Номер	Назва	Опис
1	Назва структурного підрозділу	Департамент освіти і науки Миколаївської обласної військової адміністрації
2	Дата останньої редакції	01.10.2025 р.
3	Власник документа	Департамент освіти і науки Миколаївської обласної військової адміністрації
4	Дата затвердження	01.10.2025 р.
5	Дата набрання чинності	01.10.2025 р.

6	Відповідальний за інформаційну безпеку	Калашник Ольга Павлівна, головний спеціаліст
7	Постачальники послуг	Інтернет провайдер “Дикий сад”
8	Користування Інтернетом	info@wildpark.net Інтернет провайдер “Дикий сад”
9	Блокування користувача	Після трьох невдалих спроб
10	Антивірусне програмне забезпечення	**ESET NOD 32 Antivirus** **Windows Defender**
11	Виробник Антивірусного ПЗ	Компанія ESET Microsoft
12	Оновлення антивірусу	Автоматичне оновлення

13	Система фізичної безпеки	НІ
14	Час роботи	Понеділок-Четвер з 8.00 до 17.00 П’ятниця з 8.00 до 15.45
15	Безпечні двері	НІ
16	Детектори руху	НІ
17	Датчики скла	НІ
18	Камери відеоспостереження	НІ
19	Надане обладнання	Комп’ютерна техніка з доступом до мережі інтернет
20	Збереження записів	3 роки
21	Контактний номер телефону	+380638385017

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Департаменту освіти і науки Миколаївської обласної військової адміністрації

ДАТА ОСТАННЬОЇ РЕДАКЦІЇ

01 ЖОВТНЯ 2025 РОКУ

ЗМІСТ

1. ВВЕДЕННЯ

1.1. Загальні положення

Ця політика інформаційної безпеки визначає основні засади забезпечення належного рівня інформаційної безпеки департаменту освіти і науки Миколаївської обласної військової адміністрації, далі – Політика або скорочено ПІБ. ПІБ служить центральним програмним документом з інформаційної безпеки, з яким повинні бути ознайомлені всі працівники департаменту, підрядники (постачальники послуг), і визначає дії, застереження, заборони, яких повинні дотримуватися всі користувачі інформаційних та цифрових активів департаменту. Політика роздруковується та затверджується керівником департаменту та зберігається у відповідального за інформаційну безпеку департаменту. У разі неможливості призначити окремого відповідального за інформаційну безпеку із-за обмеженості людського ресурсу, функцію відповідального за інформаційну безпеку виконує начальник відділу.

Належний рівень інформаційної безпеки, це такий стан фізичного, інформаційного середовища та середовища користувачів інформаційних та цифрових активів департаменту освіти і науки Миколаївської обласної військової адміністрації, який гарантує конфіденційність, доступність, цілісність інформації департаменту та спостережність і контрольованість систем/підсистем, в яких ця інформація циркулює.

Належний рівень інформаційної безпеки досягається за рахунок вмілого застосування комплексу програмних/технічних засобів, організаційних заходів, спрямованих на забезпечення захищеності даних від зловмисного використання та за умови оновлення програмного забезпечення та модернізації комп’ютерного обладнання департаменту за рахунок коштів в межах наявного фінансового ресурсу.

Вимоги та обмеження ПІБ, застосовуються до мережевої інфраструктури, баз даних, носіїв інформації, засобів шифрування, друкованих документів, мультимедіа файлів, засобів бездротового зв'язку, телекомунікаційних систем, аудіо повідомлень та будь-яких інших засобів, що використовуються для передачі, обробки та зберігання інформації у всіх апаратних, програмних та інших інформаційних та цифрових системах департаменту. Цієї політики повинні дотримуватися всі штатні та тимчасові працівники в усіх місцях (на робочому місці чи працюючи віддалено), а також підрядники – постачальники послуг, які працюють з департаментом

1.2. Глосарій

1.2.1. Загальні терміни та абревіатури, які використовуються в цьому документі.

Актив – матеріальні та нематеріальні об’єкти або інформація, що мають цінність для департаменту.

ВІБ – відповідальний за інформаційну безпеку, призначена особа, яка відповідає за впровадження та дотримання Політики інформаційної безпеки в департаменті. У разі неможливості призначити окремого відповідального за інформаційну безпеку, його функцію виконує начальник відділу.

