



УКРАЇНА
СОЛОТВИНСЬКА СЕЛИЩНА РАДА
ІВАНО-ФРАНКІВСЬКОГО РАЙОНУ ІВАНО-ФРАНКІВСЬКОЇ ОБЛАСТІ
ВИКОНАВЧИЙ КОМІТЕТ

РІШЕННЯ

26 серпня 2026 року

селище Солотвин

№ 130

Про затвердження Політики інформаційної безпеки Солотвинської селищної ТГ

На виконання ключових законодавчих актів України у сфері кібербезпеки, а саме законів України «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах», «Про основні засади забезпечення кібербезпеки України», «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури», постанови Кабінету Міністрів України від 26.11.2025 № 1533 «Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози», постанови Кабінету Міністрів України від 26.11.2025 № 1531 «Про затвердження мінімальних вимог до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем», наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 30.01.2026 № 75 «Про затвердження Каталогу заходів з кіберзахисту, базових заходів з кіберзахисту, форми плану кіберзахисту та методичних рекомендацій щодо здійснення заходів з кіберзахисту», наказу Адміністрації Держспецзв'язку від 04.06.2026 № 410 «Про затвердження Порядку приєднання суб'єктів забезпечення кібербезпеки до платформи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози», виконком селищної ради

ВИРІШИВ:

1. Затвердити Політику інформаційної безпеки Солотвинської селищної територіальної громади (додаток 1).
2. Відповідальній особі з кіберзахисту Купчаку Ярославу Івановичу (інженер з охорони праці):
 - 1.1. До 10.09.2026 забезпечити підключення органу місцевого самоврядування

до платформи обміну індикаторами компрометації MISP CERT-UA та адаптованого програмного продукту MISP-UA.

- 1.2. Провести оцінку та визначення поточного профілю кіберзахисту Солотвинської селищної ради відповідно до методичних рекомендацій щодо здійснення заходів з кіберзахисту, затверджених наказом Адміністрації Держспецзв'язку від 30.01.2026 № 75
- 1.3. До 15.09.2026 проінформувати управління з питань цифрового розвитку Івано-Франківської обласної державної адміністрації про виконання заходів кіберзахисту.
2. Керуючий справами (секретарю) виконавчого комітету Ірині Струк:
 - 2.1. Ознайомити з цим рішенням відповідальних осіб з кіберзахисту Солотвинської селищної територіальної громади.
 - 2.2. Забезпечити оприлюднення рішення на офіційному сайті селищної ради.
3. Відповідальним особам з кіберзахисту ознайомити підлеглих з «Політикою інформаційної безпеки Солотвинської селищної територіальної громади».
4. Контроль за виконанням даного рішення покласти на заступника селищного голови з питань діяльності виконавчих органів ради Андрія Кріцака.

Секретар селищної ради

Василь МАНДЗЮК

Додаток 1
до рішення виконавчого комітету
від 26 серпня 2026 року № 130

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
Солотвинської селищна територіальної громади

Зміст

1. Загальні положення...	5
2. Терміни та визначення...	5
3. Політика інформаційної безпеки	6
3.1. Управління інформаційною безпекою...	7
3.2. Розподіл обов'язків з інформаційної безпеки...	7
3.3. Безпека людських ресурсів...	7
3.4. Навчання та обізнаність...	8
3.5. Класифікація та управління інформацією...	8
3.6. Обробка, передача та зберігання даних...	8
3.7. Використання особистих пристроїв...	8
3.8. Парольна політика...	9
3.9. Використання електронної пошти...	9
3.10. Безпека мережі...	10
3.11. Використання робочих пристроїв...	10
3.12. Встановлення безпечних оновлень...	11
3.13. Обмеження встановлення програмного забезпечення...	11
3.14. Захист від шкідливого ПЗ...	11
3.15. Логування та моніторинг...	12
3.16. Віддалений доступ...	12
3.17. Резервне копіювання...	12
3.18. Безпека комунікацій...	12
13	
3.19. Управління активами	13
3.20. Управління ризиками...	13
3.21. Управління інцидентами...	13
3.22. Безперервність діяльності...	13
4. Перегляд, оновлення та розповсюдження...	14
5. Перелік відповідальних осіб...	14
Додаток 1. Політика управління інцидентами кібербезпеки...	15
Додаток 2. План реагування на інциденти кібербезпеки...	21

1. Загальні положення

Політика інформаційної безпеки Солотвинської селищної територіальної громади (далі – Політика) визначає загальні вимоги до інформаційної безпеки у Солотвинській селищній територіальній громаді (далі – Солотвинська селищна ТГ), основні принципи, цілі та завдання управління інформаційною безпекою Солотвинської селищної ТГ.

Дана Політика є обов'язковим документом для ознайомлення при прийомі на роботу та є доступною для ознайомлення будь-якому співробітникові Солотвинської селищної ТГ або третій стороні.

Ця Політика є офіційно прийнятою Керівництвом Солотвинської селищної ТГ системою поглядів на проблеми забезпечення інформаційної безпеки, встановлює принципи побудови процесів управління інформаційною безпекою на основі систематизованої розробки та впровадження політик, положень, регламентів, стандартів, інструкцій та інших нормативних документів в області інформаційної безпеки.

Метою даної Політики є:

- **Забезпечення захисту інформаційних ресурсів** Солотвинської селищної від зовнішніх і внутрішніх загроз;
- **Безперервність роботи всіх служб і сервісів** Солотвинської селищної ТГ;
- **Мінімізація ризиків операційної діяльності** Солотвинської селищної ТГ;
- **Створення позитивної репутації** Солотвинської селищної ТГ при взаємодії з третіми сторонами;
- **Відповідність законодавству України та вимогам контролюючих органів в області інформаційної безпеки та захисту персональних даних.**

Дана Політика поширюється на всі процеси діяльності Солотвинської селищної ТГ та є обов'язковою для виконання всіма співробітниками Солотвинської селищної ТГ. Порушення вимог Політики тягне за собою дисциплінарну відповідальність та відповідальність згідно з чинним законодавством України.

