Україна
НОВОТРОЇЦЬКА СЕЛИЩНА ВІЙСЬКОВА АДМІНІСТРАЦІЯ
ГЕНІЧЕСЬКОГО РАЙОНУ ХЕРСОНСЬКОЇ ОБЛАСТІ
РОЗПОРЯДЖЕННЯ

від 01.06.2026 Станіслав № 116

Про затвердження Політики інформаційної безпеки Новотроїцької селищної військової адміністрації, Новотроїцької селищної ради та її виконавчих органів

Керуючись указом Президента України від 19.09.2022 р. №658/2022, «Про утворення військових адміністрацій населених пунктів у Херсонській області», розпорядженням Президента України від 19.09.2022 р. № 184/2022-рп, відповідно до частини другої статті 10, п.8 частини шостої статті 15 Закону України «Про правовий режим воєнного стану», постановою Верховної Ради України від 03.11.2022 р. №2706-IX «Про здійснення начальниками військових адміністрацій населених пунктів у Бериславському, Генічеському, Каховському, Скадовському, Херсонському районах Херсонської області повноважень, передбачених частиною другою статті 10 Закону України «Про правовий режим воєнного стану», відповідно до Законів України «Про основні засади забезпечення кібербезпеки України», «Про захист інформації в інформаційно-телекомунікаційних системах», враховуючи укази Президента України: від 24.02.2022р. №64/2022 «Про введення воєнного стану в Україні», затверджений Законом України від 24.02.2022 р. № 2102-IX (з подальшими змінами, затвердженими відповідними законами України), від 01.02.2022 р. № 37/2022 «Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про План реалізації Стратегії кібербезпеки України», з метою забезпечення належного рівня захисту інформаційних ресурсів, підвищення ефективності управління інформаційною безпекою, запобігання загрозам несанкціонованого доступу до інформації:

1. Затвердити Політику інформаційної безпеки Новотроїцької селищної військової адміністрації, Новотроїцької селищної ради та її виконавчих органів (додається).

2. Встановити, що Політика інформаційної безпеки Новотроїцької селищної військової адміністрації, Новотроїцької селищної ради та її

виконавчих органів є обов’язковою до виконання усіма працівниками зазначених установ.

3. Начальнику відділу земельних відносин та екології Новотроїцької селищної ради, Тетяні ПЕРЕПЕЛИЦІ, забезпечити координацію заходів щодо впровадження та дотримання Політики у Новотроїцькій селищній військовій адміністрації, Новотроїцькій селищній раді та її виконавчих органах.

4. Контроль за виконанням цього розпорядження покласти на керуючого справами виконавчого комітету Новотроїцької селищної ради, Тетяну ЛЕВОШИЧ.

Начальник селищної
військової адміністрації Сергій ПЕРЕТЯТЬКО

Додаток
до розпорядження начальника
селищної військової адміністрації
від 01.06.2026 № 116

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
Новотроїцької селищної військової адміністрації, Новотроїцької селищної ради та її виконавчих органів

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Загальні положення

Ця Політика інформаційної безпеки (далі — Політика або ПІБ) визначає основні правила та вимоги щодо захисту інформації в Новотроїцькій селищній військовій адміністрації, Новотроїцькій селищній раді та її виконавчих органах.

ПІБ є головним документом з інформаційної безпеки в установах громади. З нею зобов'язані ознайомитися всі працівники. Документ визначає дії, яких необхідно дотримуватися, та дії, які заборонені при роботі з інформацією та цифровими активами. Політика зберігається у відповідальної особи з інформаційної безпеки.

Належний рівень інформаційної безпеки — це стан, за якого забезпечується:

- **конфіденційність** — інформація доступна лише тим, хто має на це право;
- **цілісність** — інформація є точною та не змінена без дозволу;
- **доступність** — інформація доступна тоді, коли це необхідно;
- **контрольованість** — дії в системах фіксуються та можуть бути перевірені.

Цей рівень досягається поєднанням технічних засобів захисту та свідомої поведінки кожного працівника. Жодна технологія не замінить відповідального ставлення людини до інформації.

Вимоги ПІБ поширюються на все, що використовується для роботи з інформацією: комп'ютери, ноутбуки, принтери, електронну пошту, веб-ресурси, носії інформації, засоби зв'язку та будь-які інші цифрові інструменти.

Політика є обов'язковою для всіх працівників незалежно від місця роботи — в офісі чи дистанційно.

1.2. Терміни та визначення

Актив — матеріальні та нематеріальні об'єкти або інформація, що мають цінність для Організації.

Брандмауер — програмний або апаратний засіб, який контролює мережевий трафік і дозволяє або блокує з'єднання відповідно до встановлених правил.

ВІБ — відповідальний за інформаційну безпеку. Призначена особа, яка відповідає за впровадження та дотримання цієї Політики. Якщо окремого ВІБ не призначено — його функції виконує начальник відповідного структурного підрозділу.

Вірус — шкідливе програмне забезпечення, що здатне самовідтворюватися та завдавати шкоди файлам, програмам або системі в цілому.

Доступність інформації — гарантія того, що уповноважені працівники мають доступ до потрібної інформації у потрібний час. У разі втрати — можливість її своєчасного відновлення.

Зовнішні носії інформації — флешки, USB-накопичувачі, компакт-диски, карти пам'яті та інші пристрої для зберігання і перенесення даних.

ІБ — інформаційна безпека — комплекс організаційних, технічних та правових заходів, спрямованих на захист інформації від несанкціонованого доступу, зміни або знищення.

ІС — інформаційна система — сукупність технічних та програмних засобів для обробки та зберігання інформації.

ІТ — інформаційні технології.

Конфіденційність інформації — гарантія того, що доступ до інформації мають лише уповноважені особи.

Користувач — будь-який працівник Організації, який має доступ до інформаційних ресурсів у межах своїх службових обов'язків.

Оргганізація – Новотроїцька селищна військова адміністрація

Персонал — усі працівники Новотроїцької селищної військової адміністрації, Новотроїцької селищної ради та її виконавчих органів, які використовують інформаційні ресурси та обладнання у своїй роботі.

ПІБ — Політика інформаційної безпеки — цей документ.

ПК — персональний комп'ютер.

Спостережність системи — можливість фіксувати дії користувачів та процесів у системі з метою виявлення порушень і встановлення відповідальних осіб.

Третя сторона — фізична або юридична особа, яка перебуває у договірних відносинах з Організацією та має доступ до її інформаційних ресурсів.

Цілісність інформації — гарантія того, що інформація є точною, актуальною та може змінюватися лише уповноваженими особами.

Шифрування — перетворення інформації у нечитабельний формат, доступний лише авторизованим користувачам.

VPN (Virtual Private Network) — захищений канал передачі даних через загальнодоступні мережі (інтернет).

Інші терміни, що вживаються у цій Політиці, застосовуються у значеннях, визначених чинним законодавством України.

1.3. Застосовані нормативні документи

Цю Політику розроблено на основі таких нормативних актів та стандартів:

1. Закон України «Про основні засади забезпечення кібербезпеки України»;
2. Закон України «Про інформацію»;
3. Закон України «Про захист персональних даних»;
4. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»;
5. Закон України «Про електронні документи та електронний документообіг»;
6. Закон України «Про правовий режим воєнного стану»;
7. Постанова КМУ №518 від 19.06.2019 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури»;
8. ISO/IEC 27001:2013 — Системи управління інформаційною безпекою. Вимоги;
9. ISO/IEC 27002:2013 — Звід правил з управління інформаційною безпекою;
10. ISO 27032 — Настанови з кібербезпеки;
11. ISO 27035 — Управління інцидентами інформаційної безпеки.

2. ОБОВ'ЯЗКИ ПРАЦІВНИКІВ

2.1. Вимоги до працівників

Працівники є першою і найважливішою лінією захисту інформаційного простору. Кожен працівник несе особисту (зокрема дисциплінарну та адміністративну) відповідальність за безпеку, цілісність та конфіденційність інформації, з якою він працює під час виконання службових обов'язків, незалежно від її формату — електронного чи паперового..

Захист робочого місця та обладнання

Кожен працівник зобов'язаний дбайливо ставитися до службового обладнання та вживати всіх доступних заходів для його фізичної безпеки та запобігання доступу сторонніх осіб.

