування на папері у випадку порушення функціонування електронних систем, французька президентська кампанія Емануеля Макрона стала «жертвою масованої та координованої атаки», а Німеччина боролася за захист своїх систем після інцидентів з атаки аналітичних центрів, які тісно пов'язані з двома основними партіями в країни.

Така тенденція справедливо викликає занепокоєння політичних партій та кампаній, які беруть участь у виборах у всьому світі. В рамках майбутніх циклів, спроби, що ставлять вибори під загрозу, можуть поширитися на нові країни або передбачати виникнення нової тактики. Кожній політичній організації, відповідно, слід включити план комунікацій під час кризи кіберпростору як частину власної загальної стратегії безпеки.

Такий план повинен надавати змогу партійному керівництву продемонструвати свою впевненість в управлінні кіберінциденту. Усі публічні заяви повинні демонструвати, що партійні чиновники компетентно регулюють ситуацію. Будь-які конкретні деталі, які вони повідомляють, повинні бути незмінними. Наприклад, масштаб інциденту, ймовірно буде змінюватися, тому партійним чиновникам не слід на початковому етапі обговорювати цей аспект публічно. Зміна перебігу ситуації може підірвати впевненість в управлінні інцидентом та власне у виборчій системі.

Окрім того, існують елементи кіберінциденту, які потребують спеціальної підготовки, оскільки криза кіберпростору відрізняється від інших криз в ключових питаннях:

> Скоріш за все вам буде відомо небагато фактів, коли вам вперше доведеться повідомляти про інцидент, і, маючи відносно обмежену інформацію, ви маєте продемонструвати, що впевнено та кваліфіковано здійснюєте управління інцидентом.

> Багато журналістів, які висвітлюють історії, що стосуються кіберпростору, володіють технічними та політичними питаннями й мають цілий ряд добре інформованих та правдивих джерел, тому вони можуть дізнатися про деталі інциденту раніше за вас.

> Кіберінциденти можуть вимагати координації діяльності широкого кола урядових та неурядових інститутів, які зазвичай не співпрацюють між собою.

> Інциденти, що направлені проти інфраструктури політичних кампаній, можуть спричиняти наслідки, які виходять за традиційні рамки різних юрисдикцій.

> Кіберінцидент здатен підірвати довіру громадськості до кандидата, політичної партії або навіть до самої демократичної виборчої системи. Важливо спілкуватися чесно, але таким чином, щоб уникнути необґрунтованого хвилювання.

Шаблон описує ключові компоненти комунікаційного плану, який політичні партії та кампанії зможуть розбудувати та пристосувати до своїх потреб. Цей Шаблон розроблено для спільного використання зі **Стратегією забезпечення кібербезпеки під час проведення кампанії, Європейське видання**.

Наступні розділи містять, зокрема, пропозиції, які слід зберегти, змінити або видалити, з огляду на ваші потреби. **Їх подано у форматі шаблону, включно зі внесеним у дужках текстом для внесення назви вашої організації або деталей конкретної ситуації.**

Шаблон починається з того, як користуватися цим комунікаційним планом. Далі він описує передові практики, ключові комунікаційні процеси, а також сценарії, на основі яких ви зможете підготуватись.
Окрім координованого комунікаційного процесу, який викладено у цьому Шаблоні, вашим партійним чиновникам слід вжити додаткових заходів для підготовки до кіберінциденту. Заходи, які можна вжити негайно:

- Узгодити комунікаційний план із технічним планом реагування та регулярно їх оновлювати.
- Сумлінно тестувати ці плани за допомогою моделювання на різних рівнях вашої партії.
- Отримувати регулярне оновлення інформації про кібер-загрози, особливо якщо вони стосуються виборів.
- Підтримувати відносини з чиновниками та експертами, які матимуть стосунок до розслідування та координації реагування на будь-який кіберінцидент.
- За можливості інформувати населення про роботу, яку ви виконуєте. Налаштуйтеся на те, що під час виборів, можливо, виникне певна кібер-загроза, та поясніть, як така активність відрізняється від імовірних необхідних заходів для переривання виборчого процесу.

Важливо часто оновлювати комунікаційні плани реагування – щонайменше щороку – для ознайомлення нових учасників з процесом та для забезпечення застосування досвіду, накопиченого вами раніше, а також досвіду інших країн.

# Як користуватися комунікаційним планом

Комунікаційний план `[ОРГАНІЗАЦІЇ]` включає керівництво та типові матеріали, щоб допомогти нам відреагувати на пов'язаний з виборами кіберінцидент швидко та скоординовано протягом перших декількох днів після виникнення інциденту у сфері кібербезпеки.

Хоча кожна ситуація є унікальною, цей план забезпечує основу, яку ми можемо використати для планування належної реакції на інцидент з метою збереження довіри до кандидата, партії та виборчого процесу.

`[ОРГАНІЗАЦІЯ]` повинна бути виключним власником цього плану та оновлювати його мінімум раз на рік, особливо якщо виникають та видозмінюються нові кібер-загрози.

## Ключові компоненти охоплюють:

**Передові практики щодо кіберінцидентів**: Цей розділ включає передові практики спілкування зі ЗМІ та іншими ключовими зацікавленими сторонами.

**Схему комунікаційного процесу**: Ця складова включає схеми, які визначають, хто здійснює управління заходами реагування на кризову ситуацію, хто виступатиме речником та регулюватиме щоденні комунікації в умовах кризи протягом інциденту.

**Контрольний перелік на предмет реагування на інциденти**: Контрольний перелік широко охоплює заходи, які потрібно вжити протягом перших декількох днів після того, як стало відомо про інцидент.

**Встановлення базових комунікацій:** Важливо повідомляти про заходи, які вживаються для подолання наслідків кіберінцидентів. Такі дії сприятимуть встановленню вихідного розуміння громадськістю ризиків та сумлінних зусиль, яких докладає ваша організація для пом'якшення ситуації. У цьому розділі наводиться приклад.

**Сценарій планування керівництвом та матеріалами**: Цей розділ містить можливі сценарії інцидентів, з якими ми можемо зіткнутися, та керівні принципи реагування на них.

[Також він містить комунікаційні матеріали для можливого використання у різних сценаріях. ЗВЕРТАЄМО УВАГУ, ЩО ВАШІЙ ОРГАНІЗАЦІЇ НЕОБХІДНО РОЗРОБИТИ ЦІ МАТЕРІАЛИ ЗА ДОПОМОГОЮ КЕРІВНИХ ПРИНЦИПІВ, ЯКІ ПОДАНО У ШАБЛОНІ.]

# Передові практики комунікацій під час кризи кіберпростору

Одним із головних пріоритетів під час кризи кіберпростору є захист цілісності `[кампанії [та/або] партії]`. Найефективніший спосіб досягнення цієї мети полягає в тому, щоб впевнено реагувати, коли інцидент набув, або невдовзі набуде розголосу.

Щоб здійснювати управління інцидентів із впевненістю, політичні організації заздалегідь повинні підготуватися, тренуватися, а також тестувати заходи реагування заздалегідь. У нинішньому динамічному політичному та інформаційному середовищі кожна організація у певний момент імовірно буде вимушена реагувати на кібер-виклики. Незалежно від того, чи це підготовка до кіберінциденту або іншого виду кризової ситуації, цей план допоможе розробити добре продуманий аглоритм дій та реагування. Такі заходи стануть ключовим елементом у наших зусиллях щодо захисту нашої `[кампанії/партії]`.

## Злагодженість комунікацій

> **Встановити керівні принципи для спілкування із зовнішніми сторонами інциденту.** Створити комунікаційний план, який встановлює внутрішні та зовнішні межі для збільшення обсягу інформування про інцидент. Керівні принципи мають визначити особу або групу, що відповідатиме за спілкування з ключовими зовнішніми зацікавленими сторонами – ЗМІ, члени партії та правоохоронні органи. Вони також мають встановити часові рамки для таких комунікацій та ключових осіб, які залучені до комунікацій під час реагування зі складу Групи реагування на кіберінциденти, зокрема представники служби по зв'язкам з громадськістю, юридичні представники, а також вище керівництво або кандидат.

> **Встановити зв'язки між Групою реагування на кіберінциденти та співробітниками з питань комунікації.** Кожна ситуація потребуватиме співробітництва та взаємодії численних членів команд та груп. Відносини між учасниками, а також авторитет кожного з них є життєво необхідними для успішного відновлення ситуації після інциденту.