Вірус – шкідливе програмне забезпечення, здатне відтворювати сама себе і зазвичай здатне завдати великої шкоди файлам або іншим програмам на комп'ютері, який воно атакує.

Доступність інформації – властивість, яка гарантує те, що забезпечується своєчасний доступ авторизованих осіб та процесів до інформації, а також відсутні простої в процесі її обробки, тобто коли інформація знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і у той час, коли вона йому необхідна. У випадку втрати інформації існує можливість своєчасного її відновлення.

Зовнішні носії інформації –флешки, USB, флеш- накопичувачі та інші.

ІБ - інформаційна безпека, це процес, який забезпечує збереження визначених Політикою безпеки властивостей інформації та спрямований на запобігання несанкціонованим діям в інформаційній системі, що включає сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи інформаційної системи.

ІС – інформаційна система, організаційно-технічна система, у якій реалізується технологія обробки інформації з використанням технічних і програмних засобів.

ІТ – інформаційна технологія.

Конфіденційність інформації – властивість, яка гарантує те, що доступ до інформації можуть одержати тільки авторизовані особи або процеси.

Користувач - будь-яка особа зі складу працівників департаменту, уповноважена на доступ до певного інформаційного ресурсу.

Користувачі з можливостями запиту (лише для читання) – особи, яким на основі прав доступу заборонено додавати, видаляти або змінювати записи в базі даних та інших доступних їм масивах інформації. Їх системний доступ обмежується лише зчитуванням інформації.

Користувачі з можливостями редагування/оновлення – особи, яким дозволено на основі прав доступу додавати, видаляти або змінювати записи в базах даних та інших масивах інформації департаменту.

Локальна мережа – комп'ютерна мережа департаменту.

ПІБ – політика інформаційної безпеки, це центральний, програмний документ, який визначає основні засади забезпечення належного рівня інформаційної безпеки департаменту.

Персонал – всі працівники департаменту, які використовують інформаційні ресурси, комп'ютерне, телекомунікаційне і офісне обладнання відповідно до своїх посадових обов’язків.

ПК – персональний комп’ютер.

РГІБ – робоча група з інформаційної безпеки, колективний керівний орган системи управління інформаційною безпекою департаменту **(Веліховська А.Б., директор департаменту освіти і науки Миколаївської ОВА, Калашник О.П., головний спеціаліст закладів загальної середньої освіти обласного підпорядкування та інклюзивного навчання, Білик Є.М., начальник відділу матеріально-технічного забезпечення Центру ФСМТ (за згодою)).**

СУІБ - система управління інформаційною безпекою, це комплекс організаційних, програмних, технічних і фізичних заходів, спрямованих на управління ризиками, що пов'язані з використанням в департаменті інформації та інформаційних технологій.

Третя сторона – фізична чи юридична особа, яка перебуває у будь-яких договірних відносинах з департаментом та є стороною таких відносин.

Цілісність інформації – властивість, яка гарантує те, що інформація не містить помилок, є

актуальною, вичерпною, будь-які зміни інформації здійснюються авторизованими особами чи процесами.

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

1.3. Застосовані положення

Нижче наведено перелік нормативних та регулюючих законів, актів, стандартів на основі яких розроблено цей документ:

1. Закон України «Про основні засади забезпечення кібербезпеки України».
2. Закон України «Про інформацію».
3. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».
4. Закон України «Про електронні документи та електронний документообіг».
5. Постанова КМУ №518 від 19.06.2019 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури».
6. Наказ Адміністрації Державної служби спеціального зв'язку від 03.07.2023 № 570 «Про затвердження Методичних рекомендацій щодо регулювання суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі».
7. Постанова КМУ від 20.12.2024 № 1468 «Про внесення змін до Положення про організаційно-технічну модель кіберзахисту».

2. ОБОВ'ЯЗКИ ПРАЦІВНИКІВ

2.1. Вимоги до працівників

Першою лінією захисту в системі управління інформаційною безпекою є персонал або користувачі. Користувачі несуть відповідальність за безпеку всіх даних, які можуть надходити до них у будь-якому форматі.