2. Терміни та визначення

Відповідальна особа з кіберзахисту – особа, яка виконує функції та завдання, пов'язані з кіберзахистом Солотвинської селищної ТГ, відповідно до статті 5-1 Закону України «Про основні засади забезпечення кібербезпеки України».

Власник ІА – співробітник Солотвинської селищної ТГ, який несе відповідальність за: забезпечення належної класифікації інформації та активів, пов'язаних із засобами обробки інформації; визначення та періодичний перегляд обмежень доступу і класифікацій; управління конкретними ризиками, пов'язаними з активом, і визначення пов'язаних потреб в безпеці.

Внутрішній аудит – аудит ІБ, що проводиться співробітниками Солотвинської селищної ТГ, відповідно навченими та незалежним від кон

Вплив – ступінь (величина) шкоди для діяльності Солотвинської селищної ТГ, яка може виникнути внаслідок несанкціонованого розкриття інформації, несанкціонованої зміни інформації, несанкціонованого знищення інформації або втрати інформації чи порушення доступності інформаційної системи.

Доступність – властивість інформації, яка полягає в тому, щоб бути доступною та використовуватися на вимогу користувача і/або процесу.

Загроза – можлива небезпека, яка може використовувати уразливість в інформаційній системі для порушення цілісності, конфіденційності, доступності системи.

Інформаційна безпека (ІБ) – це практика забезпечення захисту інформаційних активів від загроз, які можуть на них вплинути. Вона включає в себе вичерпний набір засобів управління, які охоплюють різні фактори (людські, фізичні, екологічні та технічні) протягом життєвого циклу

інформаційних і технологічних активів, включаючи розробку, створення і впровадження нових систем, підтримка даних і систем, моніторинг використання таких активів, виявлення та реагування на потенційні загрози, дотримання чинних законів і положень про кібербезпеку і конфіденційність, а також виведення з експлуатації ІТ-систем і знищення даних.

Інформаційна система – комп'ютерні системи, програмне забезпечення, телекомунікаційне і периферійне устаткування.

Інформаційний актив (ІА) – обладнання, програмне забезпечення, дані, які беруть участь в процесах діяльності Солотвинської селищної ТГ, які визначені і управляються як єдине ціле, щоб його можна було зрозуміти, спільно використовувати, захищати та ефективно керувати. Інформаційні активи мають керовану цінність, ризики, контент і життєві цикли.

Інцидент – це подія, яка не є частиною звичайних операцій і порушує робочі процеси. Інцидент може включати відмову функції або послуги, які повинні були бути надані, або будь-які інші типи збою операції.

Конфіденційність – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і/або процесом.

Користувач – особа або Солотвинської селищної Назва ТГ, які взаємодіють з інформаційними системами.

Оцінка ризиків – процес виявлення, визначення пріоритетів та аналіз ризиків. Процес включає визначення ступеня, в якому несприятливі обставини або події можуть вплинути на Організацію. Даний процес використовує результати оцінок загроз і вразливостей для виявлення ризиків для діяльності Солотвинської селищної ТГ і оцінює ці ризики, з точки зору ймовірності виникнення і впливу. Результатом оцінки ризику є список передбачуваних потенційних впливів і явних вразливостей. Оцінка ризиків є частиною процесу управління ризиками.

Політика інформаційної безпеки – набір задокументованих управлінських рішень, створений для захисту інформації Солотвинської селищної ТГ та пов'язаних з нею ресурсів.

Ризик – ймовірність впливу на діяльність Солотвинської селищної ТГ (включаючи місію, функції, імідж, репутацію), її активи (ресурси) і співробітників в результаті експлуатації вразливостей інформаційної системи і залежно від потенційного впливу, реалізація загрози і ймовірність її реалізації.

Уразливість – недолік в інформаційній системі, який може бути використаний суб'єктом загрози (наприклад, зловмисником) для виконання несанкціонованих дій в системі і порушення цілісності, конфіденційності, доступності або спостережливості.

Цілісність – властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і/або процесом.

Шифрування – процес перетворення відкритого тексту в зашифрований з метою безпеки або конфіденційності.

Шкідливе ПЗ – програмне забезпечення, яке вживлюється в систему, як правило, таємно, з метою порушення конфіденційності, цілісності та/або доступності даних, додатків або операційної системи користувача або іншим чином шкодити або заважати роботі користувача.

SMTPS – Simple Mail Transfer Protocol Secure.

3. Політика інформаційної безпеки

3.1. Управління інформаційною безпекою

Для забезпечення ІБ, необхідно слідувати формальним загальним правилам та процедурам наведеним далі, що покривають відповідне використання ІА Солотвинської селищної ТГ.

Співробітники Солотвинської селищної ТГ та відповідні треті сторони (які мають доступ до інформації та/або ресурсів Солотвинської селищної ТГ повинні бути проінформовані про необхідність дотримання цієї Політики.

Для забезпечення постійної придатності, адекватності та ефективності ця Політика повинна переглядатися відповідальною особою з кіберзахисту через заплановані проміжки часу – щонайменше раз в рік, якщо впроваджуються суттєві зміни або за рішенням Керівництва Солотвинської селищної ТГ.

Суттєвими змінами можна вважати:

- **Зміни в процесах діяльності** Солотвинської селищної ТГ;
- **Зміни в організаційній структурі;**
- **Зміни в ІТ-інфраструктурі** Солотвинської селищної ТГ тощо.

Відповідно до сфери діяльності Солотвинської селищної ТГ необхідно також враховувати наступні моменти:

- **Законодавство, що регулює сферу діяльності** Солотвинської селищної ТГ та договірні зобов'язання;
- **Відповідальність за порушення Політики;**
- **Обов'язки Керівництва** Солотвинської селищної ТГ та інших осіб щодо безпеки систем та інформації Солотвинської селищної ТГ.

3.2. Розподіл обов'язків з інформаційної безпеки

Загальна відповідальність за ІБ Солотвинської селищної ТГ покладається на Керівництво.

Конфліктні обов'язки та сфери відповідальності повинні бути розділені, щоб зменшити можливості для несанкціонованих або ненавмисних змін чи зловживання ІА Солотвинської ТГ. Формальне розподілення відповідальності Керівництвом Солотвинської селищної ТГ забезпечує стратегічну прозорість та вплив на практику забезпечення ІБ.