> **Заохочувати міжпартійну та міжнародну комунікацію та співпрацю.** За можливості розвивати та використовувати сприятливі робочі стосунки з іншими політичними партіями та організаціями з питань кібербезпеки. Сюди можна віднести координацію та обмін інформацією про зовнішні та внутрішні загрози та/або розробку кодексів поведінки або норм щодо використання вкраденої інформації.

## Перспективне планування

| Короткострокове планування | Довгострокове планування |
|---|---|
| • Визначте внутрішні ролі та відповідальність. Переконайтесь, що в рамках `[ОРГАНІЗАЦІЇ]` існує дійсний процес ескалації та потрібні групи спілкуються між собою у випадку виникнення кіберінциденту. Призначте особу, яка буде відповідати за те, щоб забезпечити налагодження та оновлення процесу.<br><br>• Заздалегідь сплануйте реагування на кібер кризу в комунікаційному плані, включаючи протокол прийняття рішень та комунікаційних матеріалів.<br><br>• Регулярно звертайтеся до поточного плану комунікацій під час кризи кіберпростору та аналізуйте прогалини й недоліки у комунікаціях.<br><br>• Переконайтесь, щоб реагування на кіберінциденти стало частиною вашого планування на випадок надзвичайних ситуацій. Переконайтесь, що передбачена резервна система зв'язку на випадок, якщо внаслідок інциденту інфраструктура зв'язку вийде з ладу. | • За можливості проводьте моделювання кризових ситуацій у координації з юридичними, технічними та зовнішніми радниками, включаючи вище керівництво `[ОРГАНІЗАЦІЇ]`.<br><br>• Завчасно приділяйте пріоритетну увагу зацікавленим сторонам та проводьте аналіз репутаційних ризиків для розуміння ваших кібер-ризиків.<br><br>• Інформуйте внутрішні зацікавлені сторони про кіберзагрози та планування і реагування вашої організації.<br><br>• Інформуйте ЗМІ та громадськість через онлайн канали, підготовчі зустрічі, а також публічні заходи з питань стійкості політичної партії або кампанії, а також стосовно поточної роботи щодо пом'якшення наслідків кіберзагроз. |

# Комунікаційне реагування

Реагування на кіберінцидент в деяких ключових питаннях може відрізнятися від реагування на інші види кризових ситуацій. При публічному реагуванні на пов'язаний із виборами кіберінцидент, враховуйте такі передові практики:

## Передові практики комунікацій

**Будьте відкритими, але обережними.** Транспарентність зміцнює довіру, але у випадку кіберінцидента у вас буде небагато фактів під рукою, особливо на початковому етапі. Публічні коментарі мають демонструвати, що ви серйозно ставитесь до проблеми, проте уникайте будь-яких деталей, які можуть змінитися під час подальшого просування розслідування (зокрема, тип та обсяг викраденої інформації), щоб пізніше вам не довелося виправляти себе. Уникайте спекуляцій стосовно винуватця інциденту та завжди будьте чесними щодо інформації, якою ви ділитеся.

**Визначте, чи варто та яким чином здійснювати координацію діяльності з органами державної влади.** Політичні організації, які знаходяться у конфронтації з керівною партією, можуть мати особливі міркування стосовно того, як взаємодіяти з урядом. Однак, важливо розуміти позицію органів влади, які відповідають за розслідування та судове переслідування у зв'язку з кіберзлочинами.

**Зосередьте увагу на заходах, які ви вживаєте для розв'язання проблеми.** Щоб продемонструвати, що ви серйозно ставитесь до проблеми, вам потрібно говорити про заходи, які ви вживаєте для забезпечення захисту інформації кампанії або партії та усунення ширших ризиків, що загрожують системі (напр., яким чином це впливає на виборців або на цілісність виборчого процесу).

**Опишіть контекст ситуації.** Спокуса публічних спекуляцій є неминучою під час кіберінцидента, який пов'язаний із виборами. Протидійте цим спекуляціям за допомогою фактів та контексту, щоб знизити рівень дискредитації в суспільстві. За можливості використовуйте контекст, зокрема хронологію розслідування, щоб продемонструвати усю відповідальність, з якою ви ставитесь до проблеми.

**Використовуйте зовнішніх експертів.** Залучення таких експертів для розслідування та підтвердження ваших заходів допоможе зміцнити авторитет в очах ключових зацікавлених сторін, включаючи ЗМІ. Але будьте обачні, щоб не виникнуло хибне враження, що ці експерти виступають від імені вашої організації – переконайтеся, щоб вони діяли лише як експерти з надання допомоги вашим зусиллям.

**Використовуйте правильні інструменти як цифрові, так і традиційні.** Використовуйте соціальні мережі для спростування чуток. Коли починається кібер-криза, соціальні мережі є найочевиднішим джерелом миттєвої інформації на сьогодні. На практиці це означає, що їх потрібно використовувати вибірково з метою протидії дезінформації та відхиленням. Водночас, важливо визначити альтернативні засоби комунікації на випадок, якщо буде неможливо використовувати облікові записи організації в соціальних мережах.

**Отримуйте досвід від інциденту.** Використовуйте власний та чужий досвід для вдосконалення практики у сфері кібербезпеки та планів заходів у кризових ситуаціях. Проведіть брифінг про виконану роботу, щоб оцінити реагування, визначити передові практики та засвоєний досвід, а також з метою запропонувати наступні заходи вдосконалення.

## Керівні принципи комунікації з громадськістю

**Зосередьтесь на комунікаціях із вашою найголовнішою зацікавленою стороною - громадськістю.** У вас виникне бажання обговорити складові інциденту. Натомість, говоріть про те, що ви робите для задоволення потреб або інтересів громадськості у цій особливій ситуації.

**Говоріть відверто.** Технічні визначення та процеси у сфері кібербезпеки можуть втомити осіб, які не знайомі з вузькою термінологією. При першій-ліпшій можливості використовуйте комічні ситуації та приклади, щоб спростувати всю складність актуальних питань.

**Демонструйте прозорість шляхом систематичного спілкування із громадськістю.** Налагодьте комплекс постіних комунікацій зі ЗМІ та громадськістю стосовно заходів кібербезпеки, яких ви зараз вживаєте з тим, щоб перше спілкування з вами не відбулося під час кризи.

## Передові практики боротьби з дезінформацією

**Встановіть факти та перевірте їх ще раз.** Перш ніж боротися з дезінформацією, переконайтеся, що ви дієте з позиції фактів, тож перевірте їхню правдивість у численних джерелах перед тим, як розголошувати їх публічно. Поставте усі відповідні запитання та попрацюйте перед тим, як виступати, щоб випадково не надати неправдиву інформацію.

**Розробіть простий, точний, короткий контрмеседж.** Підготуйте чітку заяву, яка містить лише факти. Уникайте одночасної передачі багатьох повідомлень та використання складної лексики. Ви можете повідомити про додаткові нюанси згодом.

**Відповідайте швидко.** Дезінформацію можна швидко поширювати через соціальні мережі та коментарі в ефірі. Ваш контрмеседж має бути готовим для розповсюдження в найкоротші терміни. Призначте конкретних членів вашої групи управляти цим процесом, щоб забезпечити найшвидше реагування.

**Будьте відкритими до спілкування.** Застереження, незавершена промова або реакція «без коментарів» можуть підживлювати існування теорії змови, створивши враження, що ваша організація щось приховує. Демонстрація прозорості може допомогти у боротьбі з неправдивими заявами. Можливості продемонструвати відкритість можуть включати запрошення репортерів «за лаштунки» заходу кампанії. Також, якщо вам щось невідомо протягом інтерв'ю або публічної заяви, скажіть журналістам та громадськості, що ви повернетеся до цього питання, коли будете володіти більш детальною інформацією.

**Взаємодійте на всіх платформах.** Дезінформація може поширюватися на численних платформах, включаючи соціальні мережі та традиційні ЗМІ. Для боротьби з дезінформацією, повідомляйте чітку інформацію на усіх доступних платформах, що спирається на правдиві факти. Також, за можливості, координуйте діяльність з прихильниками та партнерами вашої діяльності, щоб поширити ваше повідомлення на їхніх соціальних та традиційних медіа платформах.