Обов'язком всіх працівників департаменту є вжиття необхідних заходів для забезпечення фізичної безпеки активів департаменту. Якщо будь хто з працівників бачить невстановлену особу в службовому приміщенні, він/вона повинен вжити всіх можливих заходів для ідентифікації такої особи та проінформувати відповідний відділ або охорону департаменту.

Захист персональних комп'ютерів (ПК). Всі ПК, які знаходяться в закладі не повинні залишати департамент без відповідного дозволу керівника чи ВІБ. Всім новим користувачам надається перший інструктаж на робочому місці щодо правил використання та зберігання ПК департаменту. При використані ПК за межами департаменту користувач повинен вжити всіх можливих заходів із забезпечення безпечного зберігання та використання ПК, інформації та програмного забезпечення, що на ньому знаходяться.

На ПК, та іншому цифровому обладнанні дозволено використання тільки ліцензійного програмного забезпечення та/або спеціального програмного забезпечення, яке надається авторизованим виробником разом з апаратним забезпеченням.

ПК без нагляду – персональні комп'ютери та ноутбуки, які залишаються без нагляду повинні бути заблоковані користувачем при виході з робочого місця. Це правило нагадується усім працівникам під час навчань з інформаційної безпеки.

Домашнє використання ПК. Дозволяється підключати до локальної мережі департаменту тільки таке комп'ютерне обладнання та програмне забезпечення, яке дозволено використовувати. На ПК, що дистанційно підключається до локальної мережі департаменту може бути встановлено лише програмне забезпечення, схвалене для використання. Персональні комп'ютери, що надаються для дистанційної роботи, повинні використовуватися виключно в службових цілях. Персонал

і підрядники повинні бути ознайомлені і розуміти перелік заборонених видів діяльності, який викладений у п.2.2. нижче. Самовільне переналаштування або зміни конфігурації не допускаються на комп'ютерах, що використовуються для дистанційної роботи персоналом.

Збереження права власності.Усі програмні засоби та документація, що встановлюються на ПК або надаються працівникам чи підрядникам для забезпечення діяльності департаменту, є власністю управління, якщо інше не передбачено умовами відповідного договору. Право власності департаменту на програмні засоби зберігається у разі їх офіційного обліку та затвердження відповідним актом, у якому зазначається перелік встановленого програмного забезпечення разом із підтвердженням ліцензійних прав. У разі використання на ПК програмного забезпечення з відкритим вихідним кодом або програм, придбаних за кошти працівників, таке ПЗ не вважається власністю департаменту, якщо не оформлено відповідним актом передачі чи договором щодо прав користування.

2.2. Заборонена діяльність

Працівникам забороняється здійснювати наступні дії. Перелік не є вичерпним. На інші заборонені види діяльності є посилання в інших місцях цього документа.

- Дії що призводять до збою інформаційної системи. Навмисні дії що призводять до збою інформаційної системи категорично заборонені. Користувачі можуть не усвідомлювати, що вони спричинили збій системи, але якщо буде виявлено, що збій стався в результаті дії користувача, повторні дії користувача, що призводять до збою інформаційної системи можуть розглядатися як навмисний вчинок.
- Спроба несанкціонованого доступу до інформаційного ресурсу або спроба обійти функцію безпеки. Це включає в себе запуск програм для злому паролів або програм для сканування локальної мережі з метою виявлення вразливостей, а також спроби обійти заборону на доступ до інформаційних ресурсів.
- Завантаження або спроба завантаження комп'ютерних вірусів, троянів, шпигунських програм або інших видів шкідливого програмного забезпечення в інформаційну систему. Винятком може бути перевірка стійкості системи уповноваженим персоналом або представниками третьої сторони, що авторизовано перевіряє СУІБ.
- Несанкціонований перегляд інформації. Умисний, несанкціонований доступ або перегляд інформації, до якої не надавалися права на доступ чи перегляд відповідно до правила «надання мінімально необхідного доступу» для виконання службових завдань. Цілеспрямована спроба перегляду або доступу до інформації, до якої не було надано доступу за визначеною в ПІБ процедурою, суворо заборонено.
- Використання особистого або недозволенного програмного забезпечення на ПК . Використання особистого або недозволенного програмного забезпечення на ПК департаменту заборонено. Все програмне забезпечення, встановлене на ПК, має бути затверджене та дозволене до використання.
- Використання неліцензійного програмного забезпечення. Все програмне забезпечення, яке встановлене на ПК повинно бути ліцензійним та/або дозволеним до використання.
- Використовувати дозволене програмне забезпечення не належним чином. Порушувати або намагатися порушити умови використання або ліцензійну угоду будь-якого програмного продукту, що дозволено до використання на ПК, суворо заборонено.
- Використовувати інформаційні системи не належним чином. Брати участь у будь-якій діяльності з будь-якою метою, яка є незаконною або суперечить чинній політиці інформаційної безпеки, суворо заборонено.

