СТІ 000Г(Б).97Л

ОСНОВИ КІБЕРБЕЗПЕКИ

(ОЗНАЙОМЧИЙ КУРС, КУРС ІНДИВІДУАЛЬНОЇ ПІДГОТОВКИ)

(ЗА ПРОГРАМОЮ БАЗОВОЇ ЗАГАЛЬНОВІЙСЬКОВОЇ ПІДГОТОВКИ (ДЛЯ ПІДГОТОВКИ МОБІЛІЗАЦІЙНИХ РЕСУРСІВ, ВЕРСІЯ 6, ТЕРМІН НАВЧАННЯ 51 ДОБА) (ЗА ДОВІДОМ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ 2025 РОКУ)

Наказ № 32 від 25 липня 2025 року

Цей стандарт індивідуальної базової загальновійськової підготовки є другим виданням, яке замінює СТІ 000Г(Б).97Л, видання перше, затверджене та введене в дію наказом начальника Центру оперативних стандартів і методики підготовки Збройних Сил України від 24.02.2025 №13.

КОМАНДУВАННЯ ПІДГОТОВКИ КОМАНДУВАННЯ СУХОПУТНИХ ВІЙСЬК ЗБРОЙНИХ СИЛ УКРАЇНИ СПІЛЬНО З 179 ОБ'ЄДНАНИМ НАВЧАЛЬНО-ТРЕНУВАЛЬНИМ ЦЕНТРОМ ВІЙСЬК ЗВ'ЯЗКУ ЗБРОЙНИХ СИЛ УКРАЇНИ ТА ЦЕНТРОМ ОПЕРАТИВНИХ СТАНДАРТІВ І МЕТОДИКИ ПІДГОТОВКИ ЗБРОЙНИХ СИЛ УКРАЇНИ

1. РІВЕНЬ ВІЙСЬКОВОЇ ОРГАНІЗАЦІЙНОЇ СТРУКТУРИ

Навчальний підрозділ (група) – військовослужбовець (рекрут, курсант).

2. ЗАВДАННЯ

2.1. Ознайомчий курс

2.1.1. Основи кібербезпеки та захисту інформації

Завдання	**000Г(Б).97Л.01**	**Знати основи кібербезпеки та захисту інформації під час проходження військової служби**
Підзавдання	000Г(Б).97Л.0101	Знати види інформації за порядком доступу
	000Г(Б).97Л.0102	Знати вимоги керівних документів щодо поводження з інформацією, яка стала відомою тому, хто навчається під час перебування на військовій службі.
	000Г(Б).97Л.0103	Знати вимоги з кібербезпеки при користуванні соціальними мережами, додатками для знайомств тощо
	000Г(Б).97Л.0104	Знати правила ведення переговорів із використанням засобів телефонного та відео конференційного зв’язку
Завдання	**000Г(Б).97Л.02**	**Знати основні кіберзагрози, спрямовані на військовослужбовця, його персональні та службові пристрої**
Підзавдання	000Г(Б).97Л.0201	Знати кіберзагрози, які безпосередньо направлені на військовослужбовця та наявні у нього особисті комунікаційні пристрої.
	000Г(Б).97Л.0202	Знати кіберзагрози через невірні налаштування АРМ (ПЕОМ), мобільні комунікаційні пристрої.
	000Г(Б).97Л.0203	Знати кіберзагрози, які реалізуються через соціальну інженерію, фішинг, шкідливі програмні засоби тощо.
	000Г(Б).97Л.0204	Знати порядок протидії кіберзагрозам.

2.2. Курс індивідуальної підготовки

2.2.1. Основи кібербезпеки та захисту інформації

Завдання	**000Г(Б).97Л.03**	**Знати вимоги керівних документів щодо заходів із кібербезпеки під час перебування на території ОВУ, з'єднань, військових частин, навчальних закладів, установ та організацій Збройних Сил України, а також на пунктах управління та в районах виконання бойових (спеціальних) завдань**
Підзавдання	000Г(Б).97Л.0301	Знати вимоги керівних документів щодо використання зовнішніх носіїв інформації у Збройних Силах України
	000Г(Б).97Л.0302	Знати вимоги керівних документів щодо заходів із кібербезпеки під час перебування в пунктах постійної дислокації, під час занять, навчань та інших заходів підготовки
	000Г(Б).97Л.0303	Знати вимоги керівних документів щодо заходів із кібербезпеки під час перебування на пунктах управління та в районах виконання бойових (спеціальних) завдань