**Уникайте повторення неправдивої інформації.** Зосередьте увагу на повідомленні конкретних фактів та уникайте повторення неправдивої інформації або негативних повідомлень. Наприклад, якщо ходять чутки, що кандидат має зв'язки зі злочинними групами, уникайте розмов про те, що чутки про кандидата та його тісні зв'язки взагалі існують. Натомість, ваше повідомлення повинно підкреслювати легітимну діяльність кандидата, зокрема проведення зустрічей з місцевими жителями та вирішення питань, важливих для його або її виборців.

## Передові практики реагування в соціальних мережах

**Оцініть заплановану діяльність у соцмережах.** Оцініть чи необхідно перенести проведення запланованих комунікацій або кампаній у соцмережах, враховуючи ситуацію.

**Використовуйте соцмережі швидко та обачно.** Оскільки соцмережі можуть спричинити непередбачувані наслідки, використовуйте їх, щоб звернути увагу громадськості на вашу заяву з цього питання, яку потрібно відразу розмістити на вашому веб-сайті.

**Слідкуйте за тоном вашого голосу.** Тон комунікацій у соцмережах неформальний, але у випадку кібер-кризи, вам потрібно використовувати більш формальний, заснований на фактах підхід для передачі ставлення вашої організації то ситуації.

**Просувайте ваші пости, якщо це необхідно.** Залежно від обговорень у соцмережах про інцидент, можливо вам потрібно буде оплатити просування ваших публікацій, щоб оминути ці судження.

## Створення груп реагування

Навіть плітка про онлайн атаку, витік даних або проблеми виборчого процесу здатна запустити комунікаційну кризу та посіяти недовіру до виборчого процесу. Позитивними моментом є те, що ви можете заздалегідь виконати роботу з підготовки до такої кризи та створити команду однодумців. Ми не можемо переоцінити, скільки часу це може заощадити при визначенні способів реагування.

Забезпечення координованої процедури налагоджує ефективне та дієве комунікаційне планування та реагування на пов'язаний із виборами кіберінцидент.

### Комунікаційний процес визначає:

- Створення Групи реагування на кіберінциденти (CIRT)
- Створення Групи реагування з питань комунікацій у кіберпросторі (CCRT)
- Поетапне планування та реагування
- Координаційні функції
- Зворотний зв'язок з метою врахування накопиченого досвіду

## Створення Групи реагування на кіберінциденти (ГРК)

Ефективні комунікації потребують від `[ОРГАНІЗАЦІЇ]` ефективного реагування на інциденти в цілому. В свою чергу ефективне регулювання інцидентів вимагає наявності групи для координації реагування організації на цей інцидент. Це реагування виходить далеко за межі комунікацій, проте має інтегрувати керівництво комунікацій в процес. Наступна організаційна структура забезпечить, щоб комунікації стали частиною загального процесу прийняття рішень. Вона формується за найбільш сприятливої ситуації, коли партія забезпечена кадрами та має повноцінне керівництво. Вам слід скоригувати структуру, щоб вона відповідала ресурсам вашої організації.

Заходи реагування на кіберінциденти за можливості повинні враховувати процеси, які `[ОРГАНІЗАЦІЯ]` вже має для негайного реагування на інші пов'язані з виборами кризові ситуації. Це керівництво може надати допомогу в організації процесу, якщо плану реагування на кризові ситуації все ще не існує. Воно має вносити коригування у випадку

конкретних відмінностей, пов'язаних із кібер втручанням – зокрема ключового залученого персоналу та можливості будь-якого інциденту отримати резонанс, а також піднімати питання цілісності виборчого процесу в цілому.

[ЛІДЕР ОРГАНІЗАЦІЇ] несе відповідальність за консультування та приведення в дію плану реагування на кіберінциденти [ОРГАНІЗАЦІЇ]. Вам слід мати уповноважених осіб, які знаходяться в резерві та можуть прийняти рішення чи активувати план. Кожна уповноважена особа повинна мати необхідну контактну інформацію та дотримуватися цієї послідовності.

У випадку значного кіберінциденту – наприклад, витоку даних, який може вплинути на результати виборів - уряд або орган з управління виборчим процесом може вимагати тимчасового зупинення, відкладення або перенесення голосування у надзвичайній ситуації, використовуючи постанову суду, законодавчі заходи або надзвичайні повноваження уряду.

[ТУТ ВИКЛАДІТЬ ПОЗИЦІЮ ОРГАНІЗАЦІЇ ЩОДО ВАРІАНТІВ, ЯКІ ЗАСТОСОВУЮТЬСЯ У ВИПАДКУ, ЯКЩО КІБЕРІНЦИДЕНТ ЗРИВАЄ ВИБОРЧИЙ ПРОЦЕС АБО РЕЗУЛЬТАТИ ВИБОРІВ]

Важливо регулярно оновлювати цю таблицю в рамках щорічного аналізу плану.

[Примітка: таблиця, викладена нижче, служить відправною точкою та має бути адаптована до структури вашої організації.]

| Посада | Уповноважена особа та контактна інформація | Резервна уповноважена особа та контактна інформація |
|---|---|---|
| **Лідер організації** | | |
| **Комунікації та зовнішні контакти** | | |
| **Керівник служби безпеки** | | |
| **Керівник відділу інформаційних технологій** | | |
| **Юридична допомога** | | |
| **Зв'язки з державними органами та громадськістю** | | |

*Примітка: Організаціям необхідно адаптуватися відповідно до власної структури. У певних випадках для деяких організацій може бути доцільним залучити джерела зовнішньої підтримки для інформаційної безпеки та досліджень. Також, в менших за обсягом організаціях може бути залучена одна особа для виконання багатьох функцій.*

**Лідер організації –** відповідальний за координацію реагування на кібер-кризу в `[ОРГАНІЗАЦІЇ]`. Залежно від ситуації, цю функцію ймовірно має виконувати та сама особа, яка виконує функцію керівника Групи реагування з питань комунікацій у кіберпросторі (CCRT) (буде розглянуто нижче).

**Комунікації та зовнішні контакти -** Відповідальний за координацію комунікацій під час реагування на кібер-кризу в `[ОРГАНІЗАЦІЇ]`. Залежно від ситуації, цю функцію ймовірно має виконувати та сама особа, яка виконує функцію Комунікаційного директора в Групі реагування з питань комунікацій у кіберпросторі (CCRT) (буде розглянуто нижче).

**Керівник служби безпеки –** Відповідальний за інформаційну безпеку організації.

**Керівник відділу інформаційних технологій –** Відповідальний за координацію IT потреб організації, включно з обладнанням.

**Юридична допомога –** Відповідальний за правовий аспект будь-якого кіберінциденту, особливо стосовно інцидентів із використанням конфіденційної інформації або інформації, яка є підставою для виникнення зобов'язання щодо надання звітності.

**Зв'язки з державними органами та громадськістю –** Відповідальний за взаємодію з державними установами (такими як правоохоронні органи), коли це необхідно і доцільно. Також відповідальний за інформування ключових внутрішніх та зовнішніх зацікавлених сторін.

## Створення Групи реагування з питань комунікацій у кіберпросторі (CCRT)

Ваша Група реагування з питань комунікацій у кіберпросторі надаватиме підтримку `[Керівнику з питань комунікацій]`, якого закріплено за Групою екстреної готовності до інцидентів у сфері кібербезпеки (CIRT). Нижче описані заходи, які ви можете вжити з метою переконатися, що ваша Група реагування з питань комунікацій у кіберпросторі (CCRT) має необхідних для цього людей. `[ОРГАНІЗАЦІЯ]` повинна запровадити наступні посади для реагування на кіберінцидент:

*Примітка: Організаціям необхідно адаптуватися відповідно до власної структури. У певних випадках для деяких організацій може бути доцільним залучити джерела зовнішньої підтримки для інформаційної безпеки та досліджень. Або в рамках менших організацій може бути залучена одна особа для виконання багатьох функцій.*

