Додаток
до рішення 54 сесії VIII скликання
Слобожанської селищної ради
від 05.03.2026 року № 5121-54/VIII

# Політика інформаційної безпеки у виконавчих органах Слобожанської селищної ради

**селище Слобожанське**
**2026 рік**

## 1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Політика інформаційної безпеки (далі – Політика) визначає основні вимоги до захисту інформації у виконавчих органах Слобожанської селищної ради (далі – Виконавчі органи), встановлює принципи та правила безпечної роботи з інформаційними ресурсами.

1.2. Дана Політика є обов'язковим документом для ознайомлення при прийомі на роботу та є доступною для ознайомлення будь-якому працівникові Виконавчих органів.

1.3. Метою даної Політики є:

Забезпечення захисту інформаційних ресурсів Виконавчих органів від зовнішніх і внутрішніх загроз;

Безперервність роботи всіх служб і сервісів Виконавчих органів;

Мінімізація ризиків операційної діяльності Виконавчих органів;

Відповідність законодавству України в області інформаційної безпеки та захисту персональних даних.

1.4. Дана Політика поширюється на всі процеси діяльності Виконавчих органів та є обов'язковою для виконання всіма працівниками. Порушення вимог Політики тягне за собою дисциплінарну відповідальність згідно з чинним законодавством України.

## 2. ОСНОВНІ ТЕРМІНИ ТА ВИЗНАЧЕННЯ

2.1. Інформаційна безпека (ІБ) – практика забезпечення захисту інформаційних активів від загроз, які можуть на них вплинути.

2.2. Інформаційний актив (ІА) – обладнання, програмне забезпечення, дані, а також працівники, які беруть участь в процесах діяльності Виконавчих органів.

2.3. Конфіденційність – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем.

2.4. Цілісність – властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем.

2.5. Доступність – властивість інформації бути доступною та використовуватися на вимогу користувача.

2.6. Інцидент – подія, яка не є частиною звичайних операцій і порушує робочі процеси.

2.7. Шкідливе ПЗ – програмне забезпечення, яке вживлюється в систему з метою порушення конфіденційності, цілісності та/або доступності даних.

## 3. РОЗПОДІЛ ОБОВ'ЯЗКІВ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

**3.1.** Загальна відповідальність за інформаційну безпеку Виконавчих органів покладається на Керівника.

**3.2**. Керівник відповідальний за:

3.2.1. Визначення критичних операційних процесів для діяльності Виконавчих органів;

3.2.2. Прийняття рішень щодо розвитку інформаційної безпеки;

3.2.3. Затвердження та поширення правил і вимог інформаційної безпеки;

3.2.4. Затвердження відповідальності за порушення правил та вимог інформаційної безпеки;

3.2.5. Контроль виконання правил та вимог інформаційної безпеки.

**3.3**. Кожен працівник Виконавчих органів несе відповідальність за:

3.3.1. Безпечне використання систем і даних для цілей діяльності Виконавчих органів;

3.3.2. Дотримання вимог цієї Політики;

3.3.3. Повідомлення Керівника про будь-які сумніви щодо ефективності процесів безпеки;

3.3.4. Повідомлення про будь-яку подію чи інцидент щодо несанкціонованого або неправильного використання активів.

## 4. УПРАВЛІННЯ ДОСТУПОМ

4.1. Права доступу повинні визначатися відповідно до посадових обов'язків працівника.

4.2. Доступ до інформаційних активів повинен надаватися відповідно до принципу мінімальних привілеїв – доступ надається тільки до тих систем, які необхідні користувачу в межах роботи.

4.3. Усі запити на доступ повинні бути схвалені безпосереднім керівником працівника перед наданням доступу.

4.4. Облікові записи користувачів повинні негайно блокуватися у разі виявлення несанкціонованого доступу або підозрілої активності.

4.5. Використання двофакторної аутентифікації в тих системах та сервісах, де це можливо, є обов'язковим.

4.6. Права користувачів повинні переглядатися регулярно та після внесення змін, таких як зміна посади або звільнення.

## 5. ПАРОЛЬНА ПОЛІТИКА

**5.1.** Для забезпечення надійного захисту інформаційних систем паролем встановлюються наступні вимоги:

5.1.1. Мінімальна довжина: 8-12 символів;

5.1.2. Пароль повинен містити символи верхнього та нижнього регістру, числа, а також спеціальні символи;

5.1.3.Не використовувати будь-які персональні дані (ім'я, прізвище, дата народження);

5.1.4. Не містить у собі загальновживані слова;

5.1.5. Максимальний термін дії пароля: 90 днів;

5.1.6. Паролі не слід зберігати або передавати у відкритому тексті.