Усі нові працівники проходять первинний інструктаж щодо правил інформаційної безпеки, використання та зберігання службових пристроїв.

Особливої обережності та підвищених заходів захисту вимагають робочі місця (комп'ютери) працівників, які здійснюють обробку персональних даних громадян, інформації з обмеженим доступом (службової, конфіденційної), військово-облікових даних, а також фінансово-економічної та кадрової документації.

Блокування екрана

Залишаючи робоче місце (навіть на короткий час), працівник зобов'язаний самостійно заблокувати екран комп'ютера (комбінацією клавіш Win + L або іншим визначеним способом). На всіх службових пристроях Організації налаштовується примусове автоматичне блокування екрана після 5 хвилин бездіяльності користувача..

Програмне забезпечення

На службових пристроях дозволено використання виключно ліцензійного, офіційно наданого або схваленого Організацією програмного забезпечення. Самостійне встановлення сторонніх програм, утиліт, розширень браузера, а також видалення або зміна системних налаштувань безпеки без попереднього погодження та дозволу відповідального за ІБ — категорично заборонені.

Дистанційна робота

Службові комп'ютери та ноутбуки, видані для дистанційної роботи, використовуються **виключно в службових цілях**. Самовільна зміна їх апаратної чи програмної конфігурації, підключення стороннього периферійного обладнання або передача пристроїв третім особам не допускається.

Право власності на обладнання та програмне забезпечення

Усе обладнання, програмне забезпечення, створені бази даних, напрацьовані інформаційні ресурси та документація, надані працівникам для виконання службових обов'язків, є власністю Організації (відповідно до балансової належності). Факт передачі матеріальних цінностей працівнику фіксується відповідним актом із зазначенням вичерпного переліку майна та інвентарних номерів.

Використання в робочих цілях програмного забезпечення з відкритим кодом або програм, придбаних за власні кошти працівника, допускається лише за погодженням з відповідальним за ІБ

та не тягне за собою виникнення майнових прав Організації на таке ПЗ, якщо інше не оформлено окремим договором..

2.2. Заборонена діяльність

Наведений перелік не є вичерпним — додаткові заборони містяться в інших розділах цієї Політики.

Умисне порушення роботи інформаційних систем

Будь-які навмисні дії, що призводять або можуть призвести до збою, уповільнення або некоректної роботи інформаційних систем Організації, категорично заборонені. Якщо встановлено, що збій стався внаслідок дій конкретного працівника, і такі дії повторюються — вони розглядаються як умисне порушення, навіть якщо працівник стверджує про їх випадковість.

Несанкціонований доступ до інформаційних ресурсів

Забороняється будь-яким способом намагатися отримати доступ до інформаційних ресурсів, систем або даних, до яких працівнику не надано офіційних прав доступу. Зокрема забороняється:

- запускати програми для підбору або злому паролів;
- сканувати локальну або зовнішню мережу з метою виявлення вразливостей;
- намагатися обійти будь-які технічні засоби захисту — брандмауери, паролі, системи автентифікації тощо.

Перегляд інформації без службової необхідності

Кожен працівник має доступ лише до тієї інформації, яка необхідна для виконання його безпосередніх службових обов'язків — це називається принципом мінімально необхідного доступу. Умисний перегляд, копіювання або використання інформації, до якої не надано офіційного доступу, суворо заборонені — навіть якщо технічна можливість такого доступу існує.

Завантаження шкідливого програмного забезпечення

Забороняється завантажувати, встановлювати або намагатися завантажити на службові пристрої будь-яке шкідливе програмне забезпечення — комп'ютерні віруси, трояни, шпигунські програми, програми-вимагачі та інше. Єдиний виняток — уповноважені особи, які проводять офіційно затверджену перевірку захищеності систем Організації.

Встановлення несанкціонованого або неліцензійного програмного забезпечення

На службових пристроях дозволяється використовувати виключно те програмне забезпечення, яке є ліцензійним і офіційно затвердженим до використання відповідальним за інформаційну безпеку. Забороняється:

- встановлювати особисте програмне забезпечення на службові пристрої;
- використовувати піратські копії програм;
- встановлювати будь-яке ПЗ без попереднього погодження з ВІБ.

Порушення умов використання програмного забезпечення

Забороняється порушувати або намагатися порушити умови ліцензійних угод будь-яких програмних продуктів, дозволених до використання на службових пристроях. Це включає використання програм у цілях, не передбачених ліцензією, або передачу ліцензійних ключів стороннім особам.

Використання службових систем з незаконною або неслужбовою метою

Службові інформаційні системи, пристрої та мережі призначені виключно для виконання посадових обов'язків. Забороняється використовувати їх для будь-якої діяльності, яка:

- є незаконною або суперечить чинному законодавству України;
- суперечить вимогам цієї Політики;
- завдає або може завдати шкоди репутації чи інтересам Організації.

2.3. Користування Інтернетом та електронною поштою

Інтернет та електронна пошта є виключно робочими інструментами, і їх цільове службове використання заохочується. Разом з тим, усі системи електронного зв'язку, облікові записи, інформаційні ресурси, повідомлення та дані, що генеруються, обробляються або зберігаються на технічних засобах Організації, є власністю Новотроїцької селищної ради, її виконавчих органів (як юридичних осіб) та Новотроїцької селищної військової адміністрації (відповідно до балансової належності та визначених законодавством повноважень на період воєнного стану), а не особистою власністю окремих працівників.

Ця Політика поширюється на всі засоби електронної комунікації, що використовуються у службовій діяльності — службову електронну пошту, месенджери, голосові повідомлення, офіційні чат-боти (зокрема Телеграм-бот), системи доступу до мережі Інтернет, а також на персональні комп'ютери, ноутбуки та інші кінцеві пристрої.

Службове та особисте використання

Усі надані працівникам інформаційні ресурси — комп'ютери, ноутбуки, електронна пошта, програмне забезпечення та доступ до інтернету — призначені насамперед для виконання службових обов'язків. Обмежене особисте використання допускається лише за умови, що воно:

- не відволікає від виконання службових обов'язків і не знижує продуктивності;
- не перешкоджає роботі Організації;
- не порушує жодного з наведених нижче обмежень.

Заборонені види використання

Незаконна діяльність та порушення авторських прав

Використання інформаційних ресурсів Організації для будь-якої незаконної діяльності суворо заборонено. Зокрема забороняється завантажувати, копіювати, розповсюджувати або використовувати піратське програмне забезпечення, музику, відео, книги та інші матеріали, що перебувають під захистом авторського права. Порушення авторських прав є не лише порушенням цієї Політики, а й злочином відповідно до законодавства України.

Комерційне використання в особистих цілях

Використання інформаційних ресурсів, обладнання або доступу до інтернету Організації для отримання особистої комерційної вигоди категорично заборонено. Це включає ведення власного бізнесу, рекламу особистих послуг або будь-яку іншу діяльність, що приносить особистий дохід.

Політична діяльність

Використання інформаційних ресурсів та обладнання Організації для будь-якої політичної діяльності — агітації, поширення політичних матеріалів, збору підписів або організації заходів на підтримку політичних сил — заборонено. Організація заохочує працівників брати участь у виборчому процесі як громадян, однак така участь не може здійснюватися з використанням службових ресурсів та в робочий час.

Переслідування та дискримінація

Забороняється використовувати будь-які засоби електронної комунікації Організації (корпоративну пошту, офіційні месенджери тощо) для створення, передачі, поширення або зберігання матеріалів, що є образливими, дискримінаційними або такими, що принижують людську гідність.

Зокрема, суворо забороняється:

- надсилати, розповсюджувати або зберігати матеріали непристойного, еротичного чи порнографічного характеру;
- поширювати повідомлення чи матеріали, які містять ознаки мови ворожнечі, расові, етнічні, релігійні чи гендерні образи, а також висловлювання, що можуть бути розтлумачені як погрози, залякування, цькування (мобінг) або дискримінація за будь-якою ознакою;
- використовувати службові канали зв'язку для ведення особистих суперечок, висловлення нецензурної лексики чи дій, що порушують Загальні правила етичної поведінки державних службовців та посадових осіб місцевого самоврядування.

Небажана та масова розсилка

Усі повідомлення, надіслані з використанням ресурсів Організації, мають бути адресними та мати пряме службове призначення. Забороняється розповсюджувати спам, «листи щастя», рекламні розсилки, несанкціоновані звернення або будь-які інші повідомлення масового характеру. Якщо працівник отримав подібне повідомлення — його необхідно видалити та нікому не пересилати.