- **Керівник політичної організації —** відповідає за координацію комунікаційної інформації з [ПОСАДОЮ] в `[ОРГАНІЗАЦІЇ]`.
- **Директор з інформаційних технологій/CIO —** відповідає за IT системи `[ОРГАНІЗАЦІЇ]` та безпеку цих систем.
- **Комунікаційний директор —** здійснює нагляд за функціональними координаційними ресурсами, процесами та персоналом для здійснення комунікацій в `[ОРГАНІЗАЦІЇ]`. Відповідає за загальне оперативне керівництво та розвиток процесу поширення комунікаційної інформації у співробітництві та взаємодії з ключовими внутрішніми та зовнішніми зацікавленими сторонами.
- **Постраждалі місцеві афілійовані особи —** це зазвичай посадові особи місцевої партії або організації із зон ураження кібератакою, які представляють позицію «на місцях» та надають інформацію стосовно інциденту для координації.
- **Директор з питань роботи зі ЗМІ —** відповідає за комунікацію зі ЗМІ та медіа моніторинг. Здійснює нагляд за короткостроковою цілодобовою комунікаційною діяльністю, тобто за виконанням комунікаційних планів.
- **Директор з питань комунікаційних планів —** відповідає за перспективні комунікаційні плани, які виходять за межі найближчого цілодобового періоду.
- **Співробітник з питань законодавчої взаємодії та взаємодії у сфері міжурядових відносин —** відповідальний за координацію урядових брифінгів для обраних посадових осіб. Наприклад, для політичної партії взаємодія може передбачати проведення брифінгів для членів парламенту від партії.
- **Співробітник з питань взаємодії із правоохоронними органами —** відповідальний за координацію комунікаційної інформації з правоохоронними органами та афілійованими комунікаторами.
- **Співробітник з питань технічної взаємодії —** відповідальний за виконання функції провідника технічної інформації між оперативною та комунікаційною групами. Забезпечує точність технічних даних, які оприлюднюються комунікаційною групою та виступає як профільний експерт з подібної інформації.

## Перелік членів Групи реагування з питань комунікацій у кіберпросторі

| Посада | Уповноважена особа | Резервна уповноважена особа |
|---|---|---|
| **Керівник політичної організації** | | |
| **Директор з інформаційних технологій/CIO** | | |
| **Комунікаційний директор** | | |
| **Постраждалі місцеві афілійовані особи** | | |
| **Директор з питань роботи зі ЗМІ** | | |
| **Директор з питань комунікаційних планів** | | |
| **Співробітник з питань законодавчої взаємодії та взаємодії у сфері міжурядових відносин** | | |
| **Співробітник з питань взаємодії із правоохоронними органами** | | |
| **Співробітник з питань технічної взаємодії** | | |

## Координація комунікацій під час інциденту:

Впорядкуйте найкращі канали комунікації. Визначте додаток чи технологію, за допомогою якого ви будете здійснювати комунікацію, якщо вам здалося, що кіберзлочинці порушили цілісність вашої системи. Наприклад, якщо зламали вашу електронну скриньку, вам необхідно використовувати безпечну систему для передачі повідомлень, таку як «Signal» або «Wick». Комунікація під час несанкціонованого проникнення є необхідною, проте ви б не бажали, щоб кіберзлочинц володіли інформацією із ваших розмов – про вжиті заходи проти їхніх дій. Комунікаційна команда реагування складатиме список відповідних контактів з головного офісу, місцевих підрозділів та афілійованих організацій, а також упорядковуватиме список урядових контактів з метою проведення зустрічі із відповідними сторонами або здійснення телефонної розмови, якщо це необхідно.

[ТУТ ОРГАНІЗАЦІЯ МАЄ ВКАЗАТИ ТЕХНІЧНІ ДЕТАЛІ]

# Процес комунікаційного реагування

Такі кроки допоможуть вам створити Групу реагування з питань комунікацій у кіберпросторі та розробити процедуру написання та затвердження повідомлень. Якщо не достатньо ресурсів для здійснення усіх цих кроків, зосереджуйте увагу на найдешевших заходах та таких, що матимуть найбільший ефект: Кроки 1, 3, 4 та 5.

**Крок 1: Прийміть рішення щодо своєї команди.** Оберіть осіб, які відповідатимуть за перераховані вище завдання. Опишіть їхні функції та визначте рішення щодо поширення інформації та здійснення комунікацій, які вони зможуть приймати у реальному часі.

**Крок 2: Розробка безпеки.** Разом з IT групою або групою безпеки чи довіреним підрядником проведіть інвентаризацію своїх даних та потенційних ризиків, а також проведіть оцінку впливу на них. Ви повинні розуміти природу інцидентів, до яких ви найбільш вразливі. Також, слід розуміти як тактика безпеки пов'язана з управлінням ризиками. Процес раннього моніторингу та функції виявлення повинні приводитись у відповідність до найбільш важливих даних організації, зокрема до бази даних донорів та членів партії, письмової кореспонденції, або історії дотацій. Встановіть, хто відповідатиме за IT взаємодію із Групою реагування з питань комунікацій у кіберпросторі (CCRT).

**Крок 3: Злагодженість дій щодо розголошення інформації.** Визначте та задокументуйте, що саме ви зобов'язані розголошувати. Розробіть процедуру прийняття рішень для проведення оцінки громадської позиції – проактивної чи пасивної – якою ви користуватиметеся у різних випадках. Звертайте увагу як на правові наслідки, так і на громадську думку.

**Крок 4: Аналіз зацікавлених сторін.** Оцініть та визначте пріоритетність ключових зацікавлених сторін на основі їхнього впливу на виборців, адже громадська думка може швидко змінитися протягом кризи кібербезпеки. Впорядкуйте постійні відносини з цими зацікавленими сторонами ДО настання кризи. Вашими зацікавленими сторонами можуть бути:

- Виборці
- Члени партії
- Виборчі органи
- Виборчі моніторингові групи
- Правоохоронні органи
- Законодавці
- ЗМІ (спеціалізовані журналісти у сфері кібербезпеки та політики)
- Інші політичні партії та кампанії
- Ініціативні групи третіх сторін

**Крок 5: Оберіть речника або речників.** Заздалегідь вирішіть, хто буде виступати від імені `[ОРГАНІЗАЦІЇ]` під час кіберінциденту, а також переконайтеся, що вони отримали підготовку в сфері роботи зі ЗМІ. Ви можете обрати різних речників для різної аудиторії. Наприклад, ваш IT керівник може мати ширші можливості для опублікування відповіді на сайті підрядника або усунення проблем із технічними засобами, коли `[ЛІДЕР ОРГАНІЗАЦІЇ]` або Комунікаційний директор може стати найкращою кандидатурою для спілкування зі ЗМІ. Враховуйте фактори, зокрема хто володіє найкращими комунікативними навичками, має досвід роботи зі ЗМІ, повноваження в організації, а також зв'язки із зацікавленими сторонами.

**Крок 6:Впорядкуйте процедуру написання та затвердження ключових повідомлень та використайте схему цієї процедури у своєму комунікаційному плані.** Така процедура буде характерною для структури Групи реагування з питань комунікацій у кіберпросторі (CCRT) `[ОРГАНІЗАЦІЇ]`, але вона спиратиметься на базовий план, адаптований до вашої організаційної структури:

> `[ВСТАВТЕ ПРОЕКТ СТРУКТУРИ ОРГАНІЗАЦІЇ]`

**Крок 7: Прийміть рішення, яку основну інформацію ви зможете повідомити зараз.** Налагодьте вихідне розуміння між ключовими зацікавленими сторонами щодо роботи `[ОРГАНІЗАЦІЇ]` у реалізації найкращих практик кібербезпеки задовго до наступних виборів. У випадку кібер ситуації, такі зусилля допоможуть підтвердити, що `[ОРГАНІЗАЦІЯ]` впроваджувала передові практики, але, на жаль, інциденти все ще інколи трапляються.