**5.2.** Забороняється:

5.2.1. Записувати паролі на паперових носіях, які зберігаються на робочому місці;

5.2.2. Передавати свій пароль іншим особам;

5.2.3. Використовувати однакові паролі для різних систем;

5.2.4. Зберігати паролі в незахищених файлах на комп'ютері.

## 6. ВИКОРИСТАННЯ ЕЛЕКТРОННОЇ ПОШТИ

**6.1.** Доступ до електронної пошти надається працівникам Виконавчих органів для виконання своїх службових обов'язків. Використання електронної пошти в особистих цілях, не пов'язаних з діяльністю Виконавчих органів, заборонено.

**6.2.** У Виконавчих органах заборонено:

6.2.1. Надсилати повідомлення, що містять конфіденційну інформацію, без необхідності виконання службових обов'язків;

6.2.2. Надсилати по електронній пошті логіни, паролі та іншу чутливу інформацію;

6.2.3. Використовувати електронну адресу для підписки на маркетингові електронні листи без попереднього узгодження з керівником;

6.2.4. Відкривати будь-яке вкладення, посилання чи додаток до електронної пошти, де працівник не має ґрунтовних підстав вважати, що інформація надійшла з надійного джерела;

6.2.5. Надсилати масові розсилки (понад 15) на зовнішні адреси без згоди керівника;

6.2.6. Надсилати матеріали, що містять шкідливе програмне забезпечення;

6.2.7. Поширювати інформацію, заборонену українським законодавством.

**6.3**. Орієнтовний, але не вичерпний перелік ознак підозрілого листа:

6.3.1. Незнайомий або підозрілий відправник;

6.3.2. Вимога терміново перейти за посиланням або відкрити вкладення;

6.3.3. Запит на введення пароля або конфіденційної інформації;

6.3.4. Численні граматичні помилки в офіційному листі;

6.3.5. Загрозливий або тривожний характер повідомлення.

**6.4.** Доступ працівника до облікових записів електронної пошти при звільненні повинен бути негайно відключений.

## 7. ВИКОРИСТАННЯ РОБОЧИХ ПРИСТРОЇВ

**7.1.** Робочі комп'ютери та інші пристрої повинні використовуватися виключно для виконання службових обов'язків.

**7.2.** Обов'язкові правила роботи з комп'ютером:

7.2.1. Блокувати комп'ютер при відході від робочого місця (комбінація клавіш Win+L);

7.2.2. Не залишати комп'ютер увімкненим без нагляду поза робочим часом;

7.2.3. Не дозволяти іншим особам користуватися вашим комп'ютером під вашим обліковим записом;

7.2.4. Використовувати лише ліцензійне програмне забезпечення.

**7.3.** Обов'язкове блокування екрану на пристроях після встановленого часу бездіяльності (рекомендовано 5-10 хвилин).

**7.4.** Працівники несуть відповідальність за забезпечення фізичної безпеки робочих пристроїв при їх використанні за межами приміщень Виконавчих органів.

## 8. ОБМЕЖЕННЯ ВСТАНОВЛЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

**8.1.** Встановлення програмного забезпечення на робочі комп'ютери повинно бути узгоджене з безпосереднім керівником.

**8.2.** Забороняється встановлювати:

8.2.1. Програмне забезпечення з ненадійних джерел;

8.2.2. Ігри та розважальні програми;

8.2.3. Програми для особистого використання;

8.2.4. Програмне забезпечення, яке може становити загрозу безпеці.

**8.3.** Працівникам дозволено встановлювати лише затверджене програмне забезпечення, необхідне для виконання службових обов'язків.

## 9. ЗАХИСТ ВІД ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

**9.1.** На всіх робочих комп'ютерах має бути встановлено та активовано антивірусне програмне забезпечення.

**9.2.** Антивірусне програмне забезпечення повинно регулярно оновлюватися до останньої версії.

**9.3.** Працівники зобов'язані:

9.3.1. Не вимикати антивірусне програмне забезпечення;

9.3.2. Не ігнорувати попередження антивірусу;

9.3.3. Негайно повідомляти керівника при виявленні шкідливого ПЗ;

9.3.4. Перевіряти USB-флешки та інші зовнішні носії перед використанням.