2.3. Користування Інтернетом та електронною поштою

Електронні засоби комунікації та Інтернет є дієвими інструментами підвищення продуктивності, Ділове використання електронних комунікацій заохочується. Однак усі системи електронного зв'язку та всі повідомлення, що генеруються на обладнанні, що належить департаменту освіти і науки Миколаївської обласної військової адміністрації, або обробляються на пристроях, що належать департаменту не вважаються власністю окремих користувачів. Отже, ця політика поширюється на весь персонал і підрядників (третю сторону) та охоплює всі електронні комунікації, включаючи, але не обмежуючись ними, телефони, електронну пошту, голосову пошту, обмін миттєвими повідомленнями, Інтернет, факс, персональні комп'ютери та сервери.

Надані працівникам інформаційні ресурси, такі як персональні комп’ютери або ноутбуки, комп'ютерні системи, мережі, електронна пошта, програмне забезпечення, а також доступ до Інтернет, призначені для використання в ділових цілях. Однак особисте використання допустимо до тих пір, поки це:

- не відволікає від виконання роботи або функціональних обов’язків,
- не зменшує продуктивність працівників,
- не перешкоджає діяльності департаменту,
- не порушує нічого з наступного:

1) Незаконна діяльність - використання інформаційних ресурсів департаменту освіти і науки Миколаївської обласної військової адміністрації для досягнення незаконних цілей або для здійснення правопорушень, суворо заборонено. Порушення авторських прав – це включає скачування, тиражування та використання піратського програмного забезпечення, музики, книг, відео та аудіо файлів, а також незаконне дублювання та/або розповсюдження інформації та іншої інтелектуальної власності, яка перебуває під авторським правом.

2) Комерційне використання – використання інформаційних ресурсів департаменту освіти і науки Миколаївської обласної військової адміністрації для отримання особистої вигоди суворо заборонено.

3) Політична діяльність – вся політична діяльність суворо заборонена в приміщеннях та з використанням інформаційних ресурсів департаменту Миколаївської обласної військової адміністрації.

4) Переслідування та дискримінація - забороняється використання комп'ютерів, електронної пошти, голосової пошти, обміну миттєвими повідомленнями, текстових повідомлень та Інтернету способами, які є образливими для інших або шкідливими та аморальними. Наприклад, показ або передача зображень, повідомлень і відео сексуального характеру суворо заборонені. Інші приклади неправильного використання включають, але не обмежуються ними, етнічні образи, расові коментарі, або все, що може бути розтлумачено як переслідування, дискримінація, зневажливе ставлення, вираз погроз або прояв неповаги до інших.

5) Небажана електронна пошта - усі повідомлення зроблені з використанням IT-ресурсів департаменту освіти і науки Миколаївської обласної військової адміністрації повинні бути адресними та доцільними. Розповсюдження «небажаної» пошти, наприклад, листів щастя, реклами або несанкціонованих клопотань, забороняється. Якщо користувачі отримали будь-яке з перерахованого вище повідомлень, необхідно їх видалити та нікому не пересилати.

Заклад зберігає за собою право здійснювати моніторинг змісту будь-якого електронного повідомлення та комунікації, що генерується або передається з використанням інформаційних активів департаменту освіти і науки Миколаївської обласної військової адміністрації. Це робиться з метою належного обслуговування та захисту інформаційно-телекомунікаційного обладнання, мереж та ефективного використання наявних ресурсів. Моніторинг може здійснюватися постійно або час від часу. Для цього можуть застосовуватися різні методи моніторингу. Наприклад, для аудиту або аналізу витрат на зв’язок, можуть відстежуватися набрані номери зі службових телефонів, тривалість дзвінків, кількість дзвінків на/з конкретного телефону, час доби і т.д. Інші

приклади, коли електронні комунікації можуть контролюватися, включають, але не обмежуються, дослідженнями та тестуваннями спрямованими на оптимізацію IT-ресурсів, усунення технічних проблем та виявлення закономірностей зловживань або незаконної діяльності.