3. ПОСИЛАННЯ НА НОРМАТИВНО-ПРАВОВІ АКТИ ТА ВІЙСЬКОВІ ПУБЛІКАЦІЇ

Позначка НПА та ВП	Повне найменування нормативно-правового акту та військової публікації
1	2
ТП 7-00(206)246.63	**1.** Програма “Базової загальновійськової підготовки (для підготовки мобілізаційних ресурсів, 6 версія) (термін навчання 51 доба) (за досвідом російсько-Української війни 2025 року)” затверджена Головнокомандувачем ЗС України 10.07.2025 (вих. АУ ГШ ЗС України від 10.07.2025 № 89123/С)
ДМ до СТІ 000Г(Б).97Л	**2.** Довідковий матеріал до стандарту “Основи кібербезпеки” (курс індивідуальної підготовки за програмою базової загальновійськової підготовки, для підготовки мобілізаційних ресурсів, версія 6, термін навчання 51 доба) (за досвідом російсько-Української війни 2025 року)”
ВКДП 7-00(03).02	**3.** Інструкція “Про порядок розроблення (розміщення) стандартів (каталогів завдань) з підготовки та проведення оцінювання за стандартами підготовки Збройних Силах України”, затверджена та введена в дію наказом Генерального штабу ЗС України від 27.01.2020 № 26
	4. Інструкція з використання зовнішніх носіїв інформації у Збройних Силах України, затверджена наказом Головнокомандувача Збройних Сил України 05.07.2023 №189
	5. Інструкція з зберігання і користування особовим складом Збройних Сил України мобільних комутаційних пристроїв та інших електронних засобів, затверджена наказом Головнокомандувача Збройних Сил України від 29.04.2024 №165
	6. Порядок організації кіберзахисту інформаційно–комунікаційних систем пунктів управління органів військового управління Збройних Сил України, затверджена наказом Головнокомандувача Збройних Сил України від 05.05.2023 №120
	7. Інструкція щодо проведення занять з основ кібербезпеки (для підготовки мобілізаційних ресурсів), затверджена Командувачем сухопутних військ у Збройних Сил України 03.01.25
ЗВП 6-00(108).01	**8.** Методичні рекомендації “З питань забезпечення особистої кібербезпеки військовослужбовця”, затверджені наказом Командувача військ зв’язку та кібербезпеки Збройних Сил України 16.08.23 № 200/нагд
	9. Методичний посібник з кібербезпеки для військових та держслужбовців (за редакцією Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБУ)
ССОП 7-00(480).68	**10.** Інструкція “З проведення процедури аналіз проведених дій”, затверджена командувачем Сухопутних військ ЗС України 04.06.2025
ВП 7-00(348).62(63)	**11.** Інструкція “З порядку впровадження системи зворотного зв’язку (FEEDBACK)”, затверджена начальником Головного управління доктрин та підготовки Генерального штабу ЗС України 09.07.2024

1	2
ВП 1-00(189)	**12.** Інструкція “З порядку отримання електронних або друкованих військових публікацій, відеоматеріалів, проведення дистанційних курсів Збройних Сил України та країн-партнерів”, затверджена начальником Головного управління доктрин та підготовки Генерального штабу (J7) ЗС України 04.04.2025 (друге видання)

Примітка. Якщо військову публікацію (національний або військовий стандарт, керівний документ і стандарт НАТО та держав-членів НАТО тощо), на яку є посилання, замінено новою або до неї внесені зміни, то потрібно застосовувати нову військову публікацію, охоплюючи всі внесені до неї зміни.

4. УМОВИ ВИКОНАННЯ

4.1. Ознайомчий курс

4.1.1. До завдання 000Г(Б).97Л.01, 000Г(Б).97Л.02, (пунктів 2.1.1. – Тема № 1)

4.1.1.1. Загальні відомості

Теоретичні заняття проводяться у стаціонарному класі або у польовому заглибленому класі (бліндажі) на ділянці місцевості, у складі навчальної взводу (групи) одразу після прибуття особового складу в навчальний центр. Заняття проводяться під керівництвом викладача (інструктора). В ході теоретичних занять військовослужбовці вивчають:

а) види інформації за порядком доступу;

б) вимоги керівних документів щодо поводження з інформацією, яка стала відома військовослужбовцю під час перебування на військовій службі;

в) вимоги з кібербезпеки при користуванні соціальними мережами, додатками для знайомств тощо, при невірному налаштуванні особистих та службових мобільних комунікаційних пристроїв, АРМ, ПЕОМ;

г) правила ведення переговорів із використанням засобів телефонного та відео конференційного зв’язку;

д) під час викладення навчального матеріалу наводяться приклади наслідків, до яких призводить недотримання вимог кіберзахисту;

е) в ході заняття у військовослужбовців формуються почуття відповідальності за ризики, на які вони наражають себе, родину, колег або виконання бойового завдання (операцію), коли передають у телефонному режимі, публікують у месенджерах, передають електронною поштою тощо інформацію службового та особистого характеру;

ж) закріплення навчального матеріалу досягається методом опитування;

и) наприкінці заняття проводиться аналіз проведених дій (АПД/AAR).

к) під час підготовки до проведення заняття керівник (інструктор) використовує довідковий матеріал до цього стандарту індивідуальної фахової підготовки ДМ до СТІ 000Г(Б).97Л (посилання **2**);

л) наприкінці заняття керівник заняття проводить оцінювання щодо засвоєного матеріалу і дає зворотній зв’язок/Feedback тим, хто навчається (посилання **11**), а також проводить аналіз проведених дій/After Action Review (далі – АПД/AAR) (посилання **10**).

Проведення керівником занять (викладачем) АПД/AAR дозволяє йому та особовому складу отримати відповіді на запитання, відгуки і оцінки про рівень та якість навчання під час тренування (підготовки).

Сутність АПД/AAR полягає у тому, що слово для розбору дій надається всім учасникам обговорення почергово, а керівник занять (викладач) виступає не “суддею на процесі”, а лише посередником (режисером, модератором) обговорення. Це дозволяє всім учасникам заходу самостійно проаналізувати проведені дії в доброзичливій комунікаційній атмосфері.