**9.4**. Орієнтовний перелік ознак зараження комп'ютера шкідливим ПЗ:

9.4.1. Суттєве зниження продуктивності комп'ютера;

9.4.2. З'являються незнайомі програми або вікна;

9.4.3. Файли зникають або не відкриваються;

9.4.4. Антивірус вимкнено або не працює;

9.4.5. Стрімке збільшення мережевого трафіку.

**9.5.** Комп'ютери, у яких виявлено шкідливе програмне забезпечення, повинні бути негайно відключені від мережі до їх повного очищення.

## 10. ВИКОРИСТАННЯ ІНТЕРНЕТУ

**10.1.** Інтернет-ресурси Виконавчих органів мають використовуватися для виконання робочих завдань, інформаційно-аналітичної роботи, обміну електронною поштою.

**10.2.** Заборонено:

10.2.1.Перегляд розважальних сайтів;

10.2.2. Завантаження медіа матеріалів не пов’язаних з виконанням службових обов’язків;

10.2.3. Відвідування підозрілих сайтів;

10.2.4. Використання інтернету для особистих потреб;

10.2.5. Завантаження файлів з невідомих джерел або авторів.

## 11. ВИКОРИСТАННЯ ОСОБИСТИХ ПРИСТРОЇВ

**11.1.** У Виконавчих органах може бути дозволено працівникам використовувати власні пристрої (телефони, планшети, ноутбуки) для виконання посадових обов'язків за погодженням з Керівником.

**11.2**. Вимоги до особистих пристроїв:

11.2.3. Встановлення пароля на розблокування;

11.2.4. Використання антивірусного програмного забезпечення;

11.2.5. Не зберігати робочі паролі в незахищеному вигляді;

11.2.6. Не передавати пристрій іншим особам;

11.2.7 Негайно повідомити керівника при втраті пристрою, який містить службову інформацію;

**11.3.** Кожен пристрій, який використовується для доступу до внутрішньої інформації, повинен використовуватися відповідально та лише в робочих цілях.

**11.4.** На особистих пристроях, які дозволені для використання у службових цілях забороняється здійснювати обробку персональних даних, володільцем чи розпорядником яких є Виконавчі органи.

## 12. ФІЗИЧНА БЕЗПЕКА

12.1. Документи з обмеженим доступом не повинні залишатися без нагляду на робочих столах після закінчення робочого дня.

12.2. Шафи з конфіденційними документами повинні замикатися.

12.3. Відвідувачі Виконавчих органів повинні завжди супроводжуватись відповідальними працівниками у тих приміщеннях/робочих зонах, де є ризик несанкціонованого доступу до інформації.

12.4. Працівники не повинні обговорювати конфіденційну інформацію в присутності сторонніх осіб або в громадських місцях.

## 13. БЕЗПЕКА КОМУНІКАЦІЙ

13.1. Обов'язковою є перевірка вкладень з поштових скриньок та інших месенджерів перед завантаженням.

13.2. Під час обміну конфіденційною інформацією повинні використовуватись захищені канали зв'язку.

13.3. При використанні месенджерів для робочого спілкування слід дотримуватись вимог, затверджених відповідними регламентами.

## 14. РЕЗЕРВНЕ КОПІЮВАННЯ

14.1. Важливі робочі документи повинні регулярно копіюватися для запобігання їх втраті.

14.2. Резервні копії конфіденційних документів повинні зберігатися в захищених місцях.

## 15. УПРАВЛІННЯ ІНЦИДЕНТАМИ

**15.1.** Кожен працівник несе відповідальність за повідомлення керівника, коли він або вона дізнаються про те, що стався або міг статися інцидент інформаційної безпеки.

15.1.1. Особа, відповідальна за кібербезпеку повинна опиратися на Політику управління інцидентами кібербезпеки (Додаток 1) та План реагування на інциденти кібербезпеки (Додаток 2).

**15.2.** Орієнтовний та невичерпний перелік ситуацій, при виявленні яких необхідно негайно повідомити про інцидент інформаційної безпеки:

15.2.1. Підозрілого листа електронної пошти з вимогою надати конфіденційну інформацію;

15.2.2. Незвичайної роботи комп'ютера;
15.2.3. Вікна з вимогою викупу за розблокування файлів;
15.2.4. Неможливості увійти в систему з правильним паролем;
15.2.5. Несанкціонованого доступу до даних;
15.2.6. Втрати пристрою з службовою інформацією.
**15.3**. Дії працівника при виявленні інциденту:
15.3.1. Негайно повідомити безпосереднього керівника;
15.3.2. За можливості відключити комп'ютер від мережі;
15.3.4. Не намагатися виправити проблему самостійно;
15.3.5. Не видаляти файли або програми без вказівки керівника;
15.3.6. Зафіксувати час та обставини виявлення інциденту.
**15.4.** Працівники можуть намагатися вирішити інциденти інформаційної безпеки лише за вказівками та з прямого дозволу керівника.