Керівництво відповідальне за:

- **Визначення критичних операційних процесів для діяльності** Солотвинської селищної ТГ;
- **Прийняття рішень щодо розвитку ІБ** Солотвинської селищної ТГ;
- **Затвердження та поширення правил і вимог ІБ в** Солотвинської селищної ТГ;
- **Затвердження відповідальності за порушення правил та вимог** Солотвинської селищної ТГ;
- **Функцію перевірки та контролю виконання в** Солотвинської селищної ТГ правил та вимог ІБ. Додатково відповідальні та їх обов'язки описані нижче в тілі цієї Політики.

3.3. Безпека людських ресурсів

Перевірка кандидатів перед працевлаштуванням, співробітників чи третіх сторін повинна чітко враховувати чутливість інформації, до якої кандидати отримають доступ, та передбачувані ризики при визначенні характеру та строків цих перевірок.

Призначення на посади та звільнення з посад повинно виконуватися відповідно до державних нормативно-правових актів.

Кожен співробітник Солотвинської селищної ТГ та третьої сторони, якому надано доступ до систем та/або даних Солотвинської селищної ТГ, несе відповідальність за безпечне використання систем і даних для цілей діяльності Солотвинської селищної ТГ та дотримання її політик.

Співробітники та треті сторони несуть відповідальність за повідомлення Керівнику про будь-які сумніви щодо ефективності процесів безпеки, про будь-яку подію чи інцидент щодо несанкціонованого або неправильного використання активів Солотвинської селищної ТГ.

Обов'язок Керівництва Солотвинської селищної ТГ вимагати від всіх співробітників та третіх сторін дотримання вимог ІБ Солотвинської селищної ТГ, відповідно до встановлених політик та процесів, а також контролювати процес їх дотримання.

Припинення трудової діяльності здійснюється згідно з чинним трудовим законодавством України.

3.4. Навчання та обізнаність

Всі співробітники, які є користувачами внутрішньої мережі повинні бути ознайомлені з внутрішніми вимогами щодо роботи з інформаційними активами Солотвинської селищної ТГ та нести персональну відповідальність за їх дотримання.

Усі співробітники та відповідні треті сторони повинні проходити відповідну підготовку з підвищення обізнаності та регулярно отримувати інформацію про оновлення організаційних політик та процедур відповідно до їх робочих функцій.

Програма обізнаності повинна забезпечувати, щоб усі співробітники досягали та підтримували принаймні базовий рівень розуміння питань ІБ, таких як загальні зобов'язання згідно з різними політиками, стандартами, процедурами, керівними принципами, законами, нормативними актами, контрактними умовами, а також загальноприйнятими стандартами етики та прийнятною поведінки.

Інструктаж (навчання) з кібергігієни проводиться відповідальною особою з кіберзахисту у такі строки: протягом одного місяця з дня призначення співробітника на посаду; не рідше одного разу на рік для всіх діючих співробітників; додатково — протягом одного місяця після настання значного кіберінциденту.

Зміст інструктажів визначається відповідно до Методичних рекомендацій щодо проведення інструктажів і тренінгів з кібергігієни, затверджених наказом Адміністрації Держспецзв'язку від 21.10.2025 № 661.

3.5. Класифікація та управління інформацією

Інформацію слід класифікувати, визначати та оцінювати ризики відповідно до її конфіденційності, цілісності, доступності та спостережливості, незалежно від носія, на якому вона зберігається і/або обробляється. Чутлива інформація повинна визначатися відповідно до її конфіденційності, цілісності, доступності та спостережливості. Вся інформація, окрім публічної, має визначатися як чутлива.

Незалежно від рівня конфіденційності, вся інформація Солотвинської селищної ТГ повинна використовуватися належним чином та тільки для дозволених цілей.

Розкриття інформації з обмеженим доступом може здійснюватися лише у законний спосіб зацікавленим особам органів влади, а також фізичним та юридичним особам за згодою Солотвинської селищної ТГ, з дотриманням вимог чинного законодавства України та вимог відповідних Договорів.

3.6. Обробка, передача та зберігання даних

Чутливі дані повинні збиратися та зберігатися лише в системах, де є обґрунтована ділова чи технічна потреба. Чутливі виробничі дані повинні бути захищені при зберіганні і/або використанні у системах, і надійно видалятись, коли вони більше не потрібні.

Чутливі дані ніколи не повинні збиратися або використовуватися для цілей, відмінних від тих, для яких дані були зібрані спочатку. Усі параметри збереження даних (періоди, цілі тощо) повинні бути законними та відповідати місцевому та міжнародному законодавству та нормам щодо захисту даних.

3.7. Використання особистих пристроїв

Використання особистих пристроїв для доступу до інформаційних систем Солотвинської селищної ТГ заборонено. Доступ до систем, послуг та ресурсів Солотвинської селищної ТГ здійснюється виключно зі службових пристроїв, закріплених за співробітником.

3.8. Парольна політика

Відповідно до Парольної політики, для забезпечення надійного захисту інформаційних систем паролем, мають бути встановлені наступні параметри:

- Мінімальна довжина: 8 символів;
- Максимальна довжина: не більше 64 символів;

- Пароль перевіряється на входження до відомих переліків скомпрометованих або поширених паролів та словникових значень;
- Забороняється використання персональних даних (імені, дати народження, найменування Солотвинської селищної ТГ] тощо) у складі пароля;
- Плановий термін дії пароля: не рідше одного разу на рік; додатково, незалежно від планового строку, зміна пароля здійснюється негайно за наявності підозри або підтвердженого факту компрометації облікового запису;
- Допускається використання пробілів та повного набору друкованих символів, включно з паролними фразами;
- Безпечне зберігання паролів: паролі не слід зберігати або передавати у відкритому тексті.
- Для облікових записів з підвищеним рівнем доступу рекомендується використання менеджерів паролів та багатофакторної автентифікації (MFA).