Моніторинг електронних комунікацій

Організація залишає за собою право здійснювати моніторинг змісту електронних повідомлень та комунікацій, що генеруються або передаються з використанням службових інформаційних ресурсів. Моніторинг проводиться з метою захисту інформаційних систем, забезпечення ефективного використання ресурсів та дотримання вимог цієї Політики. Він може здійснюватися як постійно, так і вибірково.

2.4. Доступ до мережі Інтернет

За умов, коли персонал Організації працює дистанційно та використовує домашнє інтернет-з'єднання для виконання службових обов'язків, дотримання вимог цього розділу є обов'язковим для кожного працівника. Працівники несуть персональну відповідальність за безпечне використання домашньої мережі в службових цілях.

Вимоги до домашньої мережі

Працівники зобов'язані забезпечити належний захист мережі, що використовується для службової діяльності:

- роутер має бути захищений надійним паролем — не менше 12 символів, обов'язково відмінним від заводського стандартного пароля;

- мережа Wi-Fi повинна використовувати протокол шифрування WPA2 або WPA3. Використання застарілих протоколів WEP та WPA заборонено як небезпечних;
- рекомендується виділити для службових пристроїв окрему гостьову мережу Wi-Fi, відокремлену від особистих пристроїв домогосподарства.

Захист мережевого трафіку через Cisco Umbrella

На всіх службових пристроях встановлено та активовано агент хмарного захисту Cisco Umbrella, який забезпечує фільтрацію інтернет-трафіку, блокування шкідливих ресурсів та захист DNS-запитів незалежно від того, яка мережа використовується для підключення. Деактивація або обхід Cisco Umbrella будь-яким способом категорично заборонені. У разі отримання попереджень або блокувань з боку системи — працівник зобов'язаний негайно повідомити ВІБ.

Заборонені дії під час виконання службових обов'язків

Під час використання службових пристроїв та виконання службових обов'язків забороняється:

- відвідувати ігрові сайти, торент-ресурси, файлообмінники, вебресурси з еротичним чи порнографічним контентом, розважальні чати, онлайн-платформи обміну медіафайлами, а також будь-які ресурси та сервіси країни-агресора (зокрема з доменною зоною .ru);
- передавати конфіденційну або службову інформацію — паролі, персональні дані громадян, службові документи тощо — у незашифрованому вигляді через відкриті канали зв'язку;
- допускати до службового пристрою або службових облікових записів третіх осіб, включаючи членів родини та близьких;
- підключатися до публічних або незахищених Wi-Fi мереж (кафе, транспорт, готелі) без активного VPN-з'єднання;
- вимикати або обходити будь-які засоби захисту, встановлені на службових пристроях.

Обов'язки відповідального за інформаційну безпеку

Відповідальний за ІБ зобов'язаний:

- забезпечити кожного працівника, який працює дистанційно, письмовою інструкцією з налаштування безпечної домашньої мережі до початку дистанційної роботи;
- вести актуальний облік виданих дозволів на встановлення програмного забезпечення на службових пристроях;
- здійснювати моніторинг інтернет-активності працівників засобами Cisco Umbrella у межах, визначених чинним законодавством України;
- забезпечувати, щоб у відкритому публічному доступі розміщувалася виключно інформація, призначена для публічного використання;
- регулярно перевіряти журнали подій Cisco Umbrella та реагувати на виявлені аномалії або загрози.

2.5. Повідомлення про несправності

Користувачі повинні інформувати керівництво про випадки, коли програмне забезпечення робочої станції не функціонує належним чином. Несправне програмне забезпечення становить ризик для інформаційної безпеки. Якщо користувач, або керівник користувача, підозрює зараження робочої станції вірусом, слід негайно вжити наступних заходів:

- припинити використання комп'ютера;
- не запускати на виконання ніяких команд, включаючи команду збереження даних;
- не закривати жодного з вікон або програм комп'ютера;
- не вимикати комп'ютер або периферійний пристрій на самому екрані;
- по можливості фізично відключити комп'ютер від мереж живлення та локальної мережі;

- повідомити про ураження робочої станції відповідального за ІБ, вказавши ознаки незвичайної поведінки комп'ютера (блокування екрану, виникнення несподіваного доступ до системного диска, незвичайна реакція на команди тощо) і час, коли це було вперше помічено;
- повідомити про будь-які зміни у використанні апаратного чи програмного забезпечення, які передували несправності;
- не намагатися самостійно видалити підозрілий файл!

Відповідальний з ІБ повинен вжити заходи для усуненням несправності, а також повідомити вище керівництво про результати цих дій з рекомендаціями щодо подальших кроків для запобігання подібних випадків у майбутньому.

2.6. Повідомлення про інциденти безпеки

Кожен працівник, який має доступ до інформаційних ресурсів та цифрових активів Організації, зобов'язаний негайно повідомляти про виявлені інциденти інформаційної безпеки. Своєчасне повідомлення — це не лише обов'язок, а й особистий внесок кожного у захист спільних ресурсів.

Що вважається інцидентом інформаційної безпеки

Працівник зобов'язаний повідомити про інцидент у разі:

- отримання підозрілого електронного листа з вкладеннями або посиланнями, особливо з терміновими закликами до дії — «негайно відкрийте», «оновіть дані», «перевірте рахунок» тощо;
- випадкового відкриття підозрілого вкладення або переходу за невідомим посиланням;
- появи незвичної (аномальної) поведінки операційної системи — уповільнення роботи, виконання несанкціонованих користувачем операцій, запуску невідомих програм чи появи спливаючих вікон;
- виявлення несанкціонованого доступу до службових облікових записів або підозри на компрометацію пароля;
- втрати або крадіжки службового пристрою чи носія інформації;
- виявлення витоку службової або конфіденційної інформації;
- будь-яких інших подій, що можуть свідчити про порушення інформаційної безпеки.

Дії працівника під час інциденту

У разі виявлення або підозри на інцидент працівник зобов'язаний:

- **негайно** повідомити свого безпосереднього керівника та відповідального за ІБ — не чекаючи підтвердження того, що інцидент справді стався;
- **не видаляти** підозрілі листи, файли або повідомлення до завершення розслідування — вони є доказами;
- **відключити** уражений пристрій від мережі, якщо є підозра на зараження шкідливим програмним забезпеченням;
- **не намагатися** самостійно усунути наслідки інциденту або встановити його причину — це завдання відповідального за ІБ;
- **зафіксувати** обставини події — час, що сталося, які дії передували інциденту.

Обов'язки відповідального за ІБ

Відповідальний за ІБ зобов'язаний:

- реагувати на повідомлення про інцидент якнайшвидше та вживати заходів відповідно до Плану реагування на інциденти інформаційної безпеки;
- зареєструвати кожен інцидент у журналі інцидентів інформаційної безпеки із зазначенням дати, опису події, вжитих заходів та результату;
- провести аналіз кожного інциденту з метою встановлення його причин та визначення необхідних змін у системі захисту;
- організувати навчання персоналу у разі внесення змін до Плану реагування на інциденти за результатами розслідування;
- у разі підозри на порушення законодавства України — невідкладно звернутися до правоохоронних органів.

Розслідування внутрішніх порушень

Внутрішні порушення інформаційної безпеки розслідуються у найкоротші строки. Оцінка ступеня критичності інциденту та прийняття рішення про доцільність проведення внутрішнього розслідування здійснюється відповідальним за ІБ протягом 24 годин (або не пізніше наступного робочого дня) з моменту отримання повідомлення.

Офіційне внутрішнє розслідування розпочинається не пізніше 48 годин з моменту фіксації інциденту і має бути завершене протягом 10 робочих днів (з правом продовження керівником до 30 днів у разі особливої складності).

У разі, якщо інцидент безпеки призвів (або з високою ймовірністю міг призвести) до випадкового чи незаконного знищення, втрати, зміни, несанкціонованого розголошення або доступу до персональних даних, Організація зобов’язана невідкладно, але не пізніше ніж протягом 72 годин з моменту виявлення такого інциденту, повідомити про це Уповноваженого Верховної Ради України з прав людини. Організація документує всі факти, пов’язані з такими інциндами, їх наслідки та вжиті заходи реагування.