## 16. НАВЧАННЯ ТА ОБІЗНАНІСТЬ

16.1. Всі працівники повинні бути ознайомлені з вимогами щодо роботи з інформаційними активами Виконавчих органів та нести персональну відповідальність за їх дотримання.
16.2. При прийомі на роботу кожен працівник повинен ознайомитися з цією Політикою під підпис.
16.3. Працівники повинні проходити щорічний інструктаж з питань інформаційної безпеки.
16.4. При виникненні питань щодо інформаційної безпеки працівники повинні звертатися до свого безпосереднього керівника.

## 17. ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ

**17.1.** Порушення вимог цієї Політики тягне за собою дисциплінарну відповідальність відповідно до чинного законодавства України.
**17.2.** Орієнтовний та невичерпний перелік серйозних порушень інформаційної безпеки:
17.2.1. Передача паролів або доступів стороннім особам;
17.2.2. Навмисне пошкодження інформаційних систем;
17.2.3. Розголошення конфіденційної інформації;
17.2.4. Встановлення шкідливого програмного забезпечення;
17.2.5. Несанкціонований доступ до чужих облікових записів.

## 18. ПЕРЕГЛЯД ТА ОНОВЛЕННЯ ПОЛІТИКИ

18.1. Політика переглядається щорічно для забезпечення її актуальності та відповідності потребам Виконавчих органів.
18.2. Політика також переглядається при внесенні суттєвих змін в організаційну структуру або ІТ-інфраструктуру Виконавчих органів.
18.3. Оновлена Політика підлягає затвердженню Керівництвом Виконавчих органів.

Секретар селищної ради Людмила ЛАГОДА

Додаток 1
до Політики інформаційної
безпеки у Виконавчих органах
Слобожанської селищної ради
(Підпункт 15.1.1. пункт 15.1. розділ 15)

# ПОЛІТИКА УПРАВЛІННЯ ІНЦИДЕНТАМИ КІБЕРБЕЗПЕКИ

## 1. Загальне

Політика управління інцидентами кібербезпеки (далі – Політика) визначає вимоги та послідовність дій щодо виявлення, аналізу та опрацювання інцидентів кібербезпеки (далі – КБ) у Виконавчих органах.

## 1.1. Мета Політики:

1.1.1 Організація оперативного виявлення, оцінки та реагування на інциденти КБ;

1.1.2. Мінімізації наслідків інцидентів КБ;

1.1.3. Запобігання інцидентам КБ в майбутньому, поліпшення впровадження та використання захисних заходів КБ;

1.1.4. Відповідність рівня КБ Виконавчих органів вимогам законів України, нормативно-правових актів України та міжнародних стандартів в області КБ;

1.1.5. Захист інформаційних систем Виконавчих органів від порушень конфіденційності, цілісності, доступності та спостережності.

## 1.2. Класифікація інцидентів

За наслідками інциденти КБ повинні класифікуватись за відповідно до таблиці, яка наведена у пункті 2.2.3 даної Політики.

## 1.3. Види інцидентів

В цій Політиці визначені наступні види інцидентів:

1.3.1. Порушення цілісності інформації;
1.3.2. Порушення конфіденційності;
1.3.3. Порушення доступності;
1.3.4. Порушення спостережності.

## 2. Реагування на інциденти КБ

Етап реагування на інциденти КБ в інформаційних системах Виконавчих органів повинен включати наступні кроки: Підготовка; виявлення та аналіз; стримування; усунення; відновлення; аналіз ефективності.

## 2.1. Підготовка

Для забезпечення готовності Виконавчих органів до оперативного реагування на інциденти КБ повинні бути розроблені плани реагування на окремі види інцидентів КБ, що є найбільш ймовірними для певної прикладної системи з урахуванням умов та режиму її функціонування виходячи з прогнозованих даних та експертних оцінок.

Розробка планів реагування на інциденти КБ є основою для системного підходу до процесу управління інцидентами КБ у Виконавчих органах.

2.1.1. Етап «Створення плану реагування на інцидент КБ»

Відповідальна особа за ІБ повинна проводити пошук інформації про аналогічні інциденти КБ, які відбувалися в минулому та для яких розроблено типовий план реагування.

Якщо для поточного виду інциденту КБ у базі знань існує типовий план реагування, то Відповідальна особа за ІБ переходить до його реалізації.