Департамент залишає за собою право на власний розсуд переглядати файли або електронні повідомлення будь-якого працівника в обсязі, необхідному для забезпечення ефективного використання всіх службових електронних носіїв і засобів комунікації відповідно до всіх чинних законів і нормативних актів, а також цієї Політики інформаційної безпеки.

2.4 Доступ до мережі Інтернет

Персонал, що має доступ до Інтернету, не повинен використовувати цей доступ для розваг, прослуховування музики чи радіо, прослуховування онлайн аудіо книг та перегляду фільмів та інших медійних файлів тощо. Забороняється використовувати доступ до Інтернет для особистої комерційної діяльності чи вирішення своїх побутових питань. Треба розуміти, що використання цього ресурсу не цільовим шляхом створює додаткові загрози інформаційної безпеки.

Персонал повинен розуміти, що індивідуальне використання Інтернету контролюється, і якщо виявиться, що співробітник відвідує ресурси, які небезпечні з точки зору забезпечення інформаційної безпеки, то до нього/неї будуть вжиті дисциплінарні заходи.

Ресурси які заборонено відвідувати: ігрові інтернет-сайти, торенти, файлообмінники, порносайти, чати та онлайн програми для обміну музикою, тощо. Будь-який співробітник, який цілеспрямовано, неодноразово буде намагатися відвідати заборонені ресурси в Інтернет, буде притягнутий до дисциплінарної відповідальності і може бути звільнений.

Відповідальний за інформаційну безпеку контролює виконання заходів із безпечного використання Інтернету, а саме:

- контролює, щоб тільки публічна та відкрита інформація про департамент була доступна в Інтернеті;
- використання Інтернету повинно узгоджуватися з діяльністю департаменту. Мережа не може бути використана для продажі послуг та отримання особистого прибутку;
- конфіденційні або персональні дані, включаючи номери кредитних карток, номери телефонів, паролі для входу в систему та інші дані, які можуть бути використані для доступу до конфіденційної або персональної інформації повинні передаватися через Інтернет у зашифрованому виді.

2.5. Повідомлення про несправності

Користувач повинні інформувати відповідального за ІБ 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 ПК 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 ПК 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 керівнику департаменту про результати цих дій з рекомендаціями щодо подальших кроків для запобігання подібних випадків у майбутньому.

2.6. Повідомлення про інциденти безпеки

Весь персонал, який є користувачами інформаційних ресурсів або підрядники, які мають доступ до цифрових активів департаменту освіти і науки Миколаївської обласної військової адміністрації зобов'язані повідомляти відповідального з ІБ про виявлені інциденти інформаційної безпеки. Користувач - це будь-яка особа, уповноважена на доступ до інформаційного ресурсу департаменту. Користувачі несуть відповідальність за повсякденну практичну безпеку ресурсу, яким вони користуються. Користувачі повинні повідомляти про всі інциденти безпеки або порушення політики безпеки негайно своєму безпосередньому керівнику або відповідальному з інформаційної безпеки. При неможливості негайного повідомлення про інцидент безпеки вищевказаним особам, користувач повинен без зволікань проінформувати про інцидент будь-якого члена Робочої групи з інформаційної безпеки департаменту, які вказані вище в цьому документі.

Внутрішні порушення інформаційної безпеки повинні оперативно розслідуватися. У разі підозри на порушення законодавства, відповідальний з ІБ повинен звернутися до правоохоронних органів.

2.7 Передача конфіденційної інформації

Передача конфіденційної інформації може здійснюватися за допомогою засобів електронного зв’язку, на цифрових носіях чи у паперовому виді. Конфіденційна інформація передається від однієї особи іншій під час ведення службових справ. Особа, яка отримала конфіденційну інформацію повинна забезпечити її зберігання відповідно до умов, встановлених особою, що надала таку інформацію.