Розслідування проводиться на засадах конфіденційності. Факт повідомлення про інцидент не може бути підставою для будь-яких негативних наслідків (дисциплінарного чи психологічного тиску) щодо працівника, який повідомив про нього добросовісно. Замовчування відомого працівнику інциденту або приховування його наслідків, навпаки, розглядається як грубе порушення цієї Політики та є підставою для притягнення до дисциплінарної відповідальності.

2.7. Передача конфіденційної інформації

Конфіденційна інформація може передаватися в електронному вигляді, на цифрових носіях або у паперовій формі виключно в межах виконання службових обов'язків та лише уповноваженим особам.

2.7.1 Загальні правила передачі

Особа, яка отримала конфіденційну інформацію, зобов'язана:

- забезпечити її зберігання та захист відповідно до вимог цієї Політики та умов, встановлених особою, що її надала;
- не передавати отриману інформацію третім особам без відповідного дозволу;
- використовувати отриману інформацію виключно з тією метою, для якої вона була надана.

2.7.2 Передача електронними засобами зв'язку

При передачі конфіденційної інформації електронними каналами працівник зобов'язаний:

- використовувати виключно корпоративну електронну пошту на домені Організації — використання особистих поштових скриньок для передачі службової інформації заборонено;
- переконатися у правильності адреси отримувача перед надсиланням — помилково надіслана конфіденційна інформація є інцидентом безпеки і про неї необхідно негайно повідомити ВІБ;
- не передавати конфіденційну інформацію через незахищені месенджери та соціальні мережі;
- використовувати шифрування при передачі документів, що містять персональні дані громадян, фінансову або іншу чутливу інформацію.

2.7.3 Передача на цифрових носіях

При передачі конфіденційної інформації на зовнішніх носіях (флешки, диски тощо):

- носій має передаватися особисто уповноваженій особі (під підпис у відповідному журналі обліку) або надсилатися засобами поштового зв'язку (цінною посилкою/листом з описом вкладення) чи сертифікованою кур'єрською службою доставки з обов'язковим повідомленням про вручення;
- конфіденційні дані на носії мають бути зашифровані;
- використання особистих носіїв для передачі службової інформації заборонено — використовуються лише носії, що належать Організації та обліковані ВІБ.

2.7.4 Передача у паперовій формі

При передачі конфіденційної інформації у паперовому вигляді:

- документи передаються особисто (нарочно) або надсилаються засобами поштового зв'язку (рекомендованим листом, листом з оголошеною цінністю та описом вкладення) чи кур'єрською службою з обов'язковим письмовим або електронним підтвердженням отримання;
- не допускається залишати конфіденційні документи у доступних для сторонніх осіб місцях;
- копіювання конфіденційних документів здійснюється лише за службовою необхідністю та з дотриманням заходів захисту;
- після використання конфіденційні паперові документи знищуються у спосіб, що унеможливлює їх відновлення та прочитання.

2.7.5 Передача інформації третім особам

Передача конфіденційної інформації Організації стороннім особам або організаціям допускається виключно:

- на підставі законодавчих вимог або офіційного запиту уповноваженого органу;
- за наявності письмового дозволу начальника військової адміністрації або уповноваженої ним особи.

2.7.6. Обов'язки щодо взаємодії з Уповноваженим ВРУ з прав людини

Працівники Організації, до повноважень яких належить розгляд запитів Уповноваженого Верховної Ради України з прав людини, зобов'язані забезпечити правомірне, повне та вчасне надання запитуваної інформації та матеріалів, зокрема тих, що стосуються додержання прав і свобод людини, доступу до публічної інформації та захисту персональних даних.

Передача інформації на запит Уповноваженого здійснюється виключно через захищені канали зв'язку або в установленому паперовому/електронному вигляді з метою запобігання витоку інформації під час її транспортування».

2.8. Передача даних та програмного забезпечення

Програмне забезпечення, що не дозволене до використання в Організації, не рекомендується встановлювати на пристрої, з яких здійснюється доступ до службових ресурсів — навіть якщо це особистий комп'ютер працівника. Кожна додаткова програма є потенційною точкою вразливості, через яку зловмисники можуть отримати доступ до службових даних. Якщо працівник має службову потребу у конкретному програмному забезпеченні, він може звернутися із запитом до свого безпосереднього керівника.

Службові дані — відомості про працівників, фінансова інформація, документи кадрового характеру та будь-яка інша службова інформація — не повинні зберігатися на особистих пристроях без нагальної службової необхідності. Особистий комп'ютер може не мати належного рівня захисту, а Організація не має технічної можливості гарантувати безпеку даних на пристроях, що їй не належать.

У разі виникнення такої необхідності працівник повідомляє свого керівника, який оцінює обґрунтованість запиту та за потреби погоджує його з відповідальним за ІБ.

2.9. Шифрування електронної пошти та даних

При передачі конфіденційної або службової інформації електронними каналами зв'язку працівник зобов'язаний оцінити ризик того, що така інформація може потрапити до сторонніх осіб. Якщо такий ризик існує — передача здійснюється виключно у зашифрованому вигляді.

Для шифрування файлів перед надсиланням електронною поштою використовується програмне забезпечення, погоджене з відповідальним за ІБ. Це може бути архіватор із захистом паролем або інший засіб шифрування — головне, щоб отримувач також мав можливість розшифрувати отримані дані. Пароль для розшифрування передається отримувачу окремим каналом зв'язку — наприклад, телефоном або в окремому повідомленні, але не разом із зашифрованим файлом.

Працівник, який має потребу у використанні конкретного програмного забезпечення для шифрування, звертається за дозволом до відповідального за ІБ. Самостійне використання незатверджених засобів шифрування не допускається, оскільки це може ускладнити відновлення даних у разі інциденту.

Шифрування є обов'язковим при передачі персональних даних громадян, фінансової інформації, відомостей про працівників та будь-яких інших даних, несанкціоноване розкриття яких може завдати шкоди Організації або третім особам.

3. КЛАСИФІКАЦІЯ ІНФОРМАЦІЇ

Уся інформація, що обробляється, зберігається або передається в Організації, поділяється на три категорії залежно від її чутливості та можливих наслідків розкриття.

Відкрита інформація — інформація, призначена для публічного доступу та поширення. До неї належать офіційні рішення ради, оголошення, публічні звіти, матеріали сайту громади та сайту ЦНАП, інформація Телеграм-бота громади «СВОЇ». Розкриття такої інформації не завдає шкоди Організації або громадянам.

Службова інформація — інформація, доступ до якої обмежений колом уповноважених працівників і яка використовується виключно для виконання службових обов'язків. До неї належать внутрішнє листування, проекти документів, протоколи нарад, кадрові документи, фінансові звіти та плани, інформація про інформаційні системи Організації. Розголошення службової інформації може завдати шкоди діяльності Організації або її працівникам.

Конфіденційна інформація — інформація з найвищим рівнем захисту, несанкціоноване розкриття якої може завдати суттєвої шкоди громадянам, Організації або державі. До неї належать персональні дані громадян, облікові дані для доступу до державних реєстрів та порталів, паролі та ключі шифрування, кваліфіковані електронні підписи, дані про вразливості інформаційних систем. Конфіденційна інформація передається виключно у зашифрованому вигляді та лише уповноваженим особам.

Кожен працівник зобов'язаний визначати категорію інформації, з якою він працює, та застосовувати відповідні заходи захисту. У разі сумніву щодо категорії — інформація вважається конфіденційною до отримання роз'яснення від ВІБ або керівника.

Класифікація інформації Організації та встановлення режимів доступу до неї (конфіденційна, службова) не можуть перешкоджати реалізації законних повноважень Уповноваженого Верховної Ради України з прав людини. Надання інформації, документів (їх копій), у тому числі тих, що містять персональні дані чи інформацію з обмеженим доступом, на запит Уповноваженого ВРУ з прав людини здійснюється невідкладно (або у строки, визначені законодавством про Уповноваженого), з дотриманням заходів технічного захисту інформації та відповідно до вимог Закону України "Про Уповноваженого Верховної Ради України з прав людини".

4. УПРАВЛІННЯ ДОСТУПОМ ДО ДЕРЖАВНИХ РЕЄСТРІВ ТА ПОРТАЛІВ

Працівники Організації мають доступ до державних реєстрів, інформаційних систем та порталів у зв’язку з виконанням посадових обов’язків. Цей доступ є особливо чутливим, оскільки передбачає обробку персональних даних громадян та відомостей, що становлять державний інтерес.