3.9. Використання електронної пошти

Доступ до електронної пошти надається співробітникам Солотвинської селищної ТГ для виконання своїх службових обов'язків. Використання електронної пошти співробітниками Солотвинської селищної ТГ в особистих або інших цілях, не пов'язаних з діяльністю Солотвинської селищної ТГ, заборонено.

В Солотвинській селищній ТГ заборонено:

- Надсилати повідомлення, що містять чутливу інформацію, а також дані, що містять чутливу інформацію не для виконання своїх службових обов'язків. Забороняється надсилати по електронній пошті логіни, паролі та іншу чутливу інформацію;
- Використовувати електронну адресу для підписки на маркетингові електронні листи без попереднього узгодження з відповідальною особою з кіберзахисту;
- Відкривати будь-яке вкладення, посилання чи додаток до електронної пошти, де співробітник не має ґрунтовних підстав вважати, що інформація, до якої очікується доступ, надійшла з надійного джерела;
- Надсилати масові розсилки (понад 10) на зовнішні адреси без згоди Керівника співробітника та відповідальної особи з кіберзахисту;
- Надсилати по електронній пошті матеріали, що містять шкідливе програмне забезпечення чи інші програми, призначені для порушення, знищення або обмеження функціональних можливостей будь-якого комп'ютерного чи телекомунікаційного обладнання чи інформаційних систем та послуг;
- Надсилати електронною поштою програми, які забезпечують несанкціонований доступ;
- Розповсюджувати за допомогою електронної пошти матеріали, які захищені авторським правом і зачіпають будь-який патент, торгову марку, комерційну таємницю, авторські права або будь-які інші права власності. та/або авторські права або пов'язані з ними права третіх сторін;
- Поширювати через електронну пошту інформацію, заборонену міжнародним та українським законодавством, включаючи матеріали, що

є шкідливими, загрозливими, нецензурними, а також інформацію, що порушує честь та гідність інших. Також забороняється надсилати матеріали, що розпалюють національну ворожнечу, підбурюють до насильства, закликають до незаконних дій, включаючи матеріали, що містять інструкції щодо використання вибухових речовин, зброї тощо. Доступ колишнього співробітника до облікових записів електронної пошти [Назва ТГ] повинен бути негайно відключений та деактивований.

3.10. Безпека мережі

Наступні вимоги обов'язкові до виконання:

- Вимоги до конфігурації безпеки повинні бути визначені для всього мережевого обладнання;
- Вимоги до контролю аутентифікації та доступу повинні бути визначені та повинні бути впроваджені;
- Вимоги до систем та механізмів моніторингу безпеки мережі повинні бути визначені, впровадженні, необхідним чином управлятися;
- Усі оновлення повинні вчасно встановлюватися;
- Зміни можуть бути внесені лише адміністратором систем або відповідним авторизованим користувачем;
- Процес резервного копіювання мережевих пристроїв (наприклад, системного програмного забезпечення, даних конфігурацій, файлів баз даних) повинен відбуватися регулярно;
- Вимоги до конфігурування безпеки Wi-Fi мереж:
 - Зміна паролів за замовчуванням;
 - Вимкнення WPS;
 - Вимкнення SSID Broadcast;
 - Своєчасне оновлення прошивки;
 - Обмеження можливості під'єднання пристроїв до локальної мережі.

Протоколи безпечного зв'язку

Щоб захистити інформацію в системах та додатках [Назва ТГ], необхідно належним чином управляти та контролювати мережі.

Використання протоколів безпечного зв'язку гарантують конфіденційність, цілісність, доступність та спостережливості інформації, що передається. Наступні протоколи найбільш прийнятні для використання:

- SSH2;
- SFTP;
- TLS 1.2–1.3;
- HTTPS;
- WSS:– SMTPS;
- DNS-over-HTTPS.

3.11. Використання робочих пристроїв

Солдотвинської селищної ТГ повинна встановити вимоги щодо безпеки пристроїв, змінних носіїв під час їх використання.

Обов'язкове блокування екрану на пристроях після встановленого часу бездіяльності повинне бути налаштоване на всіх робочих пристроях.

Захист робочих пристроїв шляхом шифрування жорстких дисків та паролів для розблокування повинен бути реалізованим за необхідності.

Персонал несе відповідальність за забезпечення фізичної безпеки робочих пристроїв при їх

використанні за межами приміщень Солотвинської ТГ (обмеження фізичного доступу третіх сторін, слідування вимогам блокування екрану).

Забезпечення виконання вимог щодо безпечного використання робочих пристроїв має бути автоматизовано за допомогою відповідних програмних інструментів. Політики налаштування таких інструментів повинні регулярно переглядатись на відповідність даний Політиці та іншим цільовим політикам Солотвинської селищної ТГ.

3.12. Встановлення безпечних оновлень

[Назва ТГ] повинна встановити вимоги щодо встановлення оновлень на всіх ІА, з яких надається доступ до інформації/послуг/ресурсів Солотвинської селищної ТГ.

Режим автоматичного оновлення виправлень або можливість зробити це вручну має бути забезпечена адміністратором систем. Антивірусне програмне забезпечення та інші компоненти безпеки повинні регулярно перевірятись та оновлюватись до останньої версії.

Якщо операційна система – Windows, інструмент управління виправленнями повинен бути налаштований таким чином, щоб він автоматично завантажував останні виправлення безпеки Microsoft. Перевірка та застосування виправлень повинна проводитись за необхідності.

3.13. Обмеження встановлення програмного забезпечення

Правила щодо встановлення програмного забезпечення користувачами повинні бути визначені та впроваджені Солотвинської селищної ТГ.

Забороняється встановлення та використання програмного забезпечення й комунікаційного (мережевого) обладнання, включених до Переліку забороненого до використання програмного забезпечення та комунікаційного (мережевого) обладнання, що публікується та актуалізується Державною службою спеціального зв'язку та захисту інформації України (<https://cip.gov.ua/ua/news/perelik-zaboronenogo-do-vikoristannya-programnogo-zabezpechennya-ta-komunikaciynogo-merezhevogo-obladnannya1>) на підставі рішень Ради національної безпеки і оборони України, введених у дію указами Президента України, щодо застосування санкцій. Перед встановленням нового програмного забезпечення адміністратор систем перевіряє його відсутність у зазначеному Переліку в чинній на дату перевірки редакції.