Якщо подібних інцидентів КБ у базі знань немає, Відповідальна особа за ІБ повинна розробити комплекс заходів, який оформлюється у вигляді плану реагування на інцидент КБ та зберігається в базі знань.

## 2.2. Виявлення та аналіз

**2.2.1**. Етапи «Виявлення та інформування про інцидент. Збір та реєстрація інформації про інцидент КБ»

У разі виявлення інциденту або слабких місць КБ працівники Виконавчих органів або залучені треті сторони повинні повідомити про це Відповідальну особу за ІБ.

До основних ознак інциденту відносяться наступні (невичерпний перелік):

2.2.1.1. Суттєве зниження продуктивності прикладних систем або недоступність прикладних систем;

2.2.1.2. Повідомлення антивірусного ПЗ;

2.2.1.3. Несанкціонована діяльність у мережі та прикладних системах Виконавчих органів;

2.2.1.4. Стрімке збільшення мережевого трафіку;

2.2.1.5. Численні повідомлення про помилки та збої;

2.2.1.6. Зафіксовані спроби підбору паролів;

2.2.1.7. Заздалегідь відома негативна подія безпеки;

2.2.1.8. Подія безпеки, що зафіксована у неробочий час;

2.2.1.9. Невідомі облікові записи;

2.2.1.10. Відключені засоби забезпечення безпеки;

2.2.1.11. Спроби застосування методів соціальної інженерії;

2.2.1.12. Відсутність засобів захисту інформації;

Працівник Виконавчих органів, який виявив можливі ознаки інциденту, повинен вказати у повідомленні наступну інформацію:

2.2.1.13. Опис проблеми, що спостерігається;

2.2.1.14. Час виникнення ознак інциденту;

2.2.1.15. Інші суттєві дані щодо інциденту – у відповідь на запитання Відповідальної особи за ІБ

**2.2.2.** Етап «Аналіз інциденту»

Процедура повинна розпочинатись за фактом отримання Відповідальною особою за ІБ повідомлення про виникнення інциденту КБ.

Після отримання повідомлення про інцидент Відповідальна особа за ІБ повинна провести класифікацію інциденту, аналіз зібраної інформацію та прийняти рішення щодо підтвердження його статусу.

**2.2.3**. Етап «Оповіщення про інцидент»

У Виконавчих органах оповіщення зацікавлених сторін (голова, заступники голови, Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA, яка функціонує в складі Державної служби спеціального зв'язку та захисту інформації України, Служба безпеки України, Національний координаційний центр кібербезпеки при РНБО України, залучені треті сторони – відповідно до договірних вимог, тощо) повинно здійснюватися Відповідальною особою за ІБ визначеними засобами після маркування.

Маркування повинно проводитися відповідно до наступних значень:

**Рівень 0**, некритичний (білий). Кіберінцидент/кібератака не загрожує сталому, надійному та штатному режиму функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем.

**Рівень 1**, низький (зелений). Кіберінцидент/кібератака безпосередньо загрожує сталому, надійному та штатному режиму функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем, але не загрожує захищеності (конфіденційності, цілісності і доступності) інформації та даних, що ними обробляються.

**Рівень 2**, середній (жовтий). Кіберінцидент/кібератака безпосередньо загрожує сталому, надійному та штатному режиму функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем, внаслідок чого

створюються передумови для порушення захищеності (конфіденційності, цілісності і доступності) інформації та даних, що ними обробляються, виникають передумови для припинення виконання функцій та/або надання послуг критичною інфраструктурою.

**Рівень 3**, високий (помаранчевий). Кіберінцидент/кібератака безпосередньо загрожує сталому, надійному та штатному режиму функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем, порушується захищеність (конфіденційність, цілісність і доступність) інформації та даних, що ними обробляються, внаслідок чого виникають потенційні загрози для національної безпеки і оборони, стану навколишнього природнього середовища, соціальної сфери, національної економіки та її окремих галузей, припинення виконання функцій та/або надання послуг критичною інфраструктурою. Реагування на цьому рівні може потребувати залучення сил та засобів більше ніж одного основного суб'єкта національної системи кібербезпеки.

**Рівень 4,** критичний (червоний). Кіберінцидент/кібератака безпосередньо загрожує сталому, надійному та штатному режиму функціонування кількох інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем, порушується захищеність (конфіденційність, цілісність і доступність) інформації та даних, що ними обробляються, внаслідок чого виникають реальні загрози для національної безпеки і оборони, стану навколишнього природного середовища, соціальної сфери, національної економіки та її окремих галузей, припинення виконання функцій та/або надання послуг критичною інфраструктурою. Кіберінцидент/кібератака може мати транскордонний вплив. Реагування на цьому рівні потребує залучення сил та засобів основних суб'єктів національної системи кібербезпеки.