Надання та обмеження доступу

Доступ до кожного державного реєстру або порталу надається виключно тим працівникам, для яких це передбачено їхніми посадовими обов'язками. Кожен працівник має власний персональний обліковий запис — використання спільних облікових даних категорично заборонено.

Правила роботи з реєстрами

Під час роботи з державними реєстрами та порталами працівник зобов'язаний здійснювати лише ті дії, які передбачені його службовими обов'язками — перегляд, внесення або редагування даних виключно в межах наданих повноважень. Категорично забороняється здійснювати пошук інформації або перегляд даних у реєстрах з особистих мотивів чи на приватне прохання третіх осіб. Після завершення роботи з реєстром необхідно виконати вихід з облікового запису — залишати активний сеанс без нагляду заборонено. Відомості, отримані з державних реєстрів, використовуються виключно в службових цілях і не передаються стороннім особам без законних підстав.

Захист облікових даних

Облікові дані для доступу до державних реєстрів зберігаються відповідно до вимог парольної політики цієї Політики. При підозрі на компрометацію облікових даних або втрату/викрадення носія з КЕП працівник негайно повідомляє відповідального за ІБ та змінює пароль. У разі виявлення несанкціонованого доступу до реєстру — повідомляється як відповідальний за ІБ, так і адміністратор відповідного реєстру.

Надання представникам Уповноваженого ВРУ з прав людини доступу до інформаційних систем чи реєстрів Організації з метою здійснення ними моніторингу захисту персональних даних/права на інформацію здійснюється виключно на підставі закону, за розпорядженням керівника та під контролем відповідального за інформаційну безпеку

5. УПРАВЛІННЯ ДОСТУПОМ

5.1. Встановлення паролів

3.1.1 Ідентифікатор користувача та пароль є основним засобом підтвердження особи при отриманні доступу до мереж, інформаційних систем та службових пристроїв Організації. Усі паролі мають відповідати вимогам цього розділу, що забезпечує їх стійкість до підбору та злому.

3.1.2 Пароль має складатися не менше ніж з дванадцяти символів та містити комбінацію літер латинського алфавіту верхнього і нижнього регістру, цифр та спеціальних символів. Пароль, що складається лише з літер або лише з цифр, не відповідає вимогам цієї Політики.

3.1.3 Пароль підлягає обов'язковій зміні кожні 60 днів. У разі підозри на компрометацію пароля — його необхідно змінити негайно, не чекаючи планової зміни, та повідомити про це відповідального за ІБ. При повторному встановленні пароля забороняється використовувати будь-який із трьох попередніх паролів.

Пароль є суворо конфіденційною інформацією. Передавати пароль іншим працівникам, записувати його на папері, зберігати у незахищеному текстовому файлі на робочій станції або надсилати електронною поштою категорично заборонено. Паролі зберігаються виключно у зашифрованому вигляді — для цього рекомендується використовувати затверджений менеджер паролів. При введенні пароль маскується на екрані та не відображається у журналах, звітах або будь-якій іншій документації.

5.2. Угода про конфіденційність

Усі працівники Організації підписують Зобов'язання про нерозголошення конфіденційної інформації та персональних даних (далі — Зобов’язання, Додаток 1). Підписання цього документа є обов'язковою передумовою для отримання доступу до будь-яких інформаційних ресурсів, систем та реєстрів Організації.

Працівники, з якими укладено строкові трудові договори, особи, які проходять стажування (практику), а також представники сторонніх підрядних організацій (фізичні особи-підприємці, працівники юридичних осіб, які надають Організації послуги з технічної підтримки, розробки ПЗ тощо), зобов'язані підписати Зобов’язання або відповідну угоду про конфіденційність (Non-Disclosure Agreement) до моменту отримання будь-якого (зокрема гостьового чи тимчасового) доступу до робочих місць, мережі чи інформаційних ресурсів Організації. Угода містить підтвердження того, що працівник розуміє: будь-яке несанкціоноване використання або розголошення конфіденційної інформації може призвести до відповідальності згідно з чинним законодавством України та цією Політикою.

Підписанням Зобов’язання працівник підтверджує, що він ознайомлений із кримінальною, адміністративною, цивільно-правовою та дисциплінарною відповідальністю за незаконне збирання, зберігання, використання, замовчування або розголошення інформації з обмеженим

доступом та персональних даних громадян, які стали йому відомі під час виконання посадових обов'язків.

Відповідно до статті 43 Закону України «Про запобігання корупції», працівникам Організації суворо забороняється розголошувати або використовувати в інший спосіб персональні дані чи іншу непублічну інформацію, що стала їм відома у зв’язку з виконанням службових або посадових повноважень, за винятком випадків, прямо передбачених законом.

У разі зміни посади, переведення до іншого структурного підрозділу або суттєвого розширення прав доступу до інформаційних систем, Зобов'язання за потреби переглядається або підписується за новою формою.

При припиненні трудових відносин або дії цивільно-правових договорів, у день звільнення (останній день роботи) особа підписує окреме фінальне підтвердження про те, що чинність її обов'язку щодо нерозголошення та невикористання конфіденційної інформації, персональних даних та непублічної інформації продовжується безстроково після припинення діяльності, пов'язаної з виконанням функцій Організації.

5.3 З'єднання та підключення

Будь-який доступ до інформаційних ресурсів Організації через зовнішні мережі підлягає обов'язковій авторизації та автентифікації. Підключення до службових систем без проходження через встановлені засоби контролю доступу заборонено.

У випадку, коли працівники Організації працюють дистанційно та підключаються до службових ресурсів через домашній інтернет, захист мережевого з'єднання забезпечується хмарним рішенням Cisco Umbrella, встановленим на всіх службових пристроях. Cisco Umbrella здійснює фільтрацію трафіку та захист від шкідливих ресурсів незалежно від місця підключення працівника.

Якщо працівник має службову потребу підключитися до зовнішнього ресурсу, системи або мережі у спосіб, що виходить за межі стандартного доступу, він зобов'язаний отримати попередній дозвіл відповідального за ІБ. Самостійне встановлення будь-яких додаткових каналів зв'язку, тунелів або засобів віддаленого доступу без погодження з відповідальним за ІБ заборонено.

6. АНТИВІРУСНИЙ ЗАХИСТ

6.1. Встановлення та оновлення антивірусного ПЗ

Антивірусне програмне забезпечення встановлюється на всіх службових пристроях — комп'ютерах, ноутбуках та будь-якому іншому кінцевому обладнанні, що використовується для виконання службових обов'язків. Оновлення антивірусних баз даних відбувається автоматично.

6.2. Перевірка нового програмного забезпечення

На службових пристроях використовується виключно програмне забезпечення, дозволене до використання. Перелік дозволеного програмного забезпечення наведено у Додатку 2.

Усі файли та програми, отримані електронними каналами зв'язку, підлягають обов'язковій перевірці антивірусним програмним забезпеченням одразу після отримання та до їх відкриття або запуску.

Зовнішні носії інформації — флешки, USB-накопичувачі, компакт-диски — є потенційним джерелом шкідливого програмного забезпечення. Тому будь-який зовнішній носій перед використанням обов'язково сканується антивірусним програмним забезпеченням. Завантаження комп'ютера із зовнішнього носія, отриманого з невідомого або неперевіреного джерела, заборонено. Зовнішні носії мають бути вилучені з комп'ютера одразу після завершення роботи з ними.

6.3. Збереження права власності на програмне забезпечення

Усе програмне забезпечення та документація, надані працівникам для виконання службових обов'язків, є власністю Організації, якщо інше не передбачено окремим договором. Програмне забезпечення, придбане працівником за власні кошти, залишається його особистою власністю.

7. КРИПТОГРАФІЧНИЙ ЗАХИСТ

7.1. Загальні положення

Криптографічний захист (шифрування) в Організації застосовується для забезпечення конфіденційності та цілісності інформації під час її зберігання на матеріальних носіях, передачі електронними каналами зв'язку, а також для автентифікації користувачів і підтвердження юридичної сили документів за допомогою кваліфікованого електронного підпису (КЕП). Усі криптографічні засоби, що використовуються в Організації, мають бути сертифіковані відповідно до вимог законодавства України у сфері технічного захисту інформації..