Солотвинська селищна ТГ визначає перелік дозволеного до встановлення програмного забезпечення. Встановлювати можна лише те, що є в цьому переліку. Усе інше — потребує попереднього дозволу адміністратора систем або відповідальної особи з кіберзахисту, навіть якщо програма не входить до забороненого переліку Держспецзв'язку.

Встановлення програмного забезпечення повинно бути обмежене для всіх користувачів, проте можливі винятки, які повинні бути схвалені адміністратором систем та відповідальною особою з кіберзахисту.

Функція контролю закріплена за відповідальною особою з кіберзахисту та Керівництвом, щоб забезпечити належний рівень контролю та розділення привілеїв.

3.14. Захист від шкідливого ПЗ

Попереднє тестування програмного забезпечення та перевірка файлів до їх встановлення на пристроях, з яких існує доступ до корпоративної інформації/систем/ресурсів повинні забезпечуватись адміністратором систем.

Лише програмне забезпечення, затверджене адміністратором систем та відповідальною особою з кіберзахисту, дозволено встановлювати на системи Солотвинської селищної ТГ.

Сканери проти шкідливого ПЗ необхідно налаштувати на автоматичне сканування відповідних компонентів відразу після випуску оновлень.

Солотвинська селищна ТГ має налаштувати антивірусне програмне забезпечення на: сканування під час завантаження, сканування файлових та поштових серверів принаймні один раз на день та будь-яких інших серверів – принаймні раз на тиждень, сканування файлів при відкритті, сканування вкладень вхідної та вихідної електронної пошти, веб сканування вмісту при синхронізації із скануванням портативних пристроїв, де це можливо.

Управління та перегляд журналів антивірусного програмного забезпечення має здійснюватися

адміністратором систем.

Для захисту програмного забезпечення від шкідливих програм Солотвинської селищної ТГ повинно здійснюватися: ручне/автоматичне та планове сканування, видалення заражених файлів, розміщення заражених файлів на карантин, які неможливо видалити, можливість автоматичного та запланованого оновлення, реєстрація випадків шкідливого програмного забезпечення та забезпечення можливості аналізу логів, централізоване управління та ведення логів.

Комп'ютери, у яких виявлено шкідливе програмне забезпечення, та комп'ютери без антивірусного програмного забезпечення заборонено під'єднувати до внутрішньої мережі Солотвинської селищної ТГ.

Відповідальність за контроль дотримання захисту від шкідливого ПЗ покладено на відповідальну особу з кіберзахисту.

3.15. Логування та моніторинг

Інформація, яку слід збирати з власних систем має включати в себе:

- Дату та час події;
- Ідентифікатор користувача;
- Тип запиту/дії;
- Статус запиту (успішний чи невдалий);
- Події, що включають зміни, можуть вказувати на початок та кінцевий стан тощо.

Солотвинська селищна ТГ повинна визначити необхідність проведення ручного збору логів в тих системах, де це неможливо автоматично або, якщо автоматичний аудит логів не містить необхідної інформації.

Для реалізації неможливості зміни/видалення журналів логів адміністратором систем, в Солотвинській селищній ТГ мають бути впроваджені додаткові засоби контролю та рішення для реєстрації дій. Якщо критично важливі системи не мають функції реєстрації дій адміністратора систем, потрібно перейти на версії або нові платформи з наявною такою функцією або здійснити затвердження таких винятків Керівництвом Солотвинської селищної ТГ. У разі неможливості зміни систем чи сервісів, такі винятки повинні бути погоджені з Керівництвом.

3.16. Віддалений доступ

Інтернет-ресурси Солотвинської селищної ТГ] мають використовуватися для дистанційного виконання робочих завдань, інформаційно-аналітичної роботи в інтересах Солотвинської селищної ТГ, обміну поштою із третіми сторонами.

Інше використання Інтернет-ресурсів слід розглядати як порушення.

Підключення до мережі Інтернет в Солотвинській селищній ТГ повинно здійснюватися адміністратором систем у порядку надання прав доступу. При переміщенні співробітника (звільненні, переведенні в інший підрозділ) його безпосередній Керівник повинен подати заяву на скасування прав доступу.

Віддалене підключення до інформаційних активів Солотвинської селищної ТГ має здійснюватися за допомогою визначених адміністратором систем та відповідальною особою з кіберзахисту ресурсів.

З'єднання веб-зустрічей/віддаленого управління (наприклад, TeamViewer, AnyDesk) не повинні використовуватися в мережі Солотвинської селищної ТГ для надання віддаленого доступу третім сторонам за замовчуванням. Цей тип підключень дозволений лише для технічного обслуговування та усунення несправностей систем після належної авторизації.

3.17. Резервне копіювання

Резервне копіювання повинно здійснюватися регулярно.

Критично важлива інформація, програмне забезпечення та системи, що підлягають резервному копіюванню, повинні бути визначені.

Періодичність створення резервних копій та частота їх тестування повинні бути чітко визначені.

Тип резервного копіювання (повне, інкрементне, диференційоване) повинен бути визначений адміністратором систем для кожної системи.

Резервні копії повинні зберігатися окремо від основних копій та повинен бути забезпечений належний рівень безпеки, а доступ до резервних копій повинен бути обмежений на тому ж рівні, що і для основних копій.

Доступ до резервних копій повинні мати лише визначені співробітники Солотвинської селищної ТГ.

Відповідальність за здійснення резервного копіювання покладається на відповідальну особу з кіберзахисту.

3.18. Безпека комунікацій

Солотвинська селищна ТГ повинна визначити дозволені методи для зв'язку (передачі корпоративної інформації) всередині ТГ та з третіми сторонами.

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

Заборонений доступ до ресурсів Солотвинської селищної ТГ за прямим посиланням.

Під час обміну інформацією повинні використовуватись лише захищені протоколи передачі даних.

В Солотвинській селищній ТГ повинен бути впроваджений та підтримуватись процес електронного спілкування, включаючи питання безпеки, відповідно до рівня конфіденційності переданої інформації. Там, де це необхідно, повинні бути впроваджені додаткові засоби захисту (цифровий підпис, шифрування тощо).