**Крок 8: Налагодьте зворотний зв'язок.** Створіть механізм — як протягом, так і після інциденту — для врахування зауважень виборців та інших ключових зацікавлених сторін у вашому реагуванні. Протягом інциденту, така робота може здійснюватися у формі медіа моніторингу або моніторингу соцмереж, а також проведення опитувань. Після інциденту вам слід подати звіт про виконану роботу та впевнитись, що ви внесли результати отриманого досвіду в цей шаблон комунікацій у кіберпросторі. Ваш звіт повинен охоплювати:

- Резюме інциденту (зважаючи, що воно може підлягати публічному розголошенню);
- Огляд оперативного реагування;
- Завдання комунікацій;
- Розбивку по етапах з конкретизацією:
  - завдання
  - результат
  - рекомендації

# Залучення Групи реагування з питань комунікацій у кіберпросторі (CCRT)

Пов'язані з виборами кіберінциденти відрізняються за обсягом та серйозністю, що зумовлює необхідність класифікації необхідних кроків відповідно до важливості ситуації. Отже, вам слід кваліфікувати усі інциденти згідно з одним із таких рівнів тяжкості:

1. **Низький:** Кіберінцидент, який не пов'язаний з ідентифікувальною персональною інформацією (PII) та/або включає незначні порушення в роботі системи, які, ймовірно, не будуть помітними для громадськості або не вплинуть на виборчий процес.
2. **Середній:** Кіберінцидент, який стає причиною втрати даних або ставить під загрозу дані виборців, але це не слугує підставою для виникнення зобов'язань надавати офіційне повідомлення. Проблема набуває розголосу.
3. **Високий:** Кіберінцидент, який є підставою для виникнення зобов'язань щодо надання звітності; стосується великого обсягу інформації щодо виборців та/або має руйнівні наслідки для діяльності організації.

При середньому за інтенсивністю інциденті `[ЛІДЕРУ ОРГАНІЗАЦІЇ]` потрібно прийняти рішення про те, чи варто залучати Групу реагування з питань комунікацій у кіберпросторі (CCRT), але якщо ситуація, імовірно, набуде розголосу та поставить під сумнів довіру до виборчих систем, `[ЛІДЕР ОРГАНІЗАЦІЇ]` зобов'язаний вважати на цей варіант. Ви завжди зможете припинити цей процес, якщо напруженість буде зменшуватися. Після залучення Групи реагування `[ЛІДЕР ОРГАНІЗАЦІЇ]` прийме рішення, який рівень тяжкості слід брати до уваги, ґрунтуючись на первинній оцінці ситуації.
Щойно `[ЛІДЕР ОРГАНІЗАЦІЇ]` залучить Групу реагування з питань комунікацій у кіберпросторі (CCRT), усім основним членам групи реагування буде повідомлено про це рішення. `[ВСТАВТЕ СПОСІБ ЗВ'ЯЗКУ ОРГАНІЗАЦІЇ З ЧЛЕНАМИ ГРУПИ]`.

## Злагодженість комунікацій

Щойно ви обрали найкращий спосіб здійснення комунікації для пов'язаних із виборами інцидентів, цей засіб комунікації може стати ключовим механізмом для забезпечення координації обміну оперативними даними, а також координації передачі повідомлень і комунікаційну діяльність.

При залученні Групи реагування з питань комунікацій у кіберпросторі (CCRT), `[Комунікаційний директор]` попередить групу про використання необхідної технології зв'язку для безпечної комунікації з групою. Це звернення може включати представників постраждалих громад, а також перелічених вище посадових осіб Групи реагування з питань комунікацій у кіберпросторі (CCRT), та будь-яких інших учасників цієї групи або зовнішніх радників із відповідним експертним досвідом.

Під час скликання зборів порядок денний може мати звичну структуру:

- Перевірка присутності
- Вступне слово [Комунікаційного директора]
- Коротке оперативне зведення (ситуативні повідомлення або дії)
- Короткий виклад основних комунікаційних планів і заходів та коментарі запрошених осіб
- Вимоги щодо системи передачі повідомлень
- Висновки та майбутні заходи

Примітка: Якщо ваша організація має поточні координаційні процеси, які є ефективними під час обміну та координації інформації, – регулярні сповіщення, безпечний обмін повідомленнями у групі, сервери розсилки повідомлень, **–** продовжуйте користуватися ними, особливо до початку вжиття заходів, або на їхньому початковому етапі. Однак, масштаб та обсяг інциденту може спричинити здійснення прямих комунікацій через систему «Signal», що буде більш безпечним способом комунікації.]

# Комунікаційний процес у випадку кіберінциденту

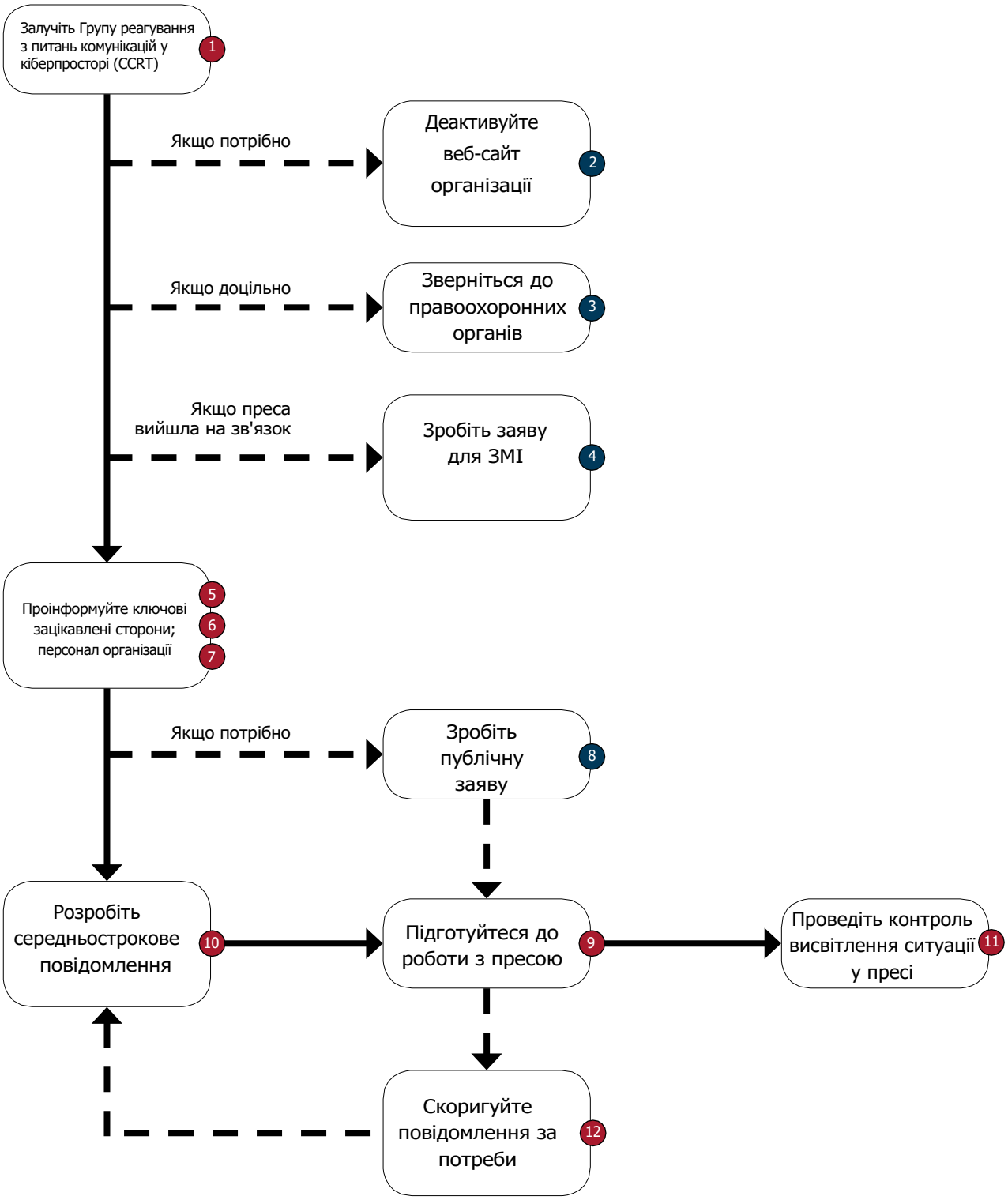
**Якщо виникає кіберінцидент, він вимагатиме створення власного комунікаційного плану.** Описані нижче кроки допоможуть вам оцінити ситуацію та вжити основних заходів паралельно із розробкою більш детального комунікаційного плану. Вам слід оцінити кожний захід щодо своєї суті, перш ніж реалізовувати конкретну стратегію на практиці. Загальні керівні принципи:

- **Крок 1**: Залучайте Групу реагування з питань комунікацій у кіберпросторі (CCRT) та отримайте технічний брифінг від Директора з інформаційних технологій (CIO) або Співробітника з питань технічної взаємодії.
- **Крок 2**: Якщо необхідно, вирішіть чи потрібно закривати веб-сайт `[ОРГАНІЗАЦІЇ]` та, консультуючись з IT спеціалістами, вирішіть чи потрібно вам запустити окремий веб-сайт або використовувати облікові записи організації у соцмережах для зовнішніх комунікацій. Це рішення має прийняти `[ЛІДЕР ОРГАНІЗАЦІЇ]`. Проінформуйте ключових працівників. Якщо веб-сайт залишається активним, можливо, буде необхідно опублікувати повідомлення про ситуацію.
- **Крок 3**: Якщо це необхідно та можливо, повідомте правоохоронні органи або інші органи влади.
- **Крок 4**: Якщо ЗМІ зателефонують або приїдуть в офіс, Група реагування з питань комунікацій у кіберпросторі (CCRT) повинна відповісти на всі запитання журналістів. За потреби, ви можете зробити заяву, яка охоплює попередній коментар для відповіді на запитання громадськості. Це продемонструє, що ви займаєтесь вирішенням інциденту, але вам не потрібно надавати усіх подробиць.
- **Крок 5**: Повідомте ключових осіб з вашої Групи реагування з питань комунікацій у кіберпросторі
- **Крок 6**: Проінформуйте організацію про розвиток кризи, реагування організації, а також про політику, яку використовує організація.
- **Крок 7**: Проінформуйте зацікавлені сторони.
- **Крок 8**: Якщо ви ще не зробили цього, подумайте, чи варто вам проінформувати ЗМІ/громадськість про інцидент. Переконайтесь, що ви повідомили ЗМІ виключно підтверджені факти, в незмінності яких ви впевнені (дуже мало фактів підпадуть під цю категорію).
- **Крок 9**: Почніть контролювати висвітлення ситуації у ЗМІ/соцмережах.
- **Крок 10**: Розробіть середньострокові повідомлення.
- **Крок 11**: Підготуйтеся до роботи з пресою/брифінгу та медіа плану.
- **Крок 12**: Налагодьте зворотний зв'язок від моніторингу ЗМІ/соцмереж або опитування та прохань, що надходять від ЗМІ з метою визначити, чи потрібно вам вносити зміни у свої повідомлення.

Примітка: Цифри у таблиці на наступній сторінці відповідають зазначеним вище крокам.

# Комунікаційний процес у випадку кіберінциденту

Цифри відповідають послідовним крокам, які зазначено на попередній сторінці



# Комунікаційні контрольні переліки у сфері координації

## Контрольні переліки у сфері комунікацій у кризових ситуаціях під час виборів

Кібер-криза потенційно може виставити `[ОРГАНІЗАЦІЮ]` у негативному світлі, а також підірвати довіру до виборчих систем. Якщо ви не впевнені, чи може ситуація перейти у кризу, віддайте перевагу залученню груп реагування, оскільки ви завжди можете припинити їхнє втручання, коли ескалація інциденту не відбулася. (Якщо це відбулося, зверніться до Плану безперервного функціонування `[ОРГАНІЗАЦІЇ]` – під час кризи це впливає на всю її діяльність).

Контрольні переліки можна адаптувати до процедур вашої юрисдикції. Вони надають керівні вказівки щодо заходів, які потрібно вживати за декілька днів до та після виникнення кіберінциденту.

### Захід: До виникнення кібер-кризи

- ☐ Визначте протокол діяльності та членів Групи реагування на кіберінциденти (CIRT) і Групи реагування з питань комунікацій у кіберпросторі CCRT. (До складу повинен входити IT персонал).
- ☐ Створіть перелік термінів загальної номенклатури кіберінциденту для їхнього використання усіма зацікавленими сторонами.
- ☐ Розробіть внутрішній комунікаційний план для ключового персоналу. (Як часто, коли та де буде зустрічатися персонал)  Інформація повинна поширюватися згідно з нормами субординації, з чіткими межами щодо розповсюдження та взаємодії з громадськістю/ЗМІ).
- ☐ Переконайтесь, що під час кризи зі всіма зацікавленими сторонами можна зв'язатися без доступу до мережі `[ОРГАНІЗАЦІЇ]`, включно зі смартфонами.
- ☐ Де можливо та доцільно, налагодьте контакти з державними агентствами, які відповідають за забезпечення кібербезпеки кампаній. Також, заздалегідь ознайомтесь із юридичними зобов'язаннями стосовно персональних та/або конфіденційних даних, якими володіє організація.
- ☐ Налагодьте контакт з вашими постачальниками технологій стосовно потенційних загроз та переконайтесь, що їм відомі функції технічної підтримки та доступні функції з підтримки політики.

- ☐ Проводьте брифінги для членів ЗМІ.
- ☐ Верифікуйте ваші облікові записи в соцмережах, оскільки це забезпечить пріоритетний доступ до гарячих ліній у випадку, якщо ваш профіль під загрозою. Використовуйте соцмережі, щоб показати процес підготовки, який проводить ваша організація.
- ☐ Підвищуйте обізнаність щодо тактики, яка використовується у дезінформаційних кампаніях.
- ☐ Підготуйте матеріали для комунікації, які можна використати під час потенційного кіберінциденту, включаючи повідомлення у соцмережах.
- ☐ Переконайтесь, що персонал розуміє свої функції під час кіберінциденту. Для тих, хто не має конкретного завдання, проведіть роз'яснення щодо важливості їхньої роботи та проінформуйте їх, яким чином вони зможуть продовжувати виконувати свою роботу в той час, коли уповноважені менеджери займаються кіберінцидентом.
- ☐ Переконайтесь у тому, що є доступ до комунікаційних планів та що їх регулярно оновлюють.

## Захід: До того моменту, як про кіберкризу стане відомо громадськості

- ☐ Забезпечте проведення технічного брифінгу. (Оцініть та перевірте всю інформацію)
- ☐ Прийміть рішення, чи потрібно залучати Групу реагування з питань комунікацій у кіберпросторі (CCRT).
- ☐ Вирішіть, чи можуть веб-сайт та облікові записи соцмереж залишатися в онлайн режимі. Якщо ви змушені їх деактивувати, запустіть замість них мікросайт (розміщений в іншій мережі).
- ☐ Якщо існує потенційна загроза для електронної пошти, використовуйте зовнішній канал комунікацій, такий як безпечний додаток для обміну повідомленнями повного шифрування («Signal» або «Wickr»).
- ☐ У разі потреби проконсультуйтеся з органами влади.
- ☐ Проведіть внутрішнє засідання у центральному залі засідань; встановіть внутрішній графік комунікацій.
- ☐ Визначте обов'язки та відповідальність Групи реагування з питань комунікацій у кіберпросторі (CCRT), якщо ви ще цього не зробили.
- ☐ Визначте та ідентифікуйте відповідні зацікавлені сторони для реагування на інцидент.
- ☐ Визначте широку комунікаційну стратегію.
- ☐ Підготуйте заяву на основі раніше підготовлених формулювань. [ДИВ. СТОРІНКУ № ШАБЛОНУ МОВИ, ЯКИЙ ВИ РОЗРОБИТЕ НИЖЧЕ У ДОКУМЕНТІ]
- ☐ Розробіть план комунікацій.

- ☐ Підготуйте додаткові комунікації, необхідні для виконання плану, зокрема послідовний комунікаційний план (включає комунікації зі ЗМІ, зацікавленими сторонами та співробітниками).
- ☐ Підготуйте план для моніторингу традиційних медіаджерел та соцмереж.
- ☐ Створіть протокол медіа реагування.
- ☐ У разі потреби проінформуйте співробітників `[ОРГАНІЗАЦІЇ]`. Цілком можливо, що спочатку лише невелика група працівників буде проінформована. Якщо потрібно, здійснюйте комунікацію в межах організації.
- ☐ Проінформуйте зацікавлені сторони (Див. перелік на наступній сторінці) та забезпечте надійну підтримку своїй організації.
- ☐ Розпочніть медіа моніторинг (традиційних джерел та соцмережі).