7.2. Безпека ключів та паролів шифрування

Технічні правила шифрування конфіденційних файлів перед їх відправленням здійснюються відповідно до вимог розділу 2.7 цієї Політики. При використанні зашифрованих архівів чи папок, пароль для їх розшифрування генерується відповідно до вимог парольної політики Організації.

Категорично забороняється передавати пароль (ключ) розшифрування в одному повідомленні або в межах одного каналу зв'язку разом із зашифрованим файлом. Пароль передається отримувачу виключно альтернативним (окремим) засобом комунікації (наприклад, якщо файл надіслано електронною поштою, пароль повідомляється телефоном або в захищеному месенджері).**7.3.**

7.3. Кваліфікований електронний підпис

Кваліфікований електронний підпис (КЕП) є персональним інструментом посадової особи. Працівник несе повну особисту відповідальність за збереження та правомірність використання свого КЕП. Особисті ключі КЕП повинні зберігатися на захищених носіях (токенах) або у вигляді зашифрованих файлових контейнерів на оптимізованих для цього службових ресурсах.

Забороняється:

- залишати апаратні носії КЕП (токени, флешки) підключеними до комп'ютера без нагляду або після завершення робочого дня;
- передавати носій КЕП та PIN-код до нього іншим працівникам чи третім особам (навіть для виконання термінових службових завдань);
- зберігати PIN-коди у відкритому вигляді на паперових нотатках поруч із робочим місцем або у текстових файлах на комп'ютері.

7.4. Захищений веб-протокол HTTPS та SSL-сертифікат

Усі офіційні веб-ресурси Організації (зокрема офіційний сайт громади, портал ЦНАП та інші інформаційні системи) обов'язково захищаються діючими SSL/TLS-сертифікатами для забезпечення шифрування за протоколом HTTPS. Відповідальний за ІБ забезпечує моніторинг та своєчасне поновлення SSL/TLS-сертифікатів до закінчення строку їх дії.

Вхід працівників до державних реєстрів, відомчих порталів чи внутрішніх робочих систем Організації дозволяється виключно через захищене шифроване з'єднання. Якщо веб-браузер видає попередження про небезпечне з’єднання, незахищений протокол (HTTP замість HTTPS) або недійсний (прострочений) сертифікат безпеки — працівник зобов'язаний негайно припинити роботу на цьому ресурсі, не вводити жодних облікових даних та терміново повідомити відповідального за ІБ.

8. ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПРИ ДИСТАНЦІЙНІЙ РОБОТІ

8.1. Загальні положення

Вимоги цього розділу застосовуються до всіх працівників Організації у разі виконання ними службових (посадових) обов'язків поза межами офіційних адміністративних приміщень Організації (дистанційна або надомна робота, робота в умовах евакуації, відрядження тощо), незалежно від того, чи встановлено такий режим тимчасово (на період дії воєнного стану, карантину), чи на постійній основі для окремих посад.

Дистанційна робота створює підвищені ризики для інформаційної безпеки та комплаєнсу, тому працівники під час роботи поза офісом несуть підвищену особисту відповідальність за збереження обладнання та захист інформації, до якої вони мають доступ.

Працівник, що працює дистанційно, дотримується всіх вимог цієї Політики без винятків. Доступ надається лише до тих ресурсів та інформації, які необхідні для виконання конкретних службових завдань. Паролі не записуються у доступних для сторонніх місцях і не повідомляються членам родини або іншим особам.

8.2. Організація віддаленого робочого місця та обладнання

Для виконання службових обов'язків у дистанційному режимі працівникам за розпорядженням керівника та відповідно до балансової належності може надаватися службове обладнання (ноутбуки, планшети, засоби зв'язку).

Використання працівниками власних (особистих) технічних засобів для службових цілей допускається як виняток лише за погодженням із відповідальним за ІБ та за умови повного налаштування на цих пристроях засобів захисту інформації, визначених цією Політикою.

Працівник, який працює дистанційно, зобов'язаний самостійно забезпечити:

- фізичну безпеку пристроїв та неможливість доступу до них третіх осіб (включаючи членів родини та близьких);
- візуальну конфіденційність (екран комп’ютера з робочими даними або державними реєстрами не повинен бути помітним стороннім особам);
- безпечний та стабільний доступ до мережі Інтернет;
- утилізацію паперових чернеток чи документів, що містять службову інформацію, у спосіб, що унеможливлює їх відновлення та прочитання (шредери тощо).

8.3. Технічний захист відділених пристроїв

На всіх пристроях, що використовуються для дистанційної роботи, обов'язково має бути встановлене, активоване та постійно оновлюване антивірусне програмне забезпечення відповідно до вимог Розділу 6 цієї Політики.

Додатковий мережевий захист та контент-фільтрація віддалених робочих місць забезпечується хмарним рішенням Cisco Umbrella, яке має функціонувати на всіх службових пристроях незалежно від точки їх підключення до Інтернету. Навмисне вимкнення, видалення або обхід системи Cisco Umbrella працівником суворо заборонено.

Залишаючи віддалене робоче місце навіть на короткий час, працівник зобов'язаний примусово блокувати екран. Налаштування автоматичного блокування екрана зафіксовано на рівні не більше 5 хвилин бездіяльності.

8.4. Безпека передачі даних та підключень

Доступ віддалених працівників до внутрішніх інформаційних ресурсів, баз даних Організації та державних реєстрів здійснюється виключно з використанням персональних облікових даних (логін, пароль, КЕП) та лише в межах, необхідних для виконання посадових функцій.

Будь-яка передача конфіденційної інформації та персональних даних в електронному вигляді здійснюється виключно через захищені канали зв'язку відповідно до вимог Розділу 2.7 та Розділу 7 цієї Політики.

У разі вимушеного підключення до Інтернету через публічні або незахищені бездротові мережі (у транспорті, готелях, закладах харчування, відкритих зонах Wi-Fi) працівник **зобов'язаний використовувати активне зашифроване VPN-з'єднання** для захисту трафіку від перехоплення.

Резервне копіювання критично важливих робочих даних, що зберігаються на віддаленому пристрої, здійснюється працівником регулярно відповідно до процедур, визначених у Розділі 10 цієї Політики.

9. ПОЛІТИКА ЧИСТОГО СТОЛУ/ЕКРАНУ

Політика чистого столу та чистого екрану спрямована на зниження ризику несанкціонованого доступу до інформації, її витоку або пошкодження як у робочий час, так і після його завершення. Виконання цих правил є однаково обов'язковим як під час роботи в адміністративних приміщеннях, так і в умовах дистанційної роботи, коли робоче місце знаходиться у домашньому чи іншому позаофісному середовищі, де можуть бути присутні треті особи.

Вимоги до робочого місця

Під час робочого дня паперові документи, що містять конфіденційну, службову або персональну інформацію, не повинні залишатися на столі без нагляду працівника. Наприкінці робочого дня, у разі тривалої відсутності або оголошення сигналу повітряної тривоги (евакуації), працівник зобов'язаний прибрати всі робочі документи та матеріальні носії інформації (флешки, токени КЕП) у недоступне для сторонніх осіб місце (сейфи, замикані шафи, шухляди або спеціальні кейси для зберігання документів вдома). Роздруковані документи, що містять службові чи персональні дані, повинні вилучатися з лотка принтера (багатофункціонального пристрою) негайно після завершення процесу друку.

Вимоги до екрану пристрою

Екран комп'ютера або ноутбука розміщується таким чином, щоб інформація на ньому (особливо інтерфейси державних реєстрів) була невидимою для сторонніх осіб.

Комп'ютер примусово блокується працівником щоразу при залишенні робочого місця — навіть на короткий час. Автоматичне примусове блокування екрана налаштовується на спрацювання через 5 хвилин бездіяльності.

На кожному пристрої має бути активоване обов’язкове введення пароля користувача при запуску операційної системи, а також при виході з режиму сну або очікування.

Після завершення виконання конкретного завдання здійснюється вихід з усіх систем та баз даних (веб-сесій реєстрів), до яких був отриманий доступ. Наприкінці робочого дня комп'ютер обов'язково вимикається (або переводиться у режим повного глибокого сну з шифруванням диска).