**Рівень 5**, надзвичайний (чорний). Кіберінцидент/кібератака безпосередньо загрожує сталому, надійному та штатному режиму функціонування значної кількості інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем, порушується захищеність (конфіденційність, цілісність і доступність) інформації та даних, що ними обробляються, внаслідок чого виникають невідворотні загрози для повноцінного функціонування держави або загроза життю громадян України. Кіберінцидент/кібератака може мати транскордонний вплив. Реагування на цьому рівні потребує максимального залучення сил та засобів основних суб'єктів національної системи кібербезпеки та інших суб'єктів забезпечення кібербезпеки.

## 2.3. Стримування

**2.3.1.** Етап «Збір інформації для розслідування інциденту»

Відповідальна особа за ІБ відповідно до плану реагування повинна зібрати інформацію про інцидент для проведення подальшого розслідування.

У випадку, коли при реалізації збору інформації про інцидент КБ планується переривання роботи інформаційно-комунікаційної системи (далі ІКС), Відповідальна особа за ІБ, повинна погодити таке переривання з Керівництвом Виконавчих органів.

**2.3.2.** Етап «Зменшення впливу інциденту»

Відповідальна особа за ІБ повинна обрати методи та заходи, спрямовані на зменшення впливу інциденту на процеси діяльності Виконавчих органів, окремо для кожного конкретного інциденту, залежно від його виду, та у відповідності з розробленим, планом реагування.

Будь-які методи, дії та порядок їхнього використання або виконання повинні погоджуватися Керівництвом Виконавчих органів.

Відповідальна особа за ІБ повинна виконати оцінку можливого впливу запланованих дій на безперервність діяльності ураженої системи та проінформувати Керівництво Виконавчих органів. За необхідності допускається ізолювання системи або роз'єднання компонентів цієї системи на період проведення повного розслідування інциденту.

## 2.4. Усунення інциденту та відновлення функціонування інформаційно-комунікаційної системи.

З метою відновлення нормального функціонування ІКС Відповідальна особа за ІБ повинна проводити заходи з усунення причин та наслідків інциденту.

Процедура усунення інциденту та відновлення функціонування залежить від виду інциденту та повинна визначатись для кожного інциденту окремо.

Після відновлення функціонування ІКС Відповідальна особа за ІБ має перевірити відсутність ознак повторення інциденту та повідомити про завершення робіт Керівництво Виконавчих органів.

## 2.5. Аналіз ефективності заходів з реагування на кіберінциденти/кібератаки

**2.5.1.** Етап «Розслідування інциденту»

Під час виконання робіт з розслідування інцидентів повинні використовуватись методи та засоби, що запобігають випадковому або навмисному внесенню змін в дані, що вивчаються та аналізуються.

Відповідальна особа за ІБ повинна з'ясувати причини інциденту та провести аналіз усіх виявлених у процесі розслідування небезпечних факторів, що призвели до відхилень:

2.5.1.1. у діях працівників Виконавчих органів;

2.5.1.2. у роботі інформаційних ресурсів та систем;

2.5.1.3. відхилень від норм експлуатації програмного забезпечення і обладнання;

2.5.1.4. відхилень від вимог політик ІБ із визначенням ступеня впливу цих відхилень на розвиток інциденту.

Відповідальна особа за ІБ повинна визначити:

2.5.1.5. які нормативні вимоги були порушені або не виконані (з посиланням на відповідні статті, розділи, пункти нормативних актів);

2.5.1.6. причетність до інциденту, якщо це мало місце, інших підприємств, організацій і установ із визначенням, наскільки це можливо;

2.5.1.7. ступеня їх впливу на виникнення і перебіг інциденту.

**2.5.2.** Етап «Аналіз ефективності»

Після завершення розслідування Відповідальна особа за ІБ повинна підготувати звіт з описом всіх проведених процедур щодо управління інцидентами КБ та закриттям інциденту КБ та надати Керівництву Виконавчих органів, а також, за необхідності, зацікавленим сторонам.

Відповідальна особа за ІБ повинна внести інформацію про закриття інциденту в журнал реєстрації інцидентів.