Під час АПД/AAR керівник занять (викладач) послідовно використовує ***ТРИ ключових питання***, які обговорюються:

1). **Що мало статися?** Наприклад, що ми мали досягнути, яке завдання було поставлено?

2). **Що насправді сталося?** (Чого ми досягли? Як виконане завдання? Що вдалось? Що не вдалось? Чому?).

3). **Що потрібно зробити, щоб стало краще?** (Як вдосконалити навчання?).

ВАЖЛИВО! *Правила здійснення АПД/AAR:*

поведінка того, хто проводить АПД/AAR або використовує його результати, має викликати і посилювати довіру в тих, хто навчається;

ЗАБОРОНЕНО! *організатору АПД/AAR виступати з трибуни або іншим чином показувати свою зверхність, принижувати гідність присутніх і проявляти хамство;*

процес самокритичного аналізу необхідно проводити негайно, поки особовий складу/навчальна група ще активна, а спогади свіжі, слід уникати критики, приниження тих, хто навчається, порівняння дій одного військовослужбовця (підрозділу в складі групи/відділення) з іншими, засудження, монологічності та тривалих у часі "розборів польотів", виявлення або призначення "крайніх";

учасникам АПД/AAR, не знайомим з процесом, повинна надаватись інформація про те, що й чому відбувається або відбувалося;

слід уникати проведення АПД/AAR у формі лекцій командирів (начальників) та тривалих у часі розборів (повчальних монологів), а заохочувати висловлення власних думок і суджень за принципом діалогічності;

вирішальне значення має створення відкритого середовища, як чинника, що заохочує дискусії і критичне мислення, а не каральної атмосфери і страху;

УВАГА! *АПД/AAR не повинно використовуватись для пошуку винних, обговоренню підлягають не тільки негативні дії (слабкі місця), а й успішно виконані завдання тощо*.

4.2. Курс індивідуальної підготовки

4.2.1. До завдання 000Г(Б).97Л.03 (пунктів 2.2.1. – Тема № 1)

4.2.1.1. Загальні відомості.

Теоретичне заняття проводяться у стаціонарному класі або у польовому заглибленому класі (бліндажі) на ділянці місцевості, у складі навчальної взводу (групи), заняття проводяться під керівництвом викладача (інструктора). В ході теоретичного заняття військовослужбовці вивчають:

а) вимоги Інструкції з використання зовнішніх носіїв інформації у Збройних Силах України;

б) вимоги Інструкції зі зберігання і користування особовим складом Збройних Сил України мобільними комунікаційними пристроями та іншими електронними засобами;

в) вимоги Порядку організації кіберзахисту інформаційно-комунікаційних систем пунктів управління органів військового управління Збройних Сил України;

г) порядок організації антивірусного захисту у Збройних Силах України.

В ході заняття у військовослужбовців формуються почуття відповідальності за ризики, на які вони наражають себе, колег або виконання бойового завдання (проведення операції), коли допускають порушення встановлених інструкцій (правил) зберігання та використання мобільних комунікаційних пристроїв та інших електронних засобів. Закріплення навчального матеріалу досягається методом опитування. Наприкінці заняття проводиться АПД/AAR.

4.3. Особливості

4.3.1. Заняття з основ кібербезпеки повинні бути простими та дохідливими для сприйняття військовослужбовцями, які мають різний рівень підготовленості в даній області знань, нести не тільки загальний характер, але і практичні рекомендації (приклади) щодо виконання заходів кібербезпеки в умовах війни.

4.3.2. Для забезпечення ефективності навчання військовослужбовців необхідно на заняттях застосовувати засоби відео проекції для відображення на екрані як навчального матеріалу, так і прикладів дій, які необхідно виконувати військовослужбовцями для правильного використання мобільних комунікаційних пристроїв та інших електронних засобів.

4.3.3. Із виконанням завдань (підзавдань) – проводиться його оцінювання (проміжний контроль за тему), по закінченню курсу проводиться контрольне заняття *(якщо контрольне заняття не проводиться то оцінки за кожну тему проміжного контролю переносяться до оціночного листа за предмет навчання, для виставлення оцінки за пройдений курс)*, результати яких заносяться до журналів обліку підготовки (електронних журналів обліку підготовки).

ВАЖЛИВО! Перелік теоретичних питань (тестів) для проведення контрольного заняття за пройдений курс з **основ кібербезпеки** обирається керівником та має відповідати тематиці програми БЗВП (посилання **2**).

4.4. Заходи безпеки

На занятті повинні підтримуватися висока дисципліна, суворий контроль за дотриманням встановлених правил і заходів безпеки.

Виконання завдань передбачає дотримання всіма військовослужбовцями заходів безпеки, які визначені вимогами керівних документів.

УВАГА! *Дотримання заходів безпеки на заняттях повинно бути спрямовано не на відмову від небезпечних і ризикованих ситуацій (завдань, вправ), а на недопущення травмування серед особового складу.*

Організація заходів безпеки досягається:

завчасним визначенням конкретних заходів безпеки, що визначені темою занять і попередньою підготовкою навчального місця;

правильною методикою проведення занять, впевненим керівництвом ними з боку викладачів (командирів підрозділів);

дотриманням військової дисципліни, вивченням військовослужбовцями правил, що забезпечують безпеку під час проведення занять;

систематичним контролем за дотриманням встановлених правил і заходів безпеки з боку керівника заняття.