Зберігання паролів

Категорично забороняється фіксувати паролі чи PIN-коди на паперових носіях (зокрема на стікерах, самоклейних записах, розташованих на моніторі, під клавіатурою чи на робочому столі), а також зберігати їх у відкритих текстових файлах на комп'ютері. Порядок безпечного поводження з паролями регламентується іншими розділами цієї Політики.

10. РЕЗЕРВНЕ КОПІЮВАННЯ ДАНИХ

Резервне копіювання є обов'язковим заходом захисту від втрати даних внаслідок технічних збоїв, кібератак, випадкового видалення або інших інцидентів. Відповідальний за ІБ організовує та контролює виконання процедури резервного копіювання в Організації.

Що підлягає резервному копіюванню

Обов'язковому резервному копіюванню підлягають службові документи та бази даних Організації, дані веб-ресурсів — сайту громади та сайту ЦНАП, дані корпоративної електронної пошти, конфігурації інформаційних систем та налаштування програмного забезпечення.

Частота та зберігання резервних копій

Резервне копіювання веб-ресурсів здійснюється не рідше одного разу на тиждень. Резервне копіювання службових документів та баз даних здійснюється не рідше одного разу на місяць або після внесення значних змін. Резервні копії зберігаються в місці, фізично або логічно відокремленому від основних даних. Резервні копії, що містять конфіденційну інформацію, зберігаються у зашифрованому вигляді. Строк зберігання резервних копій — не менше шести місяців.

Перевірка резервних копій

Відповідальний за ІБ не рідше одного разу на квартал перевіряє можливість відновлення даних з резервної копії. Результати перевірки фіксуються у журналі. Резервна копія, з якої неможливо відновити дані, вважається непридатною і підлягає заміні.

Відновлення даних

Відновлення даних з резервної копії здійснюється за рішенням відповідального за ІБ або начальника військової адміністрації у разі втрати, пошкодження або знищення основних даних. Факт відновлення фіксується у журналі інцидентів.

11. НАВЧАННЯ ТА ПІДВИЩЕННЯ ОБІЗНАНОСТІ В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

Підвищення обізнаності працівників є базовим елементом системи кіберзахисту Організації. Оскільки більшість успішних кібератак використовують людський фактор (соціальну інженерію), регулярне навчання є обов'язковим для всіх без винятку працівників Організації, включаючи керівний склад..

11.1. Види та періодичність навчальних заходів

Відповідальний за ІБ забезпечує безперервний процес підвищення кваліфікації персоналу за такими напрямами:

- Первинний (вступний) інструктаж: проводиться для кожного нового працівника (або залученого за цивільно-правовим договором спеціаліста) у перший день його роботи, до моменту надання йому доступу до комп'ютерного обладнання, внутрішньої мережі чи державних реєстрів.
- Планові навчання: проводяться для всіх працівників Організації не рідше одного разу на шість місяців з метою освіження знань та розбору поточних трендів у сфері кіберзагроз.
- Позапланові навчання: організовуються у терміновому порядку у разі:

    - внесення суттєвих змін до цієї Політики;
    - впровадження нового програмного забезпечення, систем автоматизації чи засобів захисту;
    - виявлення масованих кібератак на державний сектор чи критичну інфраструктуру України;
    - за результатами розслідування реальних інцидентів безпеки в Організації (для запобігання їх повторенню).

11.2. Формат проведення та залучення експертів

Враховуючи дистанційний режим роботи Організації, навчання та інструктажі можуть проводитися як в очному форматі, так і дистанційно — за допомогою засобів відеоконференцзв’язку (із обов'язковою верифікацією присутності працівників).

Для підвищення якості навчання Відповідальний за ІБ має право залучати зовнішніх профільних експертів: фахівців держорганів (ДССЗЗІ, Кіберполіції), розробників відомчого софту, а також використовувати сертифіковані державні онлайн-курси з кібергігієни (наприклад, на платформі Дія.Освіта).

11.3. Методичні матеріали та оперативне інформування

Відповідальний за ІБ розробляє, підтримує в актуальному стані та доводить до кожного працівника під підпис (електронний або фізичний) стислу Пам'ятку з інформаційної безпеки (кібергігієни), яка містить ключові правила з цієї Політики у форматі швидких інструкцій.

У разі виявлення цілеспрямованих фішингових розсилок, нових критичних вразливостей або специфічних загроз для органів місцевого самоврядування, Відповідальний за ІБ здійснює оперативне розсилання попереджень та інструкцій через офіційні внутрішні канали комунікації (робоча пошта, захищені чати). Працівники зобов'язані негайно ознайомлюватися з такими повідомленнями.

11.4. Контроль знань та фіксація результатів

Враховуючи дистанційний режим роботи Організації, факт проходження працівниками інструктажів та навчань фіксується виключно в електронному вигляді (шляхом реєстрації та збереження лог-файлів у внутрішній системі тестування, збирання відповідей через офіційні корпоративні Google-форми, або шляхом ведення Електронного журналу обліку навчань, який завіряється КЕП Відповідального за ІБ).

Перевірка знань за результатами планових та позапланових навчань здійснюється у формі дистанційного онлайн-тестування. Додатково Відповідальний за ІБ має право проводити профілактичний контроль обізнаності працівників за допомогою імітованих (тестових) фішингових розсилок на службові електронні скриньки.

У разі, якщо працівник демонструє незадовільні результати онлайн-тестування або відкриває посилання/вкладення під час імітованої фішингової атаки, такий працівник зобов'язаний:

- протягом 3-х робочих днів повторно самостійно опрацювати Пам'ятку з ІБ та пройти додатковий індивідуальний онлайн-інструктаж з Відповідальним за ІБ;
- пройти повторне дистанційне тестування для підтвердження успішного засвоєння матеріалу».

12. ПОРЯДОК РЕАГУВАННЯ НА ІНЦИДЕНТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

12.1 Нормативна основа та координація

Процедури реагування на події у кіберпросторі в Організації регламентуються окремим нормативно-правовим актом — Порядком реагування на різні види подій у кіберпросторі (кіберінциденти) у Новотроїцькій селищній військовій адміністрації, Новотроїцькій селищній раді та її виконавчих органах (далі — Порядок реагування).

Всі заходи зі стримування, технічного аналізу, усунення наслідків та відновлення систем здійснюються Відповідальними за кіберзахист із суворим дотриманням етапності (від підготовки до аналізу ефективності) та методичних рекомендацій Адміністрації Держспецзв'язку.

12.2 Дії працівника під час інциденту

Після виявлення інциденту та повідомлення відповідального за ІБ працівник зобов'язаний не видаляти жодних файлів, листів або повідомлень, що можуть бути пов'язані з інцидентом — вони є доказами. Якщо є підозра на зараження пристрою шкідливим програмним забезпеченням, працівник відключає його від мережі та припиняє роботу з ним до отримання відповідних інструкцій від відповідального за ІБ. Працівник фіксує обставини події — час виявлення, що саме сталося, які дії передували інциденту — та передає цю інформацію відповідальному за ІБ. Самостійно усувати наслідки інциденту або намагатися встановити його причину без відповідного доручення забороняється.

12.3 Взаємодія та зовнішнє інформування

Відповідальний за ІБ спільно з Відповідальним за кіберзахист вживають невідкладних заходів відповідно до зазначеного Порядку реагування, зокрема збирають та зберігають електронні докази, локалізують (ізолюють) уражену систему, вживають комплексних заходів для відновлення даних із резервних копій та повного усунення виявлених вразливостей.

Залежно від встановленого рівня критичності інциденту, Відповідальний за кіберзахист здійснює офіційне інформування керівництва Організації, Управління інформаційних технологій Херсонської ОВА, а також суб'єктів національної системи кібербезпеки — урядової команди CERT-UA, Ситуаційного центру забезпечення кібербезпеки СБУ (зокрема через платформу MISP-UA), Департаменту кіберполіції, Генерального штабу ЗСУ та НКЦК при РНБО України у суворій відповідності до каналів та термінів, затверджених Порядком реагування.

Кожна виявлена подія або кіберінцидент в обов'язковому порядку підлягає документуванню. Відповідальний за кіберзахист (або за його дорученням Відповідальний за ІБ) невідкладно заносить відомості про інцидент до Журналу реєстрації подій інформаційної безпеки (Додаток 3 до цієї Політики).

Висновки, отримані за результатами етапу аналізу ефективності заходів реагування, передаються Відповідальному за ІБ для актуалізації Політики, оновлення Пам'ятки з кібергігієни та проведення позапланових навчань із персоналом згідно з Розділом 11.