2.8. Передача даних та програмного забезпечення

Власне програмне забезпечення, яке не дозволене до використання в закладі не може використовуватися на комп’ютерах або в локальній мережі департаменту освіти і науки Миколаївської обласної військової адміністрації. Якщо існує потреба в конкретному програмному забезпеченні, потрібно надати запит на дозвіл своєму безпосередньому керівнику. Користувачі не повинні використовувати програмне забезпечення, що встановлене на ПК чи комп'ютерному обладнанні при дистанційній роботі без відповідного дозволу.

Дані, що є власністю департаменту включаючи інформацію про працівників, інформацію про ІТ-системи, фінансову інформацію або дані про людські ресурси, не повинні розміщуватися на будь-якому комп'ютері, який не є власністю департаменту, без письмової згоди відповідного керівника. Департамент повинен захищати всі дані та програмне забезпечення, які йому належать, тому повинен контролювати системи, в яких такі дані містяться.

2.9. Угода про конфіденційність

Користувачі інформаційних ресурсів Департаменту при працевлаштуванні підписують угоду про конфіденційність (Додаток 2). Угода повинна містити наступне твердження:

> *Я розумію, що будь-яке несанкціоноване використання або розголошення конфіденційної інформації, може призвести до покарання, відповідно до чинного законодавства та політики інформаційної безпеки.*

Тимчасово влаштовані працівники та підрядники, які не підписували угоди про конфіденційність, підписують такий документ при отриманні доступу до інформаційних ресурсів департаменту.

Угода про конфіденційність переглядається, коли відбуваються зміни умов трудової діяльності,

зокрема при звільнені працівника.

3 ПІДКЛЮЧЕННЯ ДО МЕРЕЖІ

3.1. З’єднання та підключення

Підключення до зовнішніх мереж відбувається через інтернет-провайдера.

3.2. Телекомунікаційне обладнання

До телекомунікаційного обладнання та засобів відноситься наступне:

- телефонні лінії та обладнання
- факсимільні лінії та обладнання
- телефоні навушники та гарнітура
- службові мобільні телефони
- програмне забезпечення для маршрутизації

Цей перелік не є вичерпним.

3.3. Постійні з’єднання

Забезпечення безпеки телекомунікаційних з’єднань є дуже важливим завданням. Інформаційна безпека департаменту може бути поставлена під загрозу, якщо не забезпечити безпечне користування засобами зв’язку. Відповідальний за інформаційну безпеку повинен бути залучені до процесів проектування та затвердження каналів підключення до зовнішніх мереж, а також укладення договорів з третьою стороною на отримання послуг з телекомунікаційного забезпечення департаменту.

4. АНТИВІРУСНИЙ ЗАХИСТ

4.1. Встановлення та оновлення антивірусного ПЗ

Антивірусне програмне забезпечення встановлюється на всіх комп’ютерах, та періодично оновлюється.

Конфігурації - антивірусне програмне забезпечення, яке на даний час використовується, є Windows Defender, AVAST та NOD 32. Оновлення відбувається щодня автоматично.

4.2. Перевірка нового ПЗ

На внутрішніх комп'ютерах і мережах департаменту використовується лише дозволене до використання програмне забезпечення. Хоча умовно-безкоштовне програмне забезпечення може бути корисним, використання такого програмного забезпечення має бути попередньо схвалено відповідальним з інформаційної безпеки. Оскільки програмне забезпечення часто завантажуються з Інтернет (загально доступного джерела) та може мати віруси та інше шкідливе програмне забезпечення, перед його встановленням на комп'ютерах департаменту необхідно вжити спеціальних запобіжних заходів. Ці запобіжні заходи включають визначення того, що програмне забезпечення є сумісним з існуючим ПЗ, не перешкоджає або не пошкоджує апаратне забезпечення, програмне забезпечення або інформацію, а також що програмне забезпечення не містить вірусів та інших шкідливих програм.

Усе файли і програми, які були передані в електронному вигляді на комп'ютери або мережу департаменту з іншого місця, повинні бути перевірені на віруси відразу після отримання. Перевірку та сканування на віруси здійснюється за допомогою наявного антивірусного програмного забезпечення.