3.19. Управління активами

Відповідальна особа з кіберзахисту веде перелік основних інформаційних активів [Скорочення] — комп'ютерів, серверів, ключових програм (зокрема реєстрів та систем фінансового обліку) та місць зберігання найважливіших даних.

Для кожного активу зазначається: назва, відповідальна особа та орієнтовна важливість для роботи [Скорочення] (наприклад: "без цього робота зупиниться" / "можна почекати" / "не критично").

Перелік переглядається не рідше одного разу на рік або в разі появи нової важливої системи чи обладнання, і використовується для швидкого визначення масштабу наслідків у разі кіберінциденту.

3.20. Управління ризиками

Управління ризиками є невід'ємною частиною діяльності на всіх рівнях Солотвинської селищної ТГ. Метою управління ризиками є надання Керівництву Солотвинської селищної ТГ інформації, необхідної для прийняття обґрунтованих рішень щодо зміни пріоритетів діяльності для управління областями неприйнятно високого ризику.

Солотвинська селищна ТГ має здійснювати оцінку ризиків, оскільки це процес ідентифікації, вимірювань та визначення пріоритетів ризиків ІБ.

3.21. Управління інцидентами

Солотвинська селищна ТГ повинна регулярно проводити навчання та підвищення обізнаності персоналу в сфері управління інцидентами. Підтримувати та розвивати процес реагування на всі типи інцидентів ІБ, відповідно до Політики управління інцидентами кібербезпеки (Додаток 1).

Кожен співробітник несе відповідальність за повідомлення відповідальної особи з кіберзахисту, коли він або вона дізнаються про те, що стався або міг статися інцидент ІБ, який міг поставити під загрозу безперервність діяльності Солотвинської селищної ТГ.

З міркувань безпеки та технічних міркувань Солотвинської селищної ТГ залишає за собою право відстежувати, записувати та реєструвати все використання своїх інформаційних активів і діяльність у мережі Солотвинської селищної ТГ.

3.22. Безперервність діяльності

Солотвинська селищна ТГ повинна забезпечити наявність необхідних ресурсів для безперервної діяльності та швидкого відновлення критичних систем у разі непередбачуваних ситуацій.

Керівники підрозділів несуть відповідальність за визначення вимог щодо захисту доступності систем/сервісів/даних і несуть остаточну відповідальність за їх виконання. Вимоги мають базуватися на аналізі ризиків, критичності активів і враховувати нормативні вимоги. Керівництво несе відповідальність за забезпечення необхідного фінансування для їх реалізації. Відповідальна особа з кіберзахисту повинен забезпечувати та підтримувати безперервність систем на випадок непередбачених обставин.

Після завершення відновлення системи, що зазнала збою чи кібератаки, відповідальна особа з кіберзахисту здійснює перевірку: відповідності функціонування системи штатному режиму; цілісності та повноти відновлених даних; відсутності ознак, що можуть свідчити про повторне виникнення інциденту.

Систему може бути визнано відновленою до штатного режиму функціонування лише за результатами такої перевірки, про що інформується Керівництво Солотвинської селищної ТГ. Не рідше одного разу на рік здійснюється практична перевірка можливості відновлення даних з резервних копій, що передбачає не лише підтвердження наявності резервної копії, а й фактичне тестове відновлення з неї.

4. Перегляд, оновлення та розповсюдження

Політика складається виключно зрозумілою мовою без складної термінології. Документ публікується у захищеному від редагування форматі (PDF) та розміщується у загальнодоступному місці [наприклад: на внутрішньому ресурсі / у спільній мережевій папці Солотвинської селищної ТГ, щоб кожен працівник мав до нього цілодобовий доступ. Ознайомлення працівників з Політикою фіксується під підпис.

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.

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

5. Перелік відповідальних осіб з кіберзахисту Солотвинська селищна територіальна громада]

Роль	Посада
здійснює керівництво, координацію та контроль за безпекою інформаційно-комунікаційних систем селищної ради	Купчак Ярослав Іванович –інженер з охорони праці

Секретар селищної ради

Василь МАНДЗЮК

Додаток 1
до Політики інформаційної безпеки
[Тут вписати назву своєї громади]

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 [тут вписати назву громади] (далі – Солотвинська селищна ТГ).

Метою Політики є забезпечення:

- Організація оперативного виявлення, оцінки та реагування на інциденти КБ;
- Мінімізації наслідків інцидентів КБ;
- Запобігання інцидентам КБ в майбутньому, поліпшення впровадження та використання захисних заходів КБ;
- Відповідності рівня КБ Солотвинської селищної ТГ вимогам законів України, нормативно-правових актів України та міжнародних стандартів в області КБ;
- Захисту інформаційних систем Солотвинської селищної ТГ від порушень конфіденційності, цілісності, доступності та спостережності.

1.1. Класифікація інцидентів

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

1.2. Види інцидентів

В цій Політиці визначені наступні види інцидентів:

- Порушення цілісності інформації;
- Порушення конфіденційності;
- Порушення доступності;
- Порушення спостережності.

2. Реагування на інциденти КБ

Етап реагування на інциденти КБ в інформаційних системах Солотвинської селищної ТГ повинен включати наступні кроки:

- Підготовка;
- Виявлення та аналіз;
- Стимування;
- Усунення;
- Відновлення;
- Аналіз ефективності.

2.1. Підготовка

Для забезпечення готовності Солотвинської селищної ТГ 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 в Солотвинській селищній ТГ.