ЗАСТЕРЕЖЕННЯ! *Враховуючи ситуацію в Україні та можливістю виникнення не прогнозованих ракетних та повітряних небезпек з боку противника, в* ***негайному*** *порядку здійснити заходи щодо розосередження та укриття особового складу під керівництвом інструктора*.

5. ПОРЯДОК ВИКОНАННЯ

5.1. Порядок виконання завдань ознайомчого курсу

5.1.1. Покрокове виконання завдання 000Г(Б).97Л.0101 - (пункту 2.1.1. – Тема № 1)

5.1.1.1. Керівник заняття (викладач, інструктор) доводить новий навчальний матеріал в наступній послідовності:

а) види інформації за порядком доступу;

б) правила поводження з інформацією, яка стала відомою тому, хто навчається, під час перебування на військовій службі;

в) вимоги з кібербезпеки при користуванні соціальними мережами, додатками для знайомств тощо;

г) правила ведення переговорів із використанням засобів телефонного та відео конференційного зв’язку.

5.1.1.2. На початку викладення навчального матеріалу керівник заняття (викладач, інструктор) звертає увагу військовослужбовців, що у рамках інформаційної та кібернетичної війни активно використовуються такі інструменти, як:

а) фішинг (масове розсилання шкідливих повідомлень з метою отримання даних);

б) шкідливі програмні засоби (віруси, трояни, програми-шпигуни);

в) фейкові облікові записи, які видають себе за волонтерів, побратимів чи командирів;

г) соціальні мережі та месенджері, як платформи для стеження,

д) провокацій та дестабілізації.

При цьому одним із головних слабких місць кіберзахисту є саме людський фактор — необережність, неуважність, невміння вчасно виявити загрозу. Саме тому важливо, щоб кожен військовослужбовець мав чітке розуміння:

а) які загрози можуть бути спрямовані саме на нього;

б) як ці загрози можуть бути реалізовані через звичайні пристрої (смартфон, ноутбук, планшет);

в) як правильно налаштувати персональне та службове обладнання;

г) як убезпечити себе в соціальних мережах;

д) як діяти у разі виявлення підозрілої активності.

Особливої уваги вимагає порядок поводження з інформацією, яка може стосуватись бойових завдань, особового складу, розташування техніки чи озброєння.

УВАГА! Будь-яка інформація чи її елемент (деталь), яку отримав ворог, — це реальний ризик для життя та ефективності оборони. І тому — це питання особистої відповідальності кожного військового.

5.1.1.3. Після доведення до особового складу класифікації інформації за порядком доступу та обмежень щодо її розповсюдження керівник заняття (викладач, інструктор) доводить відповідальність військовослужбовців за поширення або неналежне поводження з інформацією з обмеженим доступом.

УВАГА. ВАЖЛИВО ДЛЯ ВІЙСЬКОВОСЛУЖБОВЦІВ! На службі ви можете отримувати доступ до **службової, конфіденційної або навіть таємної інформації**, навіть не усвідомлюючи цього. Кожне повідомлення, фото, повідомлення в чаті, допис у соцмережі — може містити відомості, які заборонено розголошувати. Тому **ви зобов'язані знати, як класифікувати інформацію і як поводитись із нею відповідно до законодавства**.

5.1.1.4. Після вивчення з особовим складом правил поводження з інформацією, яка стала відомою під час перебування на військовій службі керівник заняття (викладач, інструктор) наводить приклади порушення цих правил, що привело до витоку інформації, ускладнень та ризиків, як для особового складу так і щодо виконання завдання підрозділом в цілому.

5.1.1.4. При вивченні питань кібербезпеки при користуванні соціальними мережами, додатками для знайомств тощо доводяться основні порушення, які приводять до отримання противником доступу до інформаційно-комунікаційних систем ЗС України та до інформації службового характеру при:

а) використання мобільних телефонів в районах зосередження та виконання завдань, зокрема в режимі GSM та з увімкненою геолокацією;

б) використання месенджерів (Signal, Telegram, Viber, WhatsApp) для службового користування в чатах та пересилання службової інформації;

в) публікації інформації про розташування, переміщення та дії підрозділів, бойової техніки, особового складу в додатках та соціальних мережах TikTok, Instagram, Facebook, тощо;

г) відпрацювання службових документів, у тому числі тих, що містять інформацію з обмеженим доступом, на ПЕОМ, що мають підключення до глобальних мереж, у тому числі до Інтернет.

УВАГА! Додатки для знайомств — це один із малопомітних, але надзвичайно ефективних каналів для збору розвідданих та деморалізації, який активно використовують спецслужби російської федерації. Будь пильним: навіть флірт у мережі може закінчитись втратою побратимів.

ПОРАДИ ДЛЯ ВІЙСЬКОВОСЛУЖБОВЦЯ:

а) не використовуй додатки для знайомств під час служби;

б) не вказуй реальне місце перебування, посаду, звання;

в) в районах зосередження та виконання завдань вимикай геолокацію на телефоні повністю;

г) не розповсюджуй фото та відео, за якими можлива ідентифікація твого місця знаходження;

д) не веди діалог із "новими знайомими", які занадто активно цікавляться твоєю службою;

е) не додавай до друзів контакти невідомих осіб;

ж) не відкривай файли та посилання від незнайомців (навіть від друзів, чи близьких, якщо відправлене викликає сумнів);

и у разі сумнівів або фіксації підозрілої поведінки — повідом командування.

5.1.1.5. Керівник заняття (викладач, інструктор) доводить основні правила безпечного користування телефонним та відеозвязком:

а) заборонено обговорювати:

1) плани бойових дій, переміщення підрозділів;

2) особовий склад, озброєння, втрати; службову документацію, дані про командирів; координати, географічні назви, позивні тощо.

б) заборонено використовувати звичайний (цивільний) телефон для службових переговорів.

в) використання відеозв’язку – лише за необхідності і в контрольованих умовах. Заборонено проводити відеоконференції: у присутності сторонніх осіб; у приміщеннях з елементами тактичних карт, наказів, схем; у формі, на якій видно шеврони, жетони, таблички частини.

УВАГА! Камера — лише за потреби. Бажано вмикати фон розмиття або віртуальний фон.

в) Контроль за фоновими звуками та приміщенням. Під час переговорів: зачинити двері; уникати фонового шуму та присутності осіб, які не мають допуску; не залишати мікрофон увімкненим без потреби; переконатися, що поруч немає інформації з обмеженим доступом (карти, планшети, документи).

г) Упевненість у співрозмовнику. Перш ніж почати розмову потрібно:

1) впевнитись у особі абонента;

2) за потреби — використати пароль/кодове слово;

3) не відповідати на дзвінки з невідомих номерів або підозрілих акаунтів у месенджерах;

4) не переходити за посиланнями, які надсилаються «начебто колегою».

д) не фіксувати і не записувати без дозволу.

ВАЖЛИВО! Інформаційна дисципліна — така ж важлива, як і дисципліна на полі бою. Кожен військовий — ціль для ворожої розвідки. Навіть одна необережна дія в мережі або під час розмови — це потенційна загроза всьому підрозділу. Тримай інформаційну оборону так само впевнено, як фізичну.

5.1.1.6. Наприкінці заняття здійснюється контроль засвоєння навчального матеріалу та аналіз проведених дій.

Керівник заняття методом опитування досягає закріплення вивченого матеріалу.

5.1.2. Покрокове виконання завдання 000Г(Б).97Л.0102 - (пункту 2.1.1. – Тема № 1)

5.1.2.1. Керівник заняття (викладач, інструктор) доводить новий навчальний матеріал в наступній послідовності:

а) кіберзагрози, які безпосередньо направлені на військовослужбовця та наявні у нього особисті комунікаційні пристрої;

б) кіберзагрози через невірні налаштування АРМ (ПЕОМ), мобільні комунікаційні пристрої;

в) кіберзагрози, які реалізуються через соціальну інженерію, фішинг, шкідливі програмні засоби тощо;

г) порядок протидії кіберзагрозам.

5.1.2.2. Керівник заняття (викладач, інструктор) дає визначення особистим комунікаційним пристроям та доводить основні типи кіберзагроз, які безпосередньо направлені на військовослужбовця та наявні у нього особисті комунікаційні пристрої:

а) атаки на акаунти (злом паролів, сесій, соцмереж);

б) стікеринг по геолокації;

в) прослуховування та відеонагляд через мікрофон/камеру;

г) соціальний злам: атаки через підроблену «довіру».

Зосереджує увагу на заходах захисту від прямих кіберзагроз на особисті комунікаційні пристрої:

а) заборона зберігання службових даних на особистих пристроях;

б) використання надійних паролів та двофакторної автентифікації (2FA);

в) регулярне оновлення операційної системи та антивірусу;

г) вимкнення геолокації, Bluetooth та NFC, якщо вони не потрібні;

д) фізичний контроль пристрою: не залишати без нагляду, використовувати шифрування.

5.1.2.2. До особового складу доводяться типові загрози, що виникають через неправильні налаштування АРМ та мобільних пристроїв:

а) відкриті порти та служби;

б) використання облікових записів без пароля або з правами адміністратора;

в) відсутність оновлень безпеки;

г) автоматичне підключення до публічних Wi-Fi та Bluetooth-пристроїв.

Зосереджує увагу на базових правилах безпеки налаштувань АРМ та мобільних пристроїв:

а) установити надійний пароль на вхід до ПК/АРМ, екран блокування, BIOS;

б) заборонити автоматичне оновлення з неофіційних джерел;

в) вимкнути непотрібні служби та фонові з'єднання;

г) налаштувати автоматичне оновлення ОС, антивірусу та програмного забезпечення;

д) встановити межі прав доступу для користувачів (відокремлення прав адміністратора та звичайного користувача);

е) вимкнути автоматичне підключення до мереж Wi-Fi, Bluetooth;

ж) використовувати файрвол (брандмауер) для обмеження вхідного та вихідного трафіку.

5.1.2.3. Доводить кіберзагрози, які реалізуються через соціальну інженерію, фішинг, шкідливі програмні засоби тощо:

а) фішинг (phishing);

б) смс-фішинг та месенджинг;

в) використання довіри (pretexting);

г) атаки через документи та файли;

д) імітація внутрішньої комунікації.

Керівник заняття (викладач, інструктор) доводить ознаки фішингу та соціальної інженерії:

а) несподівані листи або повідомлення з терміновими вимогами;

б) посилання на незнайомі або спотворені домени;

в) граматичні помилки в тексті повідомлень;

г) пропозиції "виграшу", "допомоги", "подарунку", що вимагають дії прямо зараз;

д) повідомлення, які викликають страх або терміновість ("Ваш акаунт буде заблоковано", "Командування чекає вашого підтвердження").

Зосереджує увагу на заходи захисту:

а) не переходь за підозрілими посиланнями з пошти, месенджерів, соцмереж;

б) перевіряй джерело повідомлення або електронного листа;

в) не відкривай файли невідомого походження, навіть якщо їх надіслали “знайомі”;

г) уникай спілкування з невідомими профілями, які активно запитують інформацію про службу;

д) користуйся антивірусом із виявленням фішингу та вмикай двофакторну автентифікацію;

е) повідомляй про підозрілі дії через лінію безпеки або командиру.

5.1.2.4. Керівник заняття (викладач, інструктор) доводить рекомендації військовослужбовцю щодо порядку протидії кіберзагрозам:

а) не намагайся вирішувати кіберінцидент самостійно, якщо не маєш відповідної підготовки;

б) не приховуй підозрілу активність — це може спричинити масові наслідки для підрозділу;

в) регулярно проходь тренінги та актуалізуй знання з кібербезпеки;

г) дотримуйся службових інструкцій щодо роботи з ПЕОМ, мобільними пристроями, мережами.

5.1.2.5. Наприкінці заняття здійснюється контроль засвоєння навчального матеріалу та аналіз проведених дій.

Керівник заняття методом опитування досягає закріплення вивченого матеріалу.

5.2. Порядок виконання завдань курсу індивідуальної підготовки

5.2.1. Покрокове виконання завдання 000Г(Б).97Л.0103 - (пункту 2.2.1. – Тема № 1)

5.2.1.1. Керівник заняття (викладач, інструктор) доводить новий навчальний матеріал в наступній послідовності:

в) порядок використання зовнішніх носіїв інформації у Збройних Силах України;

вимоги керівних документів щодо заходів із кібербезпеки під час перебування в пунктах постійної дислокації, під час занять, навчань та інших заходів підготовки;

вимоги керівних документів щодо заходів із кібербезпеки під час перебування на пунктах управління та в районах виконання бойових (спеціальних) завдань.

5.2.1.2. Доводяться основні вимоги Інструкції з використання зовнішніх носіїв інформації у Збройних Силах України (посилання **4**), наводяться приклади порушень та проводиться їх аналіз.

УВАГА! ПОРАДИ З ВИКОРИСТАННЯ ЗОВНІШНІХ НОСІЇВ ІНФОРМАЦІЇ:

а) завжди вчасно здійснюй оновлення баз антивірусної програми;

б) після підключення носія інформації обов'язково просканує його антивірусною програмою;

в) для використання інформації зі змінного носія, у панелі керування комп'ютера відключи автозапуск змінних носіїв інформації;

г) використовуй лише обліковані носії інформації в межах свого підрозділу. Пам'ятай, що кожен носій має свій «гриф»;

д) не використовуй у службових цілях сторонні носії інформації, особливо особисті;

е) не користуйся облікованими носіями в особистих цілях.

ВАЖЛИВО! За порушення правил зберігання та обробки інформації з обмеженим доступом (цілком таємної, таємної, навіть для службового користування) існує покарання, яке полягає в притягненні винного до відповідальності, в тому числі й до кримінальної.

5.2.1.2. Доводяться вимоги Інструкції зі зберігання і користування особовим складом Збройних Сил України мобільними комунікаційними пристроями та іншими електронними засобами (посилання **5**), пояснює порядок їх використання:

а) в пунктах постійної дислокації;

б) під час занять, навчань та інших заходів підготовки;

в) на пунктах управління угрупувань військ (сил), військових частин;

г) в районах виконання бойових (спеціальних) завдань.

5.2.1.3. Пояснюється порядок організації антивірусного захисту у Збройних Силах України та його важливість у реалізації заходів кібербезпеки.

УВАГА! Працювати на автоматизованих робочих місцях, інформаційно-комунікаційних чи автоматизованих системах без встановлених та належним чином налаштованих антивірусних програмних засобів ЗАБОРОНЕНО. Це є порушенням вимог Інструкції з організації антивірусного захисту в МОУ та ЗСУ і створює загрозу кібербезпеці.

5.2.1.4. Наприкінці заняття здійснюється контроль засвоєння навчального матеріалу та аналіз проведених дій.

Керівник заняття методом опитування досягає закріплення вивченого матеріалу.

6. ОЦІНОЧНІ ЛИСТИ

6.1. До завдань ознайомчого курсу

6.1.1. До завдань 000Г(Б).97Л.01, 000Г(Б).97Л.02

№ з/п	Особовий склад	солдат *Прізвище, ініціали)*	солдат *Прізвище, ініціали)*	солдат *Прізвище, ініціали)*	солдат *Прізвище, ініціали)*	солдат *Прізвище, ініціали)*	солдат *Прізвище, ініціали)*	солдат *Прізвище, ініціали)*	солдат *Прізвище, ініціали)*	солдат *Прізвище, ініціали)*	солдат *Прізвище, ініціали)*
	Елементи, що оцінюються	Вик/ Невик	Вик/ Невик	Вик/ Невик	Вик/ Невик	Вик/ Невик	Вик/ Невик	Вик/ Невик	Вик/ Невик	Вик/ Невик	Вик/ Невик
І. Теоретичні знання											
а	Чи знає військовослужбовець види інформації за порядком доступу?										
б*	Чи знає військовослужбовець вимоги керівних документів щодо поводження з інформацією службового характеру?										
в*	Чи знає військовослужбовець кіберзагрози, які безпосередньо направлені на військовослужбовця та наявні у нього особисті та службові мобільні комунікаційні пристрої та протидію таким кіберзагрозам?										
г	Чи знає військовослужбовець правила ведення переговорів із використанням засобів телефонного та відео конференційного зв’язку?										
Загальна кількість елементів за тему завдання, що оцінюється:											

Таблиця оцінювання проміжного контролю
за тему № 1 предмету навчання СТІ БЗВП/ висновок щодо рівня підготовки

Номер		Найменування заходу	Елементи, що сплановані	солдат *Прізвище, ініціали)*		солдат *Прізвище, ініціали)*		солдат *Прізвище, ініціали)*		солдат *Прізвище, ініціали)*		солдат *Прізвище, ініціали)*		солдат *Прізвище, ініціали)*		солдат *Прізвище, ініціали)*		солдат *Прізвище, ініціали)*		солдат *Прізвище, ініціали)*	
				Елементи, що засвоєно	%	Елементи, що засвоєно	%	Елементи, що засвоєно	%	Елементи, що засвоєно	%	Елементи, що засвоєно	%	Елементи, що засвоєно	%	Елементи, що засвоєно	%	Елементи, що засвоєно	%	Елементи, що засвоєно	%
розділу	теми		кількість																		
Загальна кількість елементів, за якими здійснено оцінювання (* включаючи критично важливі елементи)			**4 (*2)**																		
Елементи, які передбачають оцінювання теоретичних знань:			**4 (*2)**																		
I.	1.	Оцінка за розділ (тему)																			
Оцінка стандарту індивідуальної підготовки за проміжний контроль теми предмету навчання (виконання індивідуальних завдань):																					

6.1.2. Оціночний лист завдань ознайомчого курсу за предмет навчання “Основи кібербезпеки”

№ з/п	Елементи, що оцінюються	солдат *Прізвище, ініціали)*	солдат *Прізвище, ініціали)*	солдат *Прізвище, ініціали)*	солдат *Прізвище, ініціали)*	солдат *Прізвище, ініціали)*	солдат *Прізвище, ініціали)*	солдат *Прізвище, ініціали)*	солдат *Прізвище, ініціали)*	солдат *Прізвище, ініціали)*	солдат *Прізвище, ініціали)*
Теоретичні знання											
1.	Теоретичні питання відповідно до завдань 000Г(Б).97Л.01, 000Г(Б).97Л.02 (тема №1)										
Загальна оцінка за теми (розділи), що оцінюється:											
Загальна оцінка за СТІ БЗВП											

6.2. До завдань курсу індивідуальної підготовки

6.2.1. До завдання 000Г(Б).97Л.03

№ з/п	Особовий склад	солдат *Прізвище, ініціали)*	солдат *Прізвище, ініціали)*	солдат *Прізвище, ініціали)*	солдат *Прізвище, ініціали)*	солдат *Прізвище, ініціали)*	солдат *Прізвище, ініціали)*	солдат *Прізвище, ініціали)*	солдат *Прізвище, ініціали)*	солдат *Прізвище, ініціали)*	солдат *Прізвище, ініціали)*
	Елементи, що оцінюються	Вик/ Невик	Вик/ Невик	Вик/ Невик	Вик/ Невик	Вик/ Невик	Вик/ Невик	Вик/ Невик	Вик/ Невик	Вик/ Невик	Вик/ Невик
Теоретичні знання											
а	Чи знає військовослужбовець вимоги керівних документів з використання зовнішніх носіїв інформації у Збройних Силах України										
б	Чи знає військовослужбовець вимоги керівних документів щодо заходів із кібербезпеки під час перебування в пунктах постійної дислокації військових частин?										
в*	Чи знає військовослужбовець вимоги керівних документів щодо заходів із кібербезпеки під час перебування на території військових навчальних закладів ЗС України (під час занять, навчань та інших заходів підготовки?										
г*	Чи знає військовослужбовець вимоги керівних документів щодо заходів із кібербезпеки під час перебування в районах виконання бойових (спеціальних) завдань?										
Загальна кількість елементів за тему завдання, що оцінюється:											

Таблиця оцінювання проміжного контролю
за тему № 1 предмету навчання СТІ БЗВП/ висновок щодо рівня підготовки

Номер		Найменування заходу	Елементи, що сплановані	солдат *Прізвище, ініціали)*		солдат *Прізвище, ініціали)*		солдат *Прізвище, ініціали)*		солдат *Прізвище, ініціали)*		солдат *Прізвище, ініціали)*		солдат *Прізвище, ініціали)*		солдат *Прізвище, ініціали)*		солдат *Прізвище, ініціали)*		солдат *Прізвище, ініціали)*	
				Елементи, що засвоєно	%	Елементи, що засвоєно	%	Елементи, що засвоєно	%	Елементи, що засвоєно	%	Елементи, що засвоєно	%	Елементи, що засвоєно	%	Елементи, що засвоєно	%	Елементи, що засвоєно	%	Елементи, що засвоєно	%
розділу	теми		кількість																		
Загальна кількість елементів, за якими здійснено оцінювання (* включаючи критично важливі елементи)			**4 (*2)**																		
Елементи, які передбачають оцінювання теоретичних знань:			**4 (*2)**																		
I.	1.	Оцінка за розділ (тему)																			
Оцінка стандарту індивідуальної підготовки за проміжний контроль теми предмету навчання (виконання індивідуальних завдань):																					

6.2.2. Оціночний лист завдань курсу індивідуальної підготовки за предмет навчання “Основи кібербезпеки”

№ з/п	Елементи, що оцінюються	солдат *Прізвище, ініціали)*	солдат *Прізвище, ініціали)*	солдат *Прізвище, ініціали)*	солдат *Прізвище, ініціали)*	солдат *Прізвище, ініціали)*	солдат *Прізвище, ініціали)*	солдат *Прізвище, ініціали)*	солдат *Прізвище, ініціали)*	солдат *Прізвище, ініціали)*	солдат *Прізвище, ініціали)*
Теоретичні знання											
1.	Теоретичні питання відповідно до завдання 000Г(Б).97Л.03 (тема №1)										
Загальна оцінка за теми (розділи), що оцінюється:											
Загальна оцінка за СТІ БЗВП											

6.3. Оцінювання стандарту індивідуальної базової загальновійськової підготовки (згідно з оціночним листом/Check list):

6.3.1. Оцінка за елемент розділу:

"Виконав" – якщо визначений елемент розділу виконано в повному обсязі у встановлені строки, а порядок виконання відповідав визначеним нормам та вимогам керівних документів, критичних (суттєвих) розбіжностей виявлено не було;

"Не виконав" – якщо не виконано вимог на оцінку "виконав".

6.3.1.1. У разі коли елемент включає піделементи:

"виконав" – якщо не менше 75 % піделементів оцінено як "виконав";

"не виконав" – якщо не виконано вимог на оцінку "виконав".

ВАЖЛИВО! *Якщо елемент (піделемент) розділу (підрозділу) оціночного листа стандарту індивідуальної базової загальновійськової підготовки* ***передбачає виконання нормативу (вправи, прийому)****, відповідно оцінка за норматив (вправу, прийом) виставляється, як "Виконано", у разі виконання нормативу (вправи, прийому) на оцінку не нижче* ***"ЗАДОВІЛЬНО".***

6.3.1.2. Встановлені символи, які використовуються оцінювачем під час заповнення результатів спостереження за ходом і якістю виконання кожного елементу (піделементу) навчальних питань оціночного листа стандарту індивідуальної базової загальновійськової підготовки:

** - критично важливий елемент стандарту підготовки;*

+ - позначення виконаного елемента (піделемента);

– - позначення невиконаного елемента (піделемента);

0 - позначення елементу, що не оцінювався.

6.3.2. *Оцінка набуття військовослужбовцем індивідуальних спроможностей визначається шляхом перевірки рівня теоретичних знань у формі незалежного тестування (опитування) та практичних дій (умінь та навичок) під час виконання нормативів (вправ, прийомів тощо) за тему (курс) предмету навчання відповідної програми індивідуальної підготовки.*

ВАЖЛИВО! *При цьому під час виставлення загальної оцінки пріоритетом є розділи за практичні дії (уміння, навички), включаючи виконання практичних нормативів (вправ, прийомів тощо).*

6.3.3. Оцінки за розділ (-ли) теми теоретичних знань (розділ I), практичних дій (умінь, навичок) (розділ II) військовослужбовця за проміжний контроль предмету навчання визначаються відповідно до оцінок, отриманих за елементи розділу (-ів) теми та виставляється:

"Відмінно" – якщо військовослужбовець пройшов підготовку не менше 70% елементами теми що викладались, включаючи 100 % критично важливих елементів;

"Добре" – якщо військовослужбовець пройшов підготовку не менше 60% елементами теми що викладались, включаючи 80 % критично важливих елементів;

"Задовільно" – якщо військовослужбовець пройшов підготовку не менше 50% елементами теми що викладались, включаючи 60 % критично важливих елементів;

"Незадовільно" – якщо не виконано вимог на оцінку "Задовільно".

УВАГА! *Якщо стандарт індивідуальної базової загальновійськової підготовки за предмет навчання передбачає оцінку тільки теоретичних знань або практичних дій (умінь, навичок) військовослужбовця, загальна оцінка визначається оцінкою за "теоретичні знання" або практичні дії (уміння, навички) та виставляється за показниками,* ***які наведені в пункті 6.3.3 цього*** *стандарту індивідуальної базової загальновійськової підготовки.*

6.3.4. Оцінка стандарту індивідуальної підготовки за тему або курс предмету навчання визначається оцінкою за розділ "теоретичні знання" та оцінкою за розділ "практичних дій (умінь та навичок)" та виставляється:

"Відмінно" – якщо перша оцінка не нижче ніж "добре", а друга – "відмінно";

"Добре" – якщо перша оцінка не нижче ніж "задовільно", а друга – не нижче ніж "добре";

"Задовільно"– якщо обидві оцінки не нижче "задовільно" або якщо перша оцінка "незадовільно", а друга – не нижче "добре";

"Незадовільно" – якщо не виконано умов на оцінку "задовільно".

Робочі помітки:

Спостереження	
Обговорення	
Рекомендації	

ДЛЯ ЗАМІТОК

ДЛЯ ЗАМІТОК

ДЛЯ ЗАМІТОК

ДЛЯ ЗАМІТОК

ДЛЯ ЗАМІТОК