Кожен USB-пристрій є потенційним джерелом комп'ютерного вірусу. Тому такий зовнішній носій інформації повинен бути просканований на наявність вірусів та іншого шкідливого програмного забезпечення, перш ніж інформація з них буде скопійована на комп'ютери департаменту.

4.3. Збереження прав власності

Усі програмні продукти та документація, що надаються працівникам або підрядникам є власністю департаменту, якщо на них не поширюється дія іншого договору. Програмне забезпечення, придбане працівником за власний рахунок, залишається власністю працівника, який придбав це програмне забезпечення

5. ФІЗИЧНА БЕЗПЕКА

Забезпечення фізичної безпеки працівникам полягає у створенні безпечних умов на робочому місці та одночасним забезпеченням безпечного зберігання активів департаменту. Будівля департаменту є дещо унікальним місцем з точки зору території навколо, шляхів під'їзду/виїзду, зовнішнього огородження, входів у приміщення, вимог до пожежної безпеки, систем електроживлення, забезпечення безпечного використання цифрових активів та контролю серверної кімнати. Необхідно постійно покращувати та модернізувати систему забезпечення фізичної безпеки для підвищення захисту своїх активів та інформації.

Департамент обладнано системою резервного живлення.

6 ДИСТАНЦІЙНА РОБОТА

У закладі дозволяється та використовується дистанційна робота працівників при певних, визначених керівництвом обставинах. Вимоги, щодо організації дистанційної роботи застосовуються до всіх працівників, які працюють поза межами будівлі департаменту.

Хоча дистанційна робота може бути перевагою як для користувачів, так і для організації в цілому, вона представляє нові ризики інформаційної безпеки. Персонал, що працює дистанційно повинен бути захищеним від небезпеки атак шкідливим програмним забезпеченням та несанкціонованого витоку даних з пристроїв.

6.1. Загальні вимоги

Користувачі, що працюють віддалено, зобов'язані дотримуватися всіх правил департаменту, які встановлені для працівників, а саме:

Потрібно знати: користувачі, що працюють віддалено мають доступ тільки до тих ресурсів та інформації, які потрібні для виконання функціональних завдань.

Використання пароля: користувачі, що працюють віддалено повинні дотримуватись вимог щодо встановлення та зміни паролів.

Навчання: персонал, який працює віддалено, повинен проходити ті самі навчання з інформаційної безпеки, що і персонал що працює на робочих місцях.

Специфічні вимоги: до працівників, що працюють віддалено, можуть бути застосовані додаткові вимоги, які пов'язані зі специфікою виконання функціональних завдань дистанційно.

6.2. Необхідне обладнання

Працівники, допущені до дистанційної роботи, повинні розуміти, що заклад не надає все обладнання, необхідне для забезпечення належного захисту інформації, до якої працівник має доступ; однак є певний перелік обладнання який заклад повинен надати:

Заклад надає:

- робочий комп'ютер (ноутбук) зі встановленим антивірусним ПЗ.

Працівник повинен забезпечити самостійно:

- широкосмуговий канал доступу до Інтернет;
- принтер;
- зовнішній носій для резервного копіювання;
- відокремлене від членів родини робоче місце.

6.3. Захист апаратного забезпечення

Захист від вірусів**:** користувач, що працює дистанційно, повинен постійно використовувати та оновлювати захист комп'ютера від вірусів та іншого шкідливого програмного забезпечення. Антивірусне програмне забезпечення встановлене на комп'ютерах управління і налаштоване на періодичне оновлення. Заборонено працювати без оновленого антивірусного програмного забезпечення.

Блокування екранів**:** незалежно від місця розташування, завжди блокуйте екран, перш ніж відійти від ПК.

6.4. Безпека даних

Резервне копіювання даних**:** встановлена процедура резервного копіювання, яка шифрує дані, та переміщує їх на зовнішній носій. При гострій необхідності дозволено використовувати наявні засоби шифрування (архіватор-шифрувальник WinZip) та доступний зовнішній носій.

Електронна пошта: не дозволено передавати будь-яку конфіденційну інформацію та персональні дані електронною поштою, якщо вона не зашифрована.

Захистить дані, якими ви володієте: потрібно отримувати доступ лише до тієї інформації, яка потрібна для виконання робочого завдання. Регулярно переглядайте дані, які ви зберегли, щоб переконатися, що масив даних, який зберігається знаходиться на мінімально необхідному рівні, а застарілі дані та версії файлів видалені.