2.1.1. Етап «Створення плану реагування на інцидент КБ»

Відповідальна особа з кіберзахисту 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 з кіберзахисту переходить до його реалізації. Якщо подібних інцидентів КБ у базі знань немає, відповідальна особа з кіберзахисту 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 Солотвинської селищної ТГ або залучені треті сторони повинні повідомити про це відповідальну особу з кіберзахисту. До основних ознак інциденту відносяться наступні (невичерпний перелік):

- Суттєве зниження продуктивності прикладних систем або недоступність прикладних систем;
- Повідомлення антивірусного ПЗ;
- Несанкціонована діяльність у мережі та прикладних системах Солотвинської селищної ТГ;
- Стрімке збільшення мережевого трафіку;
- Численні повідомлення про помилки та збої;
- Зафіксовані спроби підбору паролів;
- Заздалегідь відома негативна подія безпеки;
- Подія безпеки, що зафіксована у неробочий час;
- Невідомі облікові записи;
- Відключені засоби забезпечення безпеки;
- Спроби застосування методів соціальної інженерії;
- Відсутність засобів захисту інформації;
- І т.д.

Працівник Солотвинської селищної ТГ, який виявив можливі ознаки інциденту, повинен вказати у повідомленні наступну інформацію:

- Опис проблеми, що спостерігається;
- Час виникнення ознак інциденту;
- Інші суттєві дані щодо інциденту – у відповідь на запитання відповідальної особи з кіберзахисту.

2.2.2. Етап «Аналіз інциденту»

Процедура повинна розпочинатись за фактом отримання відповідальною особою з кіберзахисту повідомлення про виникнення інциденту КБ.

Після отримання повідомлення про інцидент відповідальна особа з кіберзахисту повинна провести класифікацію інциденту, аналіз зібраної інформації та прийняти рішення щодо підтвердження його статусу.

2.2.3. Етап «Оповіщення про інцидент»

В Солотвинській селищній ТГ оповіщення зацікавлених сторін секретар Солотвинської селищної ТГ, 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 з кіберзахисту визначеними засобами після маркування.

Маркування повинно проводитися відповідно до наступних значень:

Мітка (колір)	Значення
рівень 0, некритичний (білий)	Кіберінцидент/кібератака не загрожує сталому, надійному та штатному режиму функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем. (Повідомлення зовнішнім суб'єктам не обов'язкове — внутрішній реєстр.)
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. (Повідомляється регіональна/галузева CSIRT.)
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. Повідомляються регіональна/галузева CSIRT та CERT-UA.)
рівень 3, високий (помаранчевий)	Кіберінцидент/кібератака безпосередньо загрожує сталому, надійному та штатному режиму функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних 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 природного 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. (Повідомляються регіональна/галузева CSIRT, CERT-UA, СБУ.)
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. (Повідомляються регіональна/галузева CSIRT, CERT-UA, СБУ, НКЦК.)
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. (Повідомляються регіональна/галузева CSIRT — першочергово, далі CERT-UA, СБУ, НКЦК та інші суб'єкти невідкладно.)

Суб'єкт	Канал зв'язку	Телефон/примітка
Регіональна/галузева CSIRT		
CERT-UA	incidents@cert.gov.ua або cert.gov.ua/contact-us	Пн-Чт: 8:00-17:00 +38(044)281-88-25 Пт: 8:00-15:45 +38(044)281-88-05 Вихідні та святкові дні (цілодобово) +38(044)281-88-01
НКЦК		
СБУ		

2.3. Стимування

2.3.1. Етап «Збір інформації для розслідування інциденту»

Відповідальна особа з кіберзахисту 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 з кіберзахисту, повинна погодити таке переривання з Керівництвом Солотвинської селищної ТГ.

2.3.2. Етап «Зменшення впливу інциденту»

Відповідальна особа з кіберзахисту повинна обрати методи та заходи, спрямовані на зменшення впливу інциденту на процеси діяльності Солотвинської селищної ТГ, 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 Солотвинської селищної ТГ.

Відповідальна особа з кіберзахисту повинна виконати оцінку можливого впливу запланованих дій на безперервність діяльності ураженої системи та проінформувати Керівництво Солотвинської селищної ТГ. 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 з кіберзахисту 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 з кіберзахисту має перевірити відсутність ознак повторення інциденту та повідомити про завершення робіт Керівництво Солотвинської селищної ТГ.

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

- у діях працівників Солотвинської селищної ТГ;
- у роботі інформаційних ресурсів та систем;
- відхилень від норм експлуатації програмного забезпечення і обладнання;
- відхилень від вимог політик ІБ із визначенням ступеня впливу цих відхилень на розвиток інциденту.

Відповідальна особа з кіберзахисту повинна визначити:

- які нормативні вимоги були порушені або не виконані (з посиланням на відповідні статті, розділи, пункти нормативних актів);
- причетність до інциденту, якщо це мало місце, інших підприємств, організацій і установ із визначенням, наскільки це можливо;
- ступеня їх впливу на виникнення і перебіг інциденту.

2.5.2. Етап «Аналіз ефективності»

Після завершення розслідування відповідальна особа з кіберзахисту повинна підготувати звіт з описом всіх проведених процедур щодо управління інцидентами КБ та закриттям інциденту КБ та надати Керівництву Солотвинської селищної ТГ, а також, за необхідності, зацікавленим

сторонам.

Відповідальна особа з кіберзахисту повинна внести інформацію про закриття інциденту в журнал реєстрації інцидентів.

3. Система внутрішнього контролю

Всі співробітники Солотвинської селищної ТГ несуть відповідальність за своєчасність інформування відповідальну особу з кіберзахисту у разі виявлення ознак інцидентів КБ або можливості настання інциденту КБ.

4. Підтримка, оновлення та розповсюдження

Політика складається виключно зрозумілою мовою без складної термінології. Документ публікується у захищеному від редагування форматі (PDF) та розміщується у загальнодоступному місці [наприклад: *на внутрішньому ресурсі / у спільній мережевій папці ТГ*], щоб кожен працівник мав до нього цілодобовий доступ.

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 з кіберзахисту. Оновлена Політика подається до Керівництва Солотвинської селищної ТГ для остаточного затвердження. Політика переглядається щорічно для забезпечення її адекватності та відповідності потребам і цілям Солотвинської селищної ТГ або частіше, якщо це необхідно (під час внесення суттєвих змін).