## 3. Система внутрішнього контролю

Всі співробітники Виконавчих органів несуть відповідальність за своєчасність інформування Відповідальної особи за ІБ у разі виявлення ознак інцидентів КБ або можливості настання інциденту КБ.

## 4. Підтримка, оновлення та розповсюдження

Політика буде опублікована у формі, яку неможливо легко змінити, і у формі, яка є актуальною, доступною та зрозумілою для цільового читача. Політика зберігається та є легкодоступною для персоналу та третіх сторін (за необхідності) для подальшого використання.

Політика буде розповсюджена в електронному вигляді. Нова копія Політики буде поширена разом із новою версією будь-якого компонента Політики. Нова копія матиме збільшений номер версії.

Персонал, який отримує електронну копію, оновлює власну паперову версію Політики та зберігає її.

Відповідальність за керування та оновлення Політики покладено на Відповідальну особу за ІБ. Оновлена Політика подається до Керівництва Виконавчих органів для остаточного затвердження. Політика переглядається щорічно для забезпечення її адекватності та відповідності потребам і цілям Виконавчих органів або частіше, якщо це необхідно (під час внесення суттєвих змін).

Секретар селищної ради Людмила ЛАГОДА

Додаток 2
до Політики інформаційної
безпеки у виконавчих органах
Слобожанської селищної ради
(Підпункт 15.1.1. пункт 15.1. розділ 15 )

# ПЛАН РЕАГУВАННЯ НА ІНЦИДЕНТИ КІБЕРБЕЗПЕКИ

1. Порядковий номер;
2. Опис інциденту кібербезпеки;
3. Назва інциденту;
4. План дій щодо реагування на інцидент;
5. Дата/час виконання дій з реагування;
6. Очікувана дата завершення всіх дій з реагування;
7. Технічні, програмні та фінансові ресурси;
8. Місце збереження інформаційних підтверджень та доказів;
9. Відповідальна за реагування особа (ПІБ, Посада);
10. Статус(Не розпочато У процесі Завершено);
11. Коментарі .

# ПРИКЛАДИ РЕАГУВАННЯ НА ІНЦИДЕНТ КІБЕРБЕЗПЕКИ

**ФІШИНГ**

РОЗСЛІДУВАННЯ. Завдання: Визначити та впровадити кроки з розслідування інцидентів КБ, включаючи основні питання та стратегії фішингу.

1. Область та масштаб атаки
2. Аналіз повідомлень
3. Аналіз посилань та вкладень
4. Категоризація типу атак
5. Визначення критичності атаки

ВИПРАВЛЕННЯ: Спланувати заходи з усунення інцидентів у яких ці кроки запускаються разом (або скоординовано) з залученням відповідних команд спеціалістів, готових реагувати на будь-які порушення. Визначити необхідний час і компромісні підходи для усунення наслідків.

КОМУНІКАЦІЯ. Завдання: Визначити етапи проведення комунікацій під час фішинг атаки. Вказати інструменти та процедуру (зокрема хто повинен бути залучений) для кожного кроку.

ВІДНОВЛЕННЯ. Завдання: Визначити кроки відновлення після фішинг атаки. Визначити та вказати інструменти та процедуру для кожного кроку

РЕСУРСИ. Приклад: Дії користувача при ймовірній фішинговій атаці Завдання: Визначити кроки для користувачів, які мають підозру на фішинг.

ЗАПОБІГАННЯ РИЗИКАМ. Завдання: Визначити кроки для користувачів, які реагують на наявність програми-вимагача.

**ПРОГРАМИ-ВИМАГАЧІ**

РОЗСЛІДУВАННЯ. Завдання: Визначити та впровадити кроки з розслідування атак/інцидентів, які відбулись за участі програм-вимагачів, зокрема основні питання та стратегії.

1. Визначити тип програм-вимагачів
2. Визначити область застосування
3. Оцінка впливу
4. Знайти інфікованого

ВИПРАВЛЕННЯ: Спланувати заходи з усунення інцидентів, у яких ці кроки запускаються разом (або скоординовано) з залученням відповідних команд спеціалістів, готових реагувати на будь-які порушення. Розглянути час і компромісні підходи з усунення інциденту.

КОМУНІКАЦІЯ. Завдання: Визначити етапи проведення комунікацій. Вказати інструменти та процедуру (зокрема хто повинен бути залучений) для кожного кроку.

ВІДНОВЛЕННЯ. Завдання: Визначити кроки відновлення. Визначити та вказати інструменти та процедуру для кожного кроку. Не рекомендовано платити викуп: це не гарантує вирішення проблеми. Все може піти не так (наприклад, помилки можуть зробити дані неможливими для відновлення навіть за допомогою ключа). Крім того, оплата доводить, що програми-вимагачі працюють і можуть посилити атаки проти вас чи будь-кого іншого.