## Захід: Коли про кіберкризу стало відомо громадськості

- ☐ Перевірка фактів: Переконайтесь, що комунікаційні матеріали надають поточні факти.
- ☐ Виконайте послідовний план, включаючи інформування ЗМІ, якщо це доцільно.
- ☐ Визначте, чи потрібно створювати окремий мікросайт/вебсторінку.
- ☐ Запишіть офісне привітання для телефонної системи, у разі потреби.
- ☐ Ведіть список вхідних медіа-запитів та відповідей. `[ДОДАЙТЕ ЕЛЕМЕНТИ ДО ІНФО ФОРМИ ЗВОРОТНЬОГО ЗВ'ЯЗКУ, РОЗМОВИ З ЖУРНАЛІСТАМИ ТА ІНШУ ІНФОРМАЦІЮ ЩОДО ЗОВНІШНЬОГО РЕАГУВАННЯ]`
- ☐ Продовжуйте медіа моніторинг (традиційні джерела та соцмережі).
- ☐ Якщо потрібно, проаналізуйте та перегляньте повідомлення із врахуванням відгуків.

# Контрольний перелік загальних медіа запитів

## Зберіть базові факти:

- ☐ Тема повідомлення/точка зору/кінцева дата
- ☐ Платформа (блог, газета, телебачення або радіо) плюс зміст запиту та зображення
- ☐ Інші потенціальні теми інтерв'ю
- ☐ Пам'ятайте: Лише уповноважені речники мають виступати або надавати інформацію.
- ☐ Пам'ятайте: Ви маєте певні права при спілкуванні з журналістами, особливо коли вони запитують про технічні деталі, які їм не потрібно знати на цьому етапі. «Дозвольте мені зрозуміти ситуацію, щодо якої я можу вам дати відповідь» – це можливий варіант відповіді. Він може означати, що ви зможете повернутися до питання журналіста без будь-якої додаткової інформації. Ви не зобов'язані повідомляти усі деталі ситуації.
- ☐ Пам'ятайте: На журналістів здійснюється тиск, щоб вони вчасно підготували репортаж, тож вони можуть спрямувати його на вас. Не спекулюйте тим, що ви виконаєте їхнє завдання замість них.

## Проінформуйте ключових осіб:

- ☐ Проводьте внутрішні зустрічі.
- ☐ Складіть медіа план. Внесіть планування здійснення комунікації з персоналом та зацікавленими сторонами.
- ☐ Надайте повноваження речникам та контент-провайдерам. Призначте завдання.
- ☐ Надайте допомогу при написанні повідомлень. Охарактеризуйте ключову аудиторію, осіб, які наразі постраждали, та тих, хто постраждає у майбутньому.
  - ☐ Виборці
  - ☐ Члени та співробітники партії
  - ☐ ЗМІ
  - ☐ Урядові заклади
  - ☐ Вендори
  - ☐ Громадськість
- ☐ Продемонструйте лідерство, описуючи кроки, які ви вживаєте для вирішення кіберінциденту. Розгляньте ймовірність налагодження контактів із зацікавленими сторонами, які можуть постраждати в результаті виникнення кіберінцидентів, особливо, якщо їм не сподобаються, або вони будуть незгодні із вашими повідомленнями.

# Загальні ключові повідомлення та базові комунікації

Нам потрібно забезпечити базове розуміння громадськості, що [ОРГАНІЗАЦІЯ] відповідальна у своєму ставленні до кіберінциденту та впроваджує передові практики у виборчий процес. Нижче [наведено один (або більше)] зразок (зразки) цих основних комунікацій. Також, додатково до постійного сайту та повідомлень у соцмережах, розробіть ключові повідомлення стосовно діяльності [ОРГАНІЗАЦІЇ] із забезпечення готовності до кіберінцидентів та інтегруйте їх до наявного онлайн контенту й майбутніх публічних висловлювань лідерів [ОРГАНІЗАЦІЇ].

Нижче наведено зразок основних комунікацій. Додайте відповідні додаткові сопособи комунікації для вашої організації.

## Зразок повідомлення на веб-сайті, що наголошує на кібербезпеці

[ВСТАВТЕ ЗАГАЛЬНЕ ПОВІДОМЛЕННЯ ВІД ПОЛІТИЧНОЇ ПАРТІЇ ПРО КІБЕРБЕЗПЕКУ.]

## Основні типи комунікаційних матеріалів

Наступні матеріали можуть використовуватись протягом будь-якої кібер кризи під час виборів:

**Ключова стандартна заява:** Ключова стандартна заява є загальним засобом реагуванням, яка передається ЗМІ або іншим зацікавленим сторонам. Така заява не надаватиме детальну інформацію, проте підкреслюватиме, що ваша організація наразі розслідує кіберінцидент та працює з метою відновити свою діяльність після нього. Оскільки згадана заява написана та сформульована до настання кризи, у вас є можливість внести усі можливі доповнення у разі виникнення необхідності.

**Ключові повідомлення**: Основа для всіх внутрішніх та зовнішніх комунікаційних матеріалів протягом інциденту. Цей документ є лише джерелом інформації, який повинен слугувати написанню медіа заяв, запитань та відповідей, копій веб-сайту та соцмереж, електронних скриньок працівників та інших комунікаційних матеріалів. Коли нова інформація стає доступною, ключові повідомлення слід, зокрема, оновлювати та розповсюджувати між відповідними посадовими особами.

**Контрольні запитання та відповіді:** Запитання та відповіді слід використовувати тим, хто займається роботою із представниками ЗМІ та іншими зацікавленими сторонами. Цю інформацію потрібно оновлювати та розширювати паралельно із перебігом конкретних подій або серії запитань, а також коли стає відомо більше деталей про інцидент.

## Загальні проекти стандартної заяви і контрольних запитань та відповідей

Проекти стандартної заяви та контрольних запитань та відповідей слугуватимуть основою для комунікацій щодо будь-якого пов'язаного з виборами або кампанією/партією кіберінциденту. Їх можливо використати як проміжні повідомлення, під час того як збираються додаткові факти. Відповіді на контрольні запитання та звичайні відповіді можна використовувати у поєднанні зі специфічними для конкретних сценаріїв запитаннями та відповідями.

## Загальна Стандартна заява під час кіберінциденту

[ВСТАВТЕ МОВУ ШАБЛОНА, ЯКУ МОЖНА АДАПТУВАТИ ПРИ ВИНИКНЕННІ ЗАГАЛЬНОГО ПОВ'ЯЗАНОГО З ВИБОРАМИ КІБЕРІНЦИДЕНТУ. ВІН ПОВИНЕН ВКЛЮЧАТИ ПІДТВЕРДЖЕННЯ ТОГО, ЩО ВИ РОЗСЛІДУЄТЕ ПОТЕНЦІЙНИЙ КІБЕРІНЦИДЕНТ, ЩО ВИ СПІВПРАЦЮЄТЕ ІЗ ПОВАЖНИМИ ЗОВНІШНІМИ ЕКСПЕРТАМИ ТА, ЯКЩО НЕОБХІДНО, З ОРГАНАМИ ВЛАДИ. ТАКОЖ У НЬОМУ МОЖНА ЗАЗНАЧАТИ ОБМЕЖЕНІ ПОДРОБИЦІ ТОГО, ЩО ТРАПИЛОСЯ, ТІЄЮ МІРОЮ, ЩОБ ВОНИ СТАЛИ НЕОБХІДНИМИ ДЛЯ ЗБЕРЕЖЕННЯ ГРОМАДСЬКОЇ ДОВІРИ ДО ВИБОРЧОГО ПРОЦЕСУ/
СИСТЕМ. ЯКЩО МОЖЛИВО, ЗАЗНАЧТЕ ЗАХОДИ, ВЖИТІ ДЛЯ РОЗВ'ЯЗАННЯ ПРОБЛЕМИ.]

## Контрольні запитання та відповіді

[ВНЕСІТЬ ОЧІКУВАНІ ЗАПИТАННЯ, ЯКІ ВИ ОТРИМАЄТЕ ВІД НИЗКИ ЗАЦІКАВЛЕНИХ СТОРІН З ВІДПОВІДЯМИ, НАПИСАНИМИ ІЗ ВИКОРИСТАННЯМ КЛЮЧОВИХ ПОВІДОМЛЕНЬ.]

# Сценарії

Метою цього розділу є допомогти організаціям спрогнозувати різні потенційні сценарії, які вимагатимуть комунікацій під час реагування на кібер-кризу. Реагування буде варіюватись залежно від специфіки інциденту, проте планування сценаріїв, а також тренування комунікаційного реагування допоможе організаціям визначити особливі моменти та розробити загальні матеріали, які можуть бути модифіковані, якщо цього потребуватимуть обставини.