12.4 Розслідування та мінімізація ризиків

Після усунення безпосередніх наслідків інциденту відповідальний за ІБ проводить розслідування його причин із залученням відповідних працівників та за потреби зовнішніх експертів. У ході розслідування аналізуються характер та масштаб інциденту, постраждалі активи та їх важливість

для діяльності Організації, ризики витоку персональних даних або конфіденційної інформації, договірні зобов'язання, що могли бути порушені, а також ризики репутаційної шкоди.

Результати розслідування доповідаються начальнику військової адміністрації разом із рекомендаціями щодо запобігання подібним інцидентам у майбутньому. За результатами складається план заходів з усунення виявлених недоліків із зазначенням відповідальних осіб та строків виконання. Усі інциденти реєструються у журналі інцидентів інформаційної безпеки та зберігаються не менше трьох років.

За потреби проводиться аудит фізичних, організаційних та технічних заходів захисту, а також перегляд положень цієї Політики з урахуванням отриманого досвіду.

12.5 Відповідальність

Відповідальний за ІБ несе персональну відповідальність за неналежне виконання або невиконання своїх посадових обов'язків щодо організації захисту інформаційних ресурсів, координації заходів та контролю за дотриманням вимог цієї Політики в Організації.

Керівники структурних підрозділів, самостійних відділів та виконавчих органів несуть відповідальність за забезпечення контролю за дотриманням вимог цієї Політики підлеглими працівниками (зокрема тими, які виконують роботу у дистанційному режимі).

Працівники Організації несуть персональну відповідальність за збереження довірених їм технічних засобів, конфіденційність автентифікаційних даних (паролів, ЕЦП/КЕП) та дотримання встановлених правил кібергігієни.

Особи, винні у порушенні вимог цієї Політики, розголошенні конфіденційної інформації, персональних даних або чинного законодавства у сфері захисту інформації, несуть дисциплінарну, адміністративну, цивільно-правову або кримінальну відповідальність відповідно до законодавства України».

13. ПЕРЕГЛЯД ТА АКТУАЛІЗАЦІЯ ПОЛІТИКИ

Ця Політика є динамічним («живим») нормативним документом Організації та підлягає регулярному перегляду з метою забезпечення її актуальності, відповідності змінам у законодавстві України, розвитку технологій та появі нових векторів кіберзагроз.

13.1 Плановий перегляд

Плановий повний перегляд Політики здійснюється не рідше одного разу на рік. Відповідальний за ІБ проводить аудит відповідності чинних правил, готує пропозиції щодо змін та подає їх на розгляд керівництву Організації (начальнику військової адміністрації / селищному голові).

Оновлена Політика затверджується відповідним розпорядчим документом та в обов'язковому порядку доводиться до всіх працівників (включаючи тих, які працюють дистанційно).

13.2 **Позаплановий перегляд**

Позапланова актуалізація або внесення змін до окремих розділів Політики проводиться невідкладно у таких випадках:

- Суттєві зміни в інформаційно-комунікаційній інфраструктурі Організації (впровадження нових MES-систем, хмарних сервісів, зміна архітектури мережі чи конфігурації брандмауерів).
- Зміни в державному законодавстві у сфері інформаційної та кібербезпеки, а також поява нових методичних рекомендацій Адміністрації Держспецзв'язку.
- Виявлення критичних вразливостей в утилітах віддаленого доступу або загальних інфраструктурних елементах.
- За результатами аналізу ефективності реагування на кіберінцидент (згідно з п. 12.4 Розділу 12), якщо ліквідація атаки виявила системні прогалини в існуючих правилах захисту.
- За результатами регулярного тестування чи навчання персоналу (згідно з Розділом 11), якщо зафіксовано низький рівень засвоєння правил кібергігієни віддаленими працівниками.

13.3 **Набрання чинності та ознайомлення**

Політика, а також усі зміни та доповнення до неї, набувають чинності з дня їх офіційного затвердження розпорядчим актом керівника Організації.

Кожен працівник Організації (незалежно від форми виконання обов'язків — офісної чи дистанційної) зобов'язаний ознайомитися з чинною редакцією Політики або оновленнями до неї невідкладно, але не пізніше, ніж протягом 5 (п'яти) робочих днів з дати затвердження. Факт ознайомлення фіксується підписом працівника в Аркуші ознайомлення. В умовах дистанційного режиму роботи допускається підписання Аркуша ознайомлення та Зобов'язання в електронному вигляді з накладанням КЕП працівника.

Підписані Аркуші ознайомлення та персональні Зобов'язання зберігаються Відповідальним за ІБ (або долучаються до особових справ працівників) та є офіційним юридичним підтвердженням виконання вимог комплаєнсу».

Додаток 1
до Політики інформаційної безпеки
Новотроїцької селищної військової
адміністрації, Новотроїцької селищної
ради та її виконавчих органів

ЗОБОВ'ЯЗАННЯ
про нерозголошення конфіденційної інформації та персональних даних

Я, _____ (ПІБ),

що перебуваю на посаді _____,

усвідомлюючи важливість забезпечення інформаційної безпеки, захисту прав громадян та державних інтересів, беру на себе офіційне зобов'язання дотримуватися таких вимог:

1. **Дотримання конфіденційності:** Я зобов'язуюся суворо зберігати, захищати від стороннього доступу та не розголошувати конфіденційну, службову інформацію, персональні дані громадян, а також будь-яку іншу інформацію з обмеженим доступом Новотроїцької селищної ради, її виконавчих органів та Новотроїцької селищної військової адміністрації (далі — Організація), яка стане мені відома у зв'язку з виконанням посадових (службових) обов'язків.
2. **Антикорупційні обмеження:** Відповідно до вимог статті 43 Закону України «Про запобігання корупції», мені відомо про сувору заборону розголошувати або використовувати в інший спосіб персональні дані чи іншу непублічну інформацію, що стала мені відома у зв’язку з виконанням службових або посадових повноважень, з метою отримання неправомірної вигоди або в інших особистих інтересах.
3. **Чинність обов'язку після звільнення:** Я підтверджую та погоджуюся, що **припинення трудових відносин (звільнення з посади) або завершення дії цивільно-правового договору не звільняє мене від обов'язку дотримання конфіденційності**. Встановлені цим Зобов'язанням обмеження щодо використання та поширення отриманої інформації продовжують діяти безстроково після припинення моєї діяльності в Організації.
4. **Юридична відповідальність:** Я чітко розумію, що за будь-яке несанкціоноване використання, збирання, поширення, приховування або розголошення зазначеної інформації (зокрема витік персональних даних чи порушення правил роботи з державними реєстрами) я несу персональну дисциплінарну, цивільно-правову, адміністративну або кримінальну відповідальність відповідно до чинного законодавства України та Політики інформаційної безпеки Організації.

З Політикою інформаційної безпеки Організації ознайомлений(а) та зобов’язуюсь виконувати її вимоги.

Дата Підпис ПІП

_____

Додаток 2
до Політики інформаційної безпеки
Новотроїцької селищної військової
адміністрації, Новотроїцької селищної
ради та її виконавчих органів

Перелік програмного забезпечення дозволеного для типового робочого місця

Таблиця 1. Перелік програмного забезпечення для типового робочого місця

зп	Тип програмного забезпечення	Назва програмного забезпечення	Безкоштовно (Так/Ні)
1	Операційна система для персонального комп'ютера або ноутбука	Microsoft Windows	Ні
2	Антивірусне програмне забезпечення	Windows Defender	Поставляється разом з операційною системою
3	Програмне забезпечення для доступу в інтернет	Google Chrome	Так
4	Програмне забезпечення для багатофункціонального пристрою або принтера + сканера	Драйвер пристрою від виробника або з комплекту Microsoft Windows	Поставляється разом з пристроєм або з операційною системою
5	Програмне забезпечення для діловодства	Microsoft Office	Ні

_____

Додаток 3
до Політики інформаційної безпеки
Новотроїцької селищної військової
адміністрації, Новотроїцької селищної
ради та її виконавчих органів

ЖУРНАЛ РЕЄСТРАЦІЇ ПОДІЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

№	Назва події	Дата. Час	Ознаки/ індикатори	Вжиті заходи/ реагування	Рекомендації / коментарі

_____