Секретар селищної ради

Василь МАНДЗЮК

Додаток 2
до Політики інформаційної безпеки
[Тут впишіть назву громади]

План реагування на інциденти кібербезпеки

Опис інциденту кібербезпеки

[illegible]

Приклади реагування на інцидент кібербезпеки

	РОЗСЛІДУВАННЯ	ВИПРАВЛЕННЯ	КОМУНІКАЦІЯ	ВІДНОВЛЕННЯ	РЕСУРСИ	ЗАПОБІГАННЯ РИЗИКАМ
ФІШІНГ	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 посиленості та вкладень 4. Категоризація типу атак 5. Визначення критичності атаки	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. Завдання: Визначити тактичні та стратегічні кроки стримування фішингових	Завдання: Визначити етапи проведення комунікацій під час фішинг атаки. Вказати інструменти та процедури (зокрема хто повинен бути залучений) для кожного кроку.	Завдання: Визначити кроки відновлення після фішинг атаки. Визначити та вказати інструменти та процедури для кожного кроку	Приклад: Дії користувача при ймовірній фішинговій атаці Завдання: Визначити кроки для користувачів, які мають підозру на фішинг.	

	РОЗСЛІДУВАН НЯ	ВИПРАВЛЕНН Я	КОМУНІКАЦІЯ	ВІДНОВЛЕННЯ	РЕСУРСИ	ЗАПОБІГАНН Я РИЗИКАМ
		атак.				

	РОЗСЛІДУВАННЯ	ВИПРАВЛЕННЯ	КОМУНІКАЦІЯ	ВІДНОВЛЕННЯ	РЕСУРСИ	ЗАПОБІГАННЯ РИЗИКАМ
ПРОГРАМИ-ВИМАГАЧІ	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 інфікований	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. Завдання: Визначити тактичні та стратегічні кроки стримування програм-вимагачів	Завдання: Визначити етапи проведення комунікацій. Вказати інструменти та процедури (зокрема хто повинен бути залучений) для кожного кроку.	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.	Приклад: Дії користувача при підозрі про наявність програм-вимагача Завдання: Визначити кроки для користувачів, які реагують на наявність програм-вимагача.	

	РОЗСЛІДУВАННЯ	ВИПРАВЛЕННЯ	КОМУНІКАЦІЯ	ВІДНОВЛЕННЯ	РЕСУРСИ	ЗАПОБІГАННЯ РИЗИКАМ
АТАКА НА ВЕБСАЙТ	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.	Спланувати заходи з усунення проблем, у яких кроки зі стримування запускання разом (або скоординовано) з задіянням відповідних команд спеціалістів, готових реагувати на будь-які порушення. Розглянути час і компромісні підходи з усунення інциденту. Завдання: Визначити тактичні та стратегічні кроки стримування пошкодження веб-сайтів.	Завдання: Визначити кроки проведення етапу комунікацій. Вказати інструменти та процедуру для кожного кроку (зокрема хто повинен бути залучений) для кожного кроку.	Завдання: Визначити кроки відновлення. Визначити та вказати інструменти та процедуру для кожного кроку.	Приклад: Дії користувача при атаці пошкодження веб-сайту Завдання: Визначити кроки для користувачів, які реагують на атаку на веб-сайт.	Завдання: Поспілкуватися з іншими співробітниками, щоб переконатися, що всі розуміють наступні кроки та роблять свій внесок, де це можливо.

	РОЗСЛІДУВАННЯ	ВИПРАВЛЕННЯ	КОМУНІКАЦІЯ	ВІДНОВЛЕННЯ	РЕСУРСИ	ЗАПОБІГАННЯ РИЗИКАМ
		1. Створити резервну копію всіх даних, що зберігаються на веб-сервері. 2. Обов'язково тимчасово вимкнути сервер зіпсованої сторінки, поки триває розслідування. Після визначення джерела атаки виконати необхідні кроки, щоб переконатися, що сценарій атаки більше не повториться				

	РОЗСЛІДУВАННЯ	ВИПРАВЛЕННЯ	КОМУНІКАЦІЯ	ВІДНОВЛЕННЯ	РЕСУРСИ	ЗАПОБІГАННЯ РИЗИКАМ
ВТРАТА ДАНИХ	Забезпечити належний доступ до будь-якої необхідної документації та інформації, включаючи доступ у неробочий час, для наступного: - Процес управління інцидентами; - Схеми архітектури мережі; - Діаграми потоку даних; Визначити та отримати послуги стороннього провайдера. Переглянути останні кіберінциденти та їх результати	Завдання: Визначити та впровадити кроки з розслідування, зокрема основні питання та стратегії компрометації, ідентифікації та доступу.	1. Переконатися, що будь-які задіяні дані. 2. Проаналізувати будь-який підозрілий мережевий трафік. 3. Переглянути журнали безпеки та доступу, сканування вразливостей і будь-які автоматизовані результати інструментів. Проаналізувати будь-яку підозрілу активність, файли чи виявлені зразки ЗПЗ. 4. Зіставити будь-які нещодавні події безпеки або ознаки компрометації з підозрілою активністю в мережі.	Етап виправлення: - Міститись технічний механізм порушення даних; - Усунення технічного механізму витоку даних; - Відновлення уражених систем і служб та приведення до звичайного стану.	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 систем і дані	Етап заходів після інциденту має такі цілі: - Заповнити Звіт про інцидент, включаючи всі деталі інциденту та дії. - Завершити процес управління інцидентами. - Опублікувати відповідні внутрішні та зовнішні повідомлення

	РОЗСЛІДУВАННЯ	ВИПРАВЛЕННЯ	КОМУНІКАЦІЯ	ВІДНОВЛЕННЯ	РЕСУРСИ	ЗАПОБІГАННЯ РИЗИКАМ
			5.Визначити джерело компрометації даних. 6.Визначити конкретний набір даних, який було зламано, а також спосіб його зламу. 7.Визначити методологію атаки та графік кіберінцидентів		облікових записів користувачів. 4. Реінтегрувати раніше скопровані системи. 5. Відновити будь-які пошкоджені і 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	

РОЗСЛІДУВАН НЯ	ВИПРАВЛЕНН Я	КОМУНІКАЦІЯ	ВІДНОВЛЕННЯ	РЕСУРСИ	ЗАПОБІГАНН Я РИЗИКАМ
				вразливостей.	

Секретар селищної ради

Василь МАНДІЮК