## Складові сценарію

Для кожного сценарію розробіть такі матеріали реагування:

- **Стандартна заява:** Шаблон реагування для ЗМІ та інших зацікавлених осіб на випадок, якщо стане відомо про кіберінцидент та буде потрібна негайна реакція.
- **Конкретні питання та відповіді:** Очікувані питання та шаблони відповідей, характерних для цього сценарію, які випливають зі стандартної заяви та відповідають ключовим повідомленням.
- **Ключові повідомлення**: Виділяє аналогічну зі стандартною заявою інформацію, що полегшує кероване обговорення конкретних ситуацій у кіберпросторі.
- **Зразок Tweet:** Зразок публікації Tweet, який можна адаптувати до інших публікацій у соцмережах.
- **Комунікації з іншими зацікавленими сторонами:** Комунікації, розроблені для інших зацікавлених сторін, зокрема партнерів в інших партіях або країнах.

## Зразки сценаріїв

Організаціям слід розглядати типи сценаріїв, які можуть статися з найбільшою ймовірністю або які можуть мати найбільший вплив.

ПРИМІТКА: Далі наводяться можливі сценарії, а також рекомендації у дужках щодо того, яким чином наблизитися до реагування. Цей шаблон не містить зразків матеріалів реагування (стандартних заяв, питань та відповідей тощо), оскільки вони широко відрізняються в залежності від організацій. Організації мають розробити ці матеріали та включити їх до планування сценаріїв.]

## Сценарій 1: Загроза зсередини

Співробітник вашої організації з привілейованим доступом до конфіденційних матеріалів, включаючи документи з політичних стратегій, компромат, особисті справи персоналу, а також інші матеріали, розчаровується в організації. Співробітник публікує матеріали онлайн.

> **Можливе реагування:** Реагування повинно визнати, що ваша організація стала жертвою зловмисного кіберінциденту, але має уникати описання масштабів витоку або детального обговорення будь-яких документів. Повне розслідування інциденту займе певний час, тож будь-яка заява щодо розміру проблеми може згодом виявитися хибною.
> Нагадайте пресі, що ці документи були викрадені зловмисниками з прихованими намірами. Ви також можете розглянути шляхи оновлення та, якщо можливо, переконання прихильників вашої організації.

## Сценарій 2: Атака на облікові записи соцмереж

Ваша організація використовує соцмережі як головний засіб зв'язку зі своїми прихильникам. Не зважаючи на ваші найкращі запобіжні заходи, зловмисники заволоділи доступом до ваших облікових записів у соцмережах (напр. Facebook або Twitter) та публікують пости, направлені на те, щоб відштовхнути ваших прихильників.

> **Можливе реагування:** Ваша первинна заява повинна ідентифікувати облікові записи, які опинилися під загрозою, та перенаправити підписників на інше надійне джерело. Для відновлення доступу до вашого облікового запису може знадобитися деякий час, тож використовуйте всі інші канали – зокрема телебачення, радіо, а також облікові записи в інших соцмережах – для поширення вашого повідомлення. Не спекулюйте особистістю або мотивами зловмисника, який поставив під загрозу обліковий запис; передчасна інформація може бути неточною.

## Сценарій 3: Втручання у висвітлення виборів

Зловмисники заволоділи доступом до онлайн платформи, яку використовують особи, відповідальні за організацію та проведення виборів, для звітування перед громадськістю щодо загальних результатів голосування у день виборів. В той час, коли дійсний підрахунок показує, що ваша партія ймовірно отримає велику кількість місць, веб-сайт виборів показує хибні результати, які залишають вашу партію позаду. До того, як цю проблему можна розв'язати, ЗМІ використає хибну інформацію і повідомить, що ваша партія схоже поступиться місцем опозиційним партіям.

**Можливе реагування:** Мета вашої заяви полягає у тому, щоб перешкодити пресу надавання хибних результатів за правдиві та уникнути ситуації, за якої громадськість повірить у цю інформацію. Виборні органи ймовірно забезпечать власне комунікаційне реагування. Ваша первинна заява має бути обережною, оскільки вам необхідно уникнути підриву впевненості у виборах в цілому, але одночасно підвищити рівень поінформованості про наявність серйозної неточності. Оперативність має дуже важливе значення: якщо громадськість почне вірити хибним результатам, тоді правдиві результати можуть розглядатися як підроблені. У вашій заяві потрібно зазначити, що веб-сайт виборного органу очевидно знаходиться під загрозою та значно відрізняється від правильного підрахунку голосів.

## Сценарій 4: Втручання у процес голосування

Як тільки відкриються виборчі дільниці у день виборів, зловмисник використає вразливість електронних списків виборців та спричинить одночасний їхній вихід з ладу. Співробітники виборчих дільниць вимушені використовувати обмежену кількість паперових резервних копій, створюючи при цьому довгі черги, а також виражають стурбованість потенційним впливом на вибори. Більш того, порушення в функціонування електронних списків виборців зосереджуються на територіях, де планується отримати багато голосів за вашу партію.

**Можливе реагування:** На відміну від попереднього сценарію, цей може мати вирішальний вплив на результат виборів. Ваша первинна заява має бути обережною, оскільки додаткова інформація може змінити вашу думку про інцидент (напр., якщо пізніше стане очевидним, що порушення в роботі електронних списків виборців були широко поширеними та однаково стосувались територій, які підтримують опозиційні партії). Крім того, необережне реагування може спровокувати сильне - або навіть жорстоке – реагування прихильників. У заяві слід зазначити, що ви контролюєте ситуацію та стурбовані впливом збоїв у списках виборців на результати голосування, але слід додати, що інформацію уточнюють. Коли масштаб інциденту стане зрозумілим, подальші заяви можуть закликати до використання відповідних засобів правового захисту.

## Сценарій 5: Кампанія дезінформації

В день виборів велика кількість облікових записів у соцмережах публікує хибну інформацію про проведення виборів. Згодом, ці публікації мають на меті понизити явку та підірвати впевненість громадськості у результатах. Публікації містять такі скарги: довгі черги на конкретних виборчих дільницях, коли такі черги відсутні, а також що працівники виборчої дільниці не приймають бюлетені на користь конкретного кандидата, тоді коли це насправді не відбувається. Журналісти починають репостити такі неправдиві повідомлення.

Один з кандидатів у передвиборчій гонці починає перебільшувати значення хибної інформації, зазначаючи, що звіти свідчать про те, що вибори сфальсифіковані.

> **Можливе реагування:** Ваше завдання має на меті протидіяти дезінформації за допомогою точної, надійної інформації. Ваша заява повинна звертати увагу на те, що наразі ведеться організована дезінформаційна кампанія, але слід бути обережними, щоб не повторювати чи не перебільшувати значення цієї дезінформації. Заява має зазначати факти, а не повторювати та спростовувати кожне хибне твердження.
> Також вона має бути короткою, лаконічною і поширюватися за допомогою усіх можливих платформ (соцмережі, телебачення радіо тощо) Див. також розділ «Передові практики боротьби з дезінформацією».

# Висновок

Ми сподіваємося, що цей Шаблон забезпечить надійний початок для політичних партій та кампаній, які прагнуть розробити комунікаційний план реагування у сфері кібербезпеки. Ми також сподіваємось, що керівні принципи та формат цього Шаблону допоможе організаціям підготуватися та управляти кібер-ризиками, що виникають і загрожують виборчому процесу. Як і у всіх комунікаційних планах ми рекомендуємо, щоб ви систематично оновлювати ваш план для врахування змін в організаційній структурі та кадрах.

## Побачили, як можна покращити цю Стратегію?

З’явились нові технології або вразливі питання, які ми маємо вирішити?
**Ми хочемо отримати зворотний зв'язок від вас.**
Будь ласка, поділіться своїми ідеями, історіями та зауваженнями на Twitter @d3p використовуючи хештег #CyberPlaybook або надішліть нам електронний лист на адресу: connect@d3p.org, щоб ми могли продовжувати вдосконалювати цей ресурс з огляду на зміни у цифровому середовищі.

**Проект «Захист цифрової демократії»**
Центр Белфера з науки та міжнародних відносин
Гарвардської школи ім. Джона Ф. Кеннеді
вул. Дж.Ф. Кеннеді
Кембрідж, Масачусетс 02138

**www.belfercenter.org/D3P**