Введення даних у відкритому місці: не виконуйте робочі завдання, які вимагають використання конфіденційної інформації або персональних даних у громадських місцях.

6.5. Утилізація паперових носіїв

Паперові документи: всі паперові документи, які містять конфіденційну інформацію, перед утилізацією потрібно подрібнити. Заборонено викидання не подрібнених паперових документів. Інший спосіб утилізації - такі документи палити. Персонал, який працює дистанційно повинен мати або подрібнювач паперу або можливість палити паперові документи.

7. ПОЛІТИКА ЧИСТОГО СТОЛУ/ЕКРАНУ

Одним із засобів контролю за забезпечення інформаційної безпеки є політика чистого столу та чистого екрану, яка знижує ризик несанкціонованого доступу, втрату та пошкодження інформації протягом робочого часу та після його закінчення. Політика чистого столу та чистого екрану визначає методи, пов'язані із забезпеченням того, щоб конфіденційна інформація, як у цифровому, так і у паперовому/фізичному форматі, та активи (наприклад, ПК, ноутбуки, стаціонарні телефонні апарати, смартфони, цифрове обладнання та інші) не залишаються без захисту, коли вони не використовуються, чи коли персонал залишає свої робочі місця на короткий час або наприкінці дня. Дотримання політики чистого столу/екрану всього без винятку працівників дозволить суттєво убезпечити департамент освіти науки Миколаївської обласної військової адміністрації від витоку конфіденційної інформації.

Метою впровадження політики чистого столу та чистого екрану в департаменті освіти і науки Миколаївської обласної військової адміністрації є:

- запобігання витоку/втраті конфіденційних даних департаменту;
- дотримання правил кібергігієни та розвитку кіберкультури, щодо безпечного та належного поводження з конфіденційною інформацією та її носіями;

8. ОБІЗНАНІСТЬ ТА НАВЧАННЯ З ПИТАНЬ БЕЗПЕКИ

Для підвищення обізнаності стосовно питань інформаційної безпеки весь персонал департаменту, включаючи керівництво, повинен регулярно проходити відповідні навчання. Навчання з ІБ для всіх працівників проводиться на платформі Дія позапланово при необхідності.

9. ВІДПОВІДАЛЬНІСТЬ

Вимоги цієї політики поширюються на весь персонал департаменту. Усі працівники департаменту мають бути ознайомлені із її вимогами.

Вимоги

Увесь персонал департаменту повинен дотримуватись наступних правил:

- зберігати власні паролі в таємниці, не розголошувати та нікому не повідомляти їх;
- закривати активні сеанси після завершення роботи, якщо їх не можна захистити відповідним блокуючим механізмом, наприклад блокуванням екрану;
- цифрове обладнання, що не використовується повинно бути вимкнуто або переведене у безпечний режим;
- наприкінці робочого дня/зміни увесь персонал повинен упорядковувати своє робоче місце

Керівництво та всі працівники департаменту, які порушують політику інформаційної безпеки та/або чинне законодавство несуть дисциплінарну, адміністративну чи кримінальну відповідальність.

ДОДАТОК 1

Згода про нерозголошення

ВІДПОВІДАЛЬНІСТЬ ЗА РОЗГОЛОШЕННЯ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

Я розумію і погоджуюся зберігати, захищати та не розголошувати конфіденційну інформацію департаменту освіти і науки Миколаївської обласної військової адміністрації. Крім того, я розумію, що будь-яке несанкціоноване використання або розголошення інформації департаменту, може призвести до дисциплінарної, адміністративної чи кримінальної відповідальності відповідно до політики інформаційної безпеки департаменту освіти і науки Миколаївської обласної військової адміністрації та чинного законодавства.

Дата	Підпис
Дата	Підпис відповідального

ДОДАТОК 2

ЖУРНАЛ РЕЄСТРАЦІЇ ПОДІЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

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

ДОДАТОК 3

Перелік необхідного програмного забезпечення для типового робочого місця

з/п	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 (для Windows 10/11)	Поставляється разом з операційною системою
3	Програмне забезпечення для доступу в інтернет	Google Chrome	Так Посилання
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