

Інформаційна безпека та кібербезпека держави

Навчальний посібник рекомендовано для викладання навчальних дисциплін «Інформаційна безпека» та «Кібербезпека».

Він містить теоретичні матеріали та правові основи з діяльності по забезпеченню інформаційної безпеки та кібербезпеки держави, значна увага приділена місцю медіа у проведенні інформаційної політики та спеціальних інформаційних операцій (інформаційно-психологічних операцій).

Посібник призначений для забезпечення навчального процесу з підготовки здобувачів вищої освіти за названими дисциплінами. Він розрахований на студентів, слухачів і викладачів вищих закладів гуманітарної спрямованості.

Це видання також буде корисним для аспірантів, науковців, представників спецслужб та інших силових відомств.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
УКРАЇНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІМЕНІ МИХАЙЛА ДРАГОМАНОВА

**Н.М. Титова, Н.М. Рідей, В.П. Настрадін,
М.М. Присяжнюк, С.М. Мамченко,
С.В. Артюх, Р.О. Яворська**

ІНФОРМАЦІЙНА БЕЗПЕКА ТА КІБЕРБЕЗПЕКА ДЕРЖАВИ

Навчальний посібник

За загальною редакцією
кандидата технічних наук, старшого наукового співробітника
Присяжнюка Миколи Миколайовича

Київ
Видавництво Ліра-К
2024

УДК 004.946.05.94
І-74

*Рекомендовано до друку Вченою радою
Українського державного університету імені Михайла Драгоманова –
протокол № 6 від 25 січня 2024 року*

Рецензенти:

В. В. Остроухов – доктор філософських наук, професор,
М. С. Коробчинський – доктор технічних наук, професор

І-74 **Інформаційна безпека та кібербезпека держави:** навчальний посібник / [Н. М. Титова, Н. М. Рідей, В. П. Настрадін, М. М. Присяжнюк, С. М. Мамченко, С. В. Артюх, Р. О. Яворська]; за заг. ред. М. М. Присяжнюка. Київ: Видавництво Ліра-К, 2024. 224 с.
ISBN 978-617-520-744-4

Навчальний посібник рекомендовано для викладання навчальних дисциплін «Інформаційна безпека» та «Кібербезпека». Він містить теоретичні матеріали та правові основи з діяльності по забезпеченню інформаційної безпеки та кібербезпеки держави, значна увага приділена місцю медіа у проведенні інформаційної політики та спеціальних інформаційних операцій (інформаційно-психологічних операцій).

Посібник призначений для забезпечення навчального процесу з підготовки здобувачів вищої освіти за названими дисциплінами. Він розрахований на студентів, слухачів і викладачів вищих закладів гуманітарної спрямованості. Це видання також буде корисним для аспірантів, науковців, представників спецслужб та інших силових відомств.

УДК 004.946.05.94

ISBN 978-617-520-744-4

© УДУ імені Михайла Драгоманова, 2024
© Колектив авторів, 2024
© Видавництво Ліра-К, 2024