РЕСУРСИ. Приклад: Дії користувача при підозрі про наявність програми-вимагача Завдання: Визначити кроки для користувачів, які реагують на наявність програми-вимагача.

ЗАПОБІГАННЯ РИЗИКАМ: Завдання: Поспілкуватись з іншими співробітниками, щоб переконатися, що всі розуміють наступні кроки та роблять свій внесок, де це можливо.

**АТАКА НА ВЕБСАЙТ**

РОЗСЛІДУВАННЯ:

1. Негайно відключити зіпсований сервер для подальшого дослідження.
2. Визначити джерело вразливості системи, яку використав зловмисник.
3. Зібрати будь-які підказки щодо того, ким є хакер або на яку організацію він працює.
4. Зібрати іншу важливу інформацію зі сторінки, яка була зіпсована.

ВИПРАВЛЕННЯ: Спланувати заходи з усунення проблем, у яких кроки зі стримування запускаються разом (або скоординовано) з задіянням відповідних команд спеціалістів, готових реагувати на будь-які порушення. Розглянути час і компромісні підходи з усунення інциденту.

КОМУНІКАЦІЯ. Завдання: Визначити кроки проведення етапу комунікацій. Вказати інструменти та процедуру (зокрема хто повинен бути залучений) для кожного кроку.

ВІДНОВЛЕННЯ. Завдання: Визначити кроки відновлення. Визначити та вказати інструменти та процедуру для кожного кроку.

РЕСУРСИ. Приклад: Дії користувача при атаці пошкодження веб-сайту Завдання: Визначити кроки для користувачів, які реагують на атаку на веб-сайт.

ЗАПОБІГАННЯ РИЗИКАМ. Завдання: Поспілкуватись з іншими співробітниками, щоб переконатися, що всі розуміють наступні кроки та роблять свій внесок, де це можливо.

**ВТРАТА ДАНИХ**

ПІДГОТОВКА: Забезпечити належний доступ до будь-якої необхідної документації та інформації, включаючи доступ у неробочий час, для наступного:

1. Процес управління інцидентами;
2. Схеми архітектури мережі;
3. Діаграми потоку даних.

Визначити та отримати послуги стороннього провайдера. Переглянути останні кіберінциденти та їх результати.

РОЗСЛІДУВАННЯ. Завдання: Визначити та впровадити кроки з розслідування, зокрема основні питання та стратегії компрометації, ідентифікації та доступу.

1. Переконатись, що до уваги беруться всі задіяні дані.
2. Проаналізувати будь-який підозрілий мережевий трафік.
3. Переглянути журнали безпеки та доступу, сканування вразливостей і будь-які автоматизовані результати інструментів.
4. Проаналізувати будь-яку підозрілу активність, файли чи виявлені зразки ЗПЗ.
5. Зіставити будь-які нещодавні події безпеки або ознаки компрометації з підозрілою активністю в мережі.
6. Визначити джерело компрометації даних.

7. Визначити конкретний набір даних, який було зламано, а також спосіб його зламу.
8. Визначити методологію атаки та графік кіберінцидентів.

АНАЛІЗ: Етап виправлення:

1. Визначення технічного механізму порушення даних;
2. Усунення технічного механізму витоку даних;
3. Відновлення уражених систем і служб та приведення до звичайного стану.

ВИПРАВЛЕННЯ: На додаток до загальних кроків і вказівок у плані реагування на інцидент:

1. Відновити системи на основі аналізу впливу на діяльність і критичності діяльності.
2. Здійснити повне антивірусне та розширене сканування шкідливих програм усіх систем по всій організації.
3. Повторно встановити облікові дані всіх задіяних системі дані облікових записів користувачів.
4. Реінтегрувати раніше скомпрометовані системи.
5. Відновити будь-які пошкоджені або знищені дані.
6. Відновити усі призупинені служби.
7. Встановити моніторинг для виявлення подальшої підозрілої діяльності.
8. Координувати впровадження будь-яких необхідних виправлень або заходів з усунення вразливостей.

ВІДНОВЛЕННЯ: Етап заходів після інциденту має такі цілі:

1. Заповнити Звіт про інцидент, включаючи всі деталі інциденту та дії.
2. Завершити процес управління інцидентами.
3. Опублікувати відповідні внутрішні та зовнішні повідомлення.

Секретар селищної ради Людмила ЛАГОДА