ЗМІСТ

| | |
|---|------------|
| ВСТУП | 5 |
| РОЗДІЛ 1. ІНФОРМАЦІЙНА БЕЗПЕКА ТА КІБЕРБЕЗПЕКА В СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ | 8 |
| 1.1. Місце і роль інформаційної безпеки та кібербезпеки в системі національної безпеки України | 8 |
| 1.2. Визначення та сутність основних понять інформаційної безпеки та кібербезпеки | 14 |
| 1.3. Загальна характеристика національних інтересів України у сферах інформаційної безпеки та кібербезпеки | 21 |
| 1.4. Напрями, пріоритети та стратегічні цілі забезпечення інформаційної безпеки й кібербезпеки України | 22 |
| Питання для самоконтролю | 31 |
| Рекомендована література до розділу 1 | 33 |
| РОЗДІЛ 2. ВИКЛИКИ ТА ЗАГРОЗИ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ У СФЕРАХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА КІБЕРБЕЗПЕКИ | 34 |
| 2.1. Актуальні загрози національним інтересам України у сферах інформаційної безпеки та кібербезпеки | 34 |
| 2.2. Поняття та види загроз безпеці держави у кіберпросторі | 38 |
| 2.3. Основні об'єкти кіберзахисту України | 43 |
| 2.4. Комп'ютерна злочинність та кібертероризм як загрози кібербезпеці | 52 |
| Питання для самоконтролю | 78 |
| Рекомендована література до розділу 2 | 79 |
| РОЗДІЛ 3. ЗАГРОЗИ ЛЮДИНИ В ІНФОРМАЦІЙНІЙ СФЕРІ | 81 |
| 3.1. Інформаційний вплив та його різновиди | 81 |
| 3.2. Визначення об'єктів інформаційного впливу | 86 |
| 3.3. Поняття і сутність маніпулювання свідомістю людини | 97 |
| 3.4. Способи та технології маніпулювання свідомістю людини | 101 |
| 3.5. Інформаційно-психологічна безпека особи | 104 |
| Питання для самоконтролю | 113 |
| Рекомендована література до розділу 3 | 113 |
| РОЗДІЛ 4. ЗАСОБИ МЕДІА ТА ВЛАДА: ОСОБЛИВОСТІ СПІВПРАЦІ В ЦАРИНІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ | 115 |
| 4.1. Діяльність медіа в контексті інформаційної безпеки: правова підтримка | 115 |
| 4.2. Ризики та переваги комунікації в епоху інформаційного безладдя | 117 |

| | |
|---|------------|
| 4.3. Загрози інформаційній безпеці, що здійснюються через засоби медіа | 121 |
| 4.4. Використання штучних вкидань інформації в інформаційному протиборстві | 126 |
| Питання для самоконтролю | 133 |
| Рекомендована література до розділу 4 | 134 |
| РОЗДІЛ 5. ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ЖУРНАЛІСТСЬКІ ПРАКТИКИ, РОСІЙСЬКА ПРОПАГАНДА..... | |
| 5.1. Російські інформаційні нарративи проти України та специфіка їх розкриття..... | 135 |
| 5.2. Деструктивні впливи на свідомість аудиторії (російські спецоперації під прикриттям пропаганди проти вакцинації від COVID-19) | 143 |
| 5.3 Фактчекінг, як інструмент протидії в гібридній війні (на матеріалах проекту StopFake) | 145 |
| Питання для самоконтролю | 149 |
| Рекомендована література до розділу 5 | 149 |
| РОЗДІЛ 6. МАНІПУЛЯТИВНИЙ ВПЛИВ У МЕДІА | |
| 6.1. Технології масового маніпулятивного впливу | 150 |
| 6.2. Поняття та напрями реалізації сугестивних технологій маніпулятивного впливу..... | 176 |
| 6.3. Реалізація технологій маніпулювання в аудіовізуальних медіа..... | 188 |
| 6.4. Фактори впливу на діяльність медіа..... | 195 |
| 6.5. Реалізація технологій маніпулювання в онлайн-медіа | 201 |
| Питання для самоконтролю | 218 |
| Рекомендована література до розділу 6 | 219 |
| СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ..... | |
| | 220 |

ВСТУП

Сучасна епоха побудови інформаційного суспільства, тобто суспільства, в якому більшість працездатного населення (на відміну від аграрного чи індустріального) залучена до інформаційної сфери, сприяє розвитку нових форм і способів досягнення країнами політичних, економічних та інших цілей на інформаційному рівні. Не дивно, що в системі національної безпеки розвинених країн передбачено реалізацію національних стратегій (програм) національної безпеки, до яких входять політичні, воєнні, економічні, соціальні, інформаційні й інші стратегії. Особлива роль при цьому належить інформаційним стратегіям, основне призначення яких полягає в забезпеченні реалізації решти стратегій.

Останнім часом визначальної ваги набуває інформаційна безпека. Рівень інформаційного потенціалу все більшою мірою обумовлює оперативність прийняття державних рішень, структуру і якість озброєнь, оцінку рівня їх достатності, дієвість пропаганди, ефективність дій союзників і власних збройних сил і, в підсумку, результат збройного протистояння.

Концепція тотальної війни в традиційному розумінні себе зживає. Наступає епоха так званих “цивілізованих” війн, в яких політичні й економічні цілі досягаються не прямим збройним втручанням, а використанням нових форм насилля та підриву могутності противника зсередини.

Сучасному суспільству одним з основних джерел загроз національній безпеці держави стали “нетрадиційні”, зокрема інформаційні війни, які розвиненими країнами розглядаються як найбільш ефективний засіб забезпечення своїх національних інтересів.

У сучасних умовах Україна є об’єктом безперервного інформаційно-психологічного впливу, що обумовлено її геополітичним положенням і наявністю політичних, економічних та інших інтересів щодо нашої держави з боку розвинених країн та сусідніх держав, що зумовлює велику ймовірність втягнення її в інформаційну війну.

У цьому контексті проблеми забезпечення інформаційної безпеки національних інтересів у будь-якій сфері останнім часом набувають усе більшої значущості. Згідно зі ст.17 Конституції України, забезпечення інформаційної безпеки держави стоїть на одному рівні із захистом суверенітету й територіальної цілісності України, забезпеченням її економічної безпеки як найважливішими функціями держави.

Державна політика забезпечення інформаційної безпеки є невід’ємною складовою державної політики національної безпеки і являє собою офіційно прийняту систему поглядів та практичну діяльність органів державної влади і управління, спрямовану на забезпечення такого стану захищеності інтересів людини, суспільства та держави, при якому досягається інформаційний розвиток (інтелектуальний, соціально-політичний, технічний, морально-етичний), за якого сторонні інформаційні впливи не завдають їм суттєвої шкоди.

Інформаційна безпека є, як важливою самостійною сферою забезпечення національної безпеки, так і невід’ємною складовою кожної зі сфер національної безпеки. Інформаційні простір, інформаційні ресурси, інформаційна інфраструктура та технології значною мірою впливають на рівень і темпи соціально-економічного, науково-технічного й культурного розвитку. Тому розвиток України як суверенної, демократичної, правової та економічно стабільної держави можливий за умови забезпечення інформаційної безпеки.

Для сучасного етапу генезису суспільства характерне постійне зростання впливу інформаційної сфери, до складу якої входять: інформація, інформаційні зв'язки та інформаційні системи, об'єкти, які займаються підготовкою, зберіганням, поширенням і використанням інформації, а також система регулювання інформаційних відносин.

Національна безпека держави має стійку залежність від інформаційної безпеки та кібербезпеки, яка постійно зростає із розвитком інформаційних технологій.

Стратегією кібербезпеки України, затвердженою Указом Президента України від 26 серпня 2021 року (далі – Стратегія), визначено одним із пріоритетів національної безпеки України – забезпечення кібербезпеки з посиленням спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі.

Стратегія відзначає, що кіберпростір разом з іншими фізичними просторами визнано одним з можливих театрів сучасних воєнних дій. Набирає сили тенденція зі створення кібервійськ, до завдань яких належить не лише забезпечення захисту критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі, що включає виведення з ладу критично важливих об'єктів інфраструктури противника шляхом руйнування інформаційних систем, які управляють такими об'єктами.

Одним з основних джерел загроз національній та міжнародній кібербезпеці залишається російська агресивна політика, яка активно реалізує концепцію інформаційного протиборства, базовану на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно застосовуються у гібридній війні проти України. Така деструктивна активність створює реальну загрозу вчинення актів кібертероризму та кібердиверсії стосовно національної інформаційної інфраструктури.

Прогнозується зростання інтенсивності міждержавного протиборства і розвідувально-підривної діяльності у кіберпросторі. Розширюється коло держав, які намагаються сформувати власну кіберрозвідку, оволодіти сучасними технологіями розвідувально-підривної діяльності у кіберпросторі, посилюють державний контроль за національними сегментами мережі Інтернет¹.

Сучасному періоду інтенсивного розвитку суспільства притаманне зростання ролі інформаційної сфери, що поєднує інформаційний простір та кіберпростір, яка є сукупністю інформації, інформаційної інфраструктури і суб'єктів, що реалізують регулювання інформаційних відносин у суспільстві. Інформаційна сфера постає системо-утворюючим чинником життя суспільства; вона здійснює активний вплив на стан воєнної, економічної, політичної, та інших сфер національної безпеки держави.

Тому цілеспрямовані чи ненавмисні впливи на інформаційну сферу з боку зовнішніх чи внутрішніх джерел можуть завдати серйозної шкоди цим інтересам і являють собою загрози для безпеки держави, людини та суспільства.

Аналіз історії розвитку земної цивілізації показує, що на всіх її етапах інформація була як найважливішим об'єктом, так і засобом боротьби між людьми, народами, державами, військово-політичними блоками і союзами. Найактивніше інформаційно-психологічне протиборство велося в ході світових і локальних воєн, національних і релігійних конфліктів.

¹ Указ Президента України від 14 травня 2021 року № №447/2021 “Про Стратегію кібербезпеки України”. URL: <https://www.president.gov.ua/documents/4472021-40013>

В умовах розвитку ЗМІ, інформаційних технологій і цифрової техніки інформаційне протиборство у світі стає масштабнішим і результативнішим.

Аналізу ведення локальних війн і збройних конфліктів останнього десятиліття доводить, що протиборство у військовій сфері дедалі частіше переміщується у кіберпростір.

Нині склався новий всесвітній простір інформаційно-цифрової реальності, що співіснує із звичайною фізичною реальністю, але кардинально змінює звичні політичні, економічні й суспільні відносини. Інформація все більше перетворюється на символ політичного впливу та економічного процвітання, стає феноменом геополітичного рангу.

Таким чином, геополітичний авторитет держав на міжнародній арені, його можливості впливати на світові події тепер залежать не тільки від економічної й військової могутності. Усе більшого значення набувають не силові, а інформаційні фактори: можливості ефективно впливати на інтелектуальний потенціал інших країн, поширювати та впроваджувати в суспільну свідомість відповідні духовні й ідейні цінності, трансформувати та підривати традиційні підвалини націй і народів.

Науково-технічна революція початку XXI ст. спричинила в усьому світі глибокі системні перетворення. Стрімкий розвиток інформаційних технологій, інформатизація та комп'ютеризація, створення глобального інформаційного простору сформували принципово нові субстанції – *інформаційне суспільство*, *інформаційний простір* та *кіберпростір*, які мають невичерпний потенціал і відіграють важливу роль в економічному та соціальному розвитку країн світу.

Разом з цим виникли такі нові терміни, як “*кіберзагрози*”, “*кібербезпека*”, “*кібертероризм*” тощо. Створення інформаційного суспільства призводить до виникнення багатьох інформаційних загроз та кіберзагроз. Реалізація цих загроз може завдати значної шкоди як на мікро, так і на макрорівні в рамках суверенних держав, а також і в світовому масштабі. Стійку залежність від кібербезпеки, яка постійно зростає із розвитком інформаційних технологій, має національна безпека держави. Це привело до розуміння необхідності вирішення проблеми нейтралізації або мінімізації цієї сукупності загроз.

Національна безпека держави має стійку залежність від інформаційної безпеки та кібербезпеки, яка постійно зростає із розвитком інформаційних технологій.

Для ефективного забезпечення національної безпеки в інформаційній сфері необхідні відповідні висококваліфіковані спеціалісти.

Здобувачі вищої освіти отримують теоретичні знання та практичні навички, необхідні для подальшої професійної діяльності в Службі безпеки України, Міністерстві оборони України, Державній службі спеціального зв'язку та захисту інформації України та інших структурах, що забезпечують національну безпеку у сфері кібербезпеки держави.

Тому посібник буде корисним здобувачам вищої освіти, науково-педагогічним працівникам та науковцям і сприятиме реалізації вимог освітньо-кваліфікаційних характеристик й освітньо-професійних програм підготовки кваліфікованих фахівців, що передбачають оволодіння знаннями та вміннями для вирішення професійно орієнтованих типових завдань забезпечення інформаційної безпеки та кібербезпеки.

РОЗДІЛ 1

ІНФОРМАЦІЙНА БЕЗПЕКА ТА КІБЕРБЕЗПЕКА В СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

1.1. Місце і роль інформаційної безпеки та кібербезпеки в системі національної безпеки України

Оскільки інформаційна безпека та кібербезпека направлені на забезпечення стану захищеності життєво важливих інтересів людини, суспільства і держави від деструктивних інформаційних впливів, варто розглядати ці два поняття нерозривно, як важливі складові національної безпеки України.

Також варто зазначити, що інформаційна безпека є як самостійною сферою національної безпеки України, так і невід'ємною складовою кожної із її сфер, у тому числі й кібербезпеки, лежить в основі кібербезпеки. Це обумовлює необхідність розгляду її понять з урахуванням сталого поняттєвого апарату і завдань національної безпеки.

Основні засади державної політики, спрямованої на захист національних інтересів і гарантування в Україні безпеки особи, суспільства і держави від зовнішніх і внутрішніх загроз в усіх сферах життєдіяльності містяться в *Законі України “Про національну безпеку України” від 2018 року*. У ньому наведені такі визначення базових термінів:

1) національна безпека – захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від *реальних та потенційних загроз*;

2) національні інтереси – життєво важливі інтереси людини, суспільства і держави, реалізація яких забезпечує державний суверенітет України, її прогресивний демократичний розвиток, а також безпечні умови життєдіяльності і добробут її громадян;

3) загрози національній безпеці – явища, тенденції і чинники, що унеможливають чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України.

Державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, безпеки критичної інфраструктури, кібербезпеки України тощо.

Рівень розвитку та безпека інформаційного простору й кіберпростору, які є одними з найвагоміших факторів у всіх сферах національної безпеки, активно впливають на стан політичної, економічної та інших складових національної безпеки України. У зв'язку з цим доцільно розглядати інформаційну безпеку та кібербезпеку як складові інших сфер національної безпеки. Разом з цим, інформаційна безпека та кібербезпека є самостійними складовими національної

безпеки і в цьому проявляється їх подвійний характер. Це обумовлюється наступним:

- прагненням кожної держави реалізувати та захистити власні національні інтереси, що направлені на формування та накопичення національного інформаційного потенціалу в умовах глобалізації світових інформаційних процесів;

- необхідністю не лише розвивати й посилювати національний інформаційний потенціал, але й захищати від широкого спектра існуючих та потенційних інформаційних загроз та кіберзагроз;

- існуванням реальної потреби в захисті всіх суб'єктів інформаційних стосунків від можливих негативних наслідків упровадження та використання інформаційних технологій;

- наявною можливістю інформаційного тиску на Україну, навіть інформаційної агресії та кібертероризму з боку окремих країн світу з метою одержання односторонніх переваг в політичній, економічній, військовій та інших сферах, а також інформаційного впливу на свідомість і підсвідомість індивідів, сім'ю, суспільство й державу, що загрожує національній безпеці країни.

Не дивно, що в системі національної безпеки розвинених країн передбачено реалізацію національних стратегій (програм) національної безпеки, до яких входять політичні, воєнні, економічні, соціальні й інші стратегії. Особлива роль при цьому відводиться *інформаційним стратегіям та кіберстратегіям*, основне призначення яких полягає в забезпеченні реалізації решти стратегій.

Інформаційні стратегії та кіберстратегії набувають вирішального значення в разі реалізації політичних стратегій співдружності та є своєрідною “зброєю”, якщо реалізуються стратегії суперництва.

Отже, інформаційна безпека та кібербезпека є одними з основних складових національної безпеки країни.

У законі України “*Про національну безпеку України*”, як показано на Рис. 1, окремими сферами визначені інформаційна безпека та кібербезпека.

Їх забезпечення з використанням вдало сформульованої національної інформаційної політики значною мірою має сприяти досягненню успіху у виконанні завдань політичної, воєнно-політичної, воєнної, економічної, соціальної та інших сферах державної діяльності. Зокрема, впровадження успішної інформаційної політики може справити істотний вплив на зниження напруженості та розв'язання зовнішньополітичних і воєнних конфліктів.

У попередньому Законі “*Про основи національної безпеки України*” від 08.06.2017 р. були визначені основні напрями державної політики з питань національної безпеки України в інформаційній сфері, які з певних причин не увійшли до нового Закону “*Про національну безпеку України*”, але не втратили своєї актуальності. *До них відноситься:*

- забезпечення інформаційного суверенітету України;

- вдосконалення державного регулювання розвитку інформаційної сфери через створення нормативних, правових та економічних передумов для розвитку національної інформаційної інфраструктури і ресурсів, запровадження

сучасних технологій у цій сфері, наповнення інформаційного простору в середині держави та світового правдивою інформацією про Україну;



Рис. 1.1.1. Основні сфери національної безпеки України

– активне залучення ЗМІ до боротьби з корупцією, зловживаннями службовим становищем, іншими явищами, що несуть загрози національній безпеці України;

– забезпечення беззаперечного дотримання конституційних прав громадян на свободу слова, вільного доступу до інформації, недопущення безпідставного втручання органів державної влади, місцевого самоврядування та їх посадових осіб у діяльність ЗМІ, дискримінації в інформаційній сфері й переслідування за політичні позиції журналістів;

– вжиття комплексних заходів захисту національного інформаційного простору та протидії монополізації інформаційної сфери України.

За роки незалежності в Україні створено основні елементи системи забезпечення інформаційної безпеки та кібербезпеки, напрацьовано нормативно-правову базу їх діяльності, визначено основні функції й повноваження державних органів в інформаційній сфері.

Розглянемо основні елементи системи забезпечення інформаційної безпеки України, їх функції та повноваження, схему взаємодії, а також чинники, що знижують ефективність діяльності органів державної влади щодо забезпечення інформаційної безпеки України.

Правові засади побудови, поточної діяльності та розвитку системи забезпечення інформаційної безпеки України складають: Конституція України, Закон України “Про національну безпеку України”, інші законодавчі та нормативні акти, що регулюють відносини в інформаційній сфері. Створене правове підґрунтя має досить розвинутий характер: більшість правових норм

відповідають міжнародним стандартам, принципам і нормам забезпечення прав громадян на свободу слова, отримання та поширення інформації. Водночас чинна нормативно-правова база в інформаційній сфері потребує вдосконалення з метою усунення суперечностей і заповнення прогалин у законодавстві.

Правову основу забезпечення кібербезпеки України становлять Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, цей та інші закони України, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України.

Основні функції системи забезпечення інформаційної безпеки України:

– створення та забезпечення діяльності державних органів – елементів системи забезпечення інформаційної безпеки, що включає:

– створення правових засад для побудови, розвитку та функціонування системи;

– формування організаційної структури системи та її окремих елементів, визначення та раціональний розподіл їх функцій;

– комплексне забезпечення діяльності елементів системи: кадрове, фінансове, матеріальне, технічне, інформаційне та інші;

– підготовку елементів системи до виконання покладених на них функцій згідно з призначенням;

– управління діяльністю системи забезпечення інформаційної безпеки, що включає:

– вироблення стратегії і планування конкретних заходів щодо забезпечення інформаційної безпеки;

– організацію і безпосереднє керівництво системою та її структурними елементами;

– оцінку результативності дій, витрат на проведення заходів щодо забезпечення інформаційної безпеки та їх наслідків;

– здійснення планової та оперативної діяльності щодо забезпечення інформаційної безпеки, що включає:

• визначення національних інтересів та їх пріоритетів в інформаційній сфері;

• прогнозування, виявлення та оцінку можливих загроз, дестабілізуючих чинників та конфліктів в інформаційній сфері, причин їх виникнення, а також наслідків їх прояву;

• запобігання та усунення впливу загроз та дестабілізуючих чинників на національні інтереси в інформаційній сфері;

• локалізацію, деескалацію та розв'язання інформаційних конфліктів;

• ліквідацію наслідків інформаційних конфліктів або впливу дестабілізуючих чинників;

• міжнародне співробітництво в сфері інформаційної безпеки, що включає:

- розроблення нормативно-правової бази, що регулює інформаційні відносини між державами та їх взаємодію в галузі інформаційної безпеки;
- входження в існуючі та утворення нових двосторонніх і багатосторонніх структур (організацій), діяльність яких спрямована на спільне вирішення проблем інформаційної безпеки;
- участь у роботі керівних, виконавчих та забезпечувальних підрозділів цих структур (організацій), спільне проведення планових та оперативних заходів.

Шляхами забезпечення національної системи кібербезпеки є:

- вироблення і оперативна адаптація державної політики у сфері кібербезпеки, спрямованої на розвиток кіберпростору, досягнення сумісності з відповідними стандартами Європейського Союзу та НАТО;
- створення нормативно-правової та термінологічної бази у сфері кібербезпеки, гармонізації нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної безпеки та кібербезпеки відповідно до міжнародних стандартів, зокрема стандартів Європейського Союзу та НАТО;
- встановлення обов'язкових вимог інформаційної безпеки об'єктів критичної інформаційної інфраструктури, у тому числі під час їх створення, введення в експлуатацію, експлуатації та модернізації з урахуванням міжнародних стандартів та специфіки галузі, до якої належать відповідні об'єкти критичної інформаційної інфраструктури;
- формування конкурентного середовища у сфері електронних комунікацій, надання послуг із захисту інформації та кіберзахисту;
- залучення експертного потенціалу наукових установ, професійних та громадських об'єднань до підготовки проектів концептуальних документів у сфері кібербезпеки;
- проведення навчань щодо дій у разі надзвичайних ситуацій та інцидентів у кіберпросторі;
- функціонування системи аудиту інформаційної безпеки, запровадження кращих світових практик і міжнародних стандартів з питань кібербезпеки та кіберзахисту;
- розвитку мережі команд реагування на комп'ютерні надзвичайні події;
- розвитку та вдосконалення системи технічного і криптографічного захисту інформації;
- забезпечення дотримання вимог законодавства щодо захисту державних інформаційних ресурсів та інформації;
- створення та забезпечення функціонування Національної телекомунікаційної мережі;
- обміну інформацією про інциденти кібербезпеки між суб'єктами забезпечення кібербезпеки у порядку, визначеному законодавством;
- впровадження єдиної (універсальної) системи індикаторів кіберзагроз з урахуванням міжнародних стандартів з питань кібербезпеки та кіберзахисту;
- підготовки фахівців освітньо-кваліфікаційних рівнів бакалавра і магістра за державним замовленням в обсязі, необхідному для задоволення

потреб державного сектору економіки, а також за небюджетні кошти, у тому числі для підвищення кваліфікації та проведення обов'язкової періодичної атестації (переатестації) персоналу, відповідального за забезпечення кібербезпеки об'єктів критичної інфраструктури, з урахуванням міжнародних стандартів;

- впровадження організаційно-технічної моделі національної системи кібербезпеки як комплексу заходів, сил і засобів кіберзахисту, спрямованих на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів, спрямованих на мінімізацію вразливості комунікаційних систем;

- встановлення вимог (правил, настанов) щодо безпечного використання мережі Інтернет та надання електронних послуг державними органами;

- державно-приватної взаємодії у запобіганні кіберзагрозам об'єктам критичної інфраструктури, реагуванні на кібератаки та кіберінциденти, усуненні їх наслідків, зокрема в умовах кризових ситуацій, надзвичайного і воєнного стану, в особливий період;

- періодичного проведення огляду національної системи кібербезпеки, розроблення індикаторів стану кібербезпеки;

- стратегічного планування та програмно-цільового забезпечення у сфері розвитку електронних комунікацій, інформаційних технологій, захисту інформації та кіберзахисту;

- розвитку міжнародного співробітництва у сфері кібербезпеки, підтримки міжнародних ініціатив у сфері кібербезпеки, що відповідають національним інтересам України, поглиблення співпраці України з Європейським Союзом та НАТО з метою посилення спроможності України у сфері кібербезпеки, участі у заходах із зміцнення довіри при використанні кіберпростору, що проводяться під егідою Організації з безпеки і співробітництва в Європі;

- здійснення оперативно-розшукових, розвідувальних, контр-розвідувальних та інших заходів, спрямованих на запобігання, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються з використанням кіберпростору, розслідування, переслідування, оперативного реагування та протидії кіберзлочинності, розвідувально-підривній, терористичній та іншій діяльності у кіберпросторі, що завдає шкоди інтересам України, використанню мережі Інтернет у воєнних цілях;

- здійснення воєнно-політичних, військово-технічних та інших заходів для розширення можливостей Воєнної організації держави, сектору безпеки і оборони з використанням кіберпростору, створення і розвитку сил, засобів та інструментів можливої відповіді на агресію у кіберпросторі, яка може застосовуватися як засіб стримування воєнних конфліктів та загроз з використанням кіберпростору;

- обмеження участі у заходах із забезпечення інформаційної безпеки та кібербезпеки будь-яких суб'єктів господарювання, які перебувають під контролем держави, визнаної Верховною Радою України державою-агресором, або держав та осіб, стосовно яких діють спеціальні економічні та інші обмежувальні заходи

(санкції), прийняті на національному або міжнародному рівні внаслідок агресії щодо України, а також обмеження використання продукції, технологій та послуг таких суб'єктів для забезпечення технічного та криптографічного захисту державних інформаційних ресурсів, посилення державного контролю в цій сфері;

– розвитку системи контррозвідувального забезпечення кібербезпеки, призначеної для запобігання, своєчасного виявлення та протидії зовнішнім і внутрішнім загрозам безпеці України з використанням кіберпростору; усунення умов, що їм сприяють, та причин їх виникнення;

– проведення розвідувальних заходів із виявлення та протидії загрозам національній безпеці України у кіберпросторі, виявлення інших подій і обставин, що стосуються сфери кібербезпеки.

Виконання повного переліку цих функцій є необхідною умовою ефективного функціонування системи забезпечення інформаційної безпеки та кібербезпеки України.

1.2. Визначення та сутність основних понять інформаційної безпеки та кібербезпеки

Оскільки основою кібербезпеки є інформаційна безпека, то варто з'ясувати спочатку сутність інформаційної безпеки, а згодом – кібербезпеки.

Уперше основні напрямки забезпечення безпеки в інформаційній сфері, під якою часто розуміють інформаційну безпеку як складову національної безпеки України розглядалися в Концепції (основах державної політики) національної безпеки України 1997 р. (втратила чинність).

До теперішнього часу поняття “безпека інформаційної сфери” часто розуміють як “інформаційна безпека”, що є складовою національної безпеки України. Проте, ці поняття не є тотожними за змістом. Під інформаційною сферою на змістовому рівні слід розуміти безпосередньо інформацію та сферу її обігу. Тобто безпека інформаційної сфери – це стан захищеності інформації та сфер її створення, накопичення, зберігання, оброблення, розповсюдження і використання.

Безпека інформації – стан, що забезпечує захист інформації від загроз для неї (ДСТУ. *Технічний захист інформації. Терміни і визначення*).

Інформаційна безпека – це:

1) такий стан інформаційної озброєності особистості, суспільства, держави (озброєності їх знаннями), при якому досягається захищеність і реалізація їх життєво важливих інтересів і гармонічний розвиток незалежно від наявності внутрішніх і зовнішніх загроз;

2) такий стан інформаційного забезпечення завдань національної безпеки, при якому досягається захищеність і реалізація життєво важливих інтересів, гармонічного розвитку і потреб в інформації особистості, суспільства, держави незалежно від наявності внутрішніх і зовнішніх загроз;

3) стан інформаційного середовища, при якому гарантується його розвиток і використання в інтересах особистості, суспільства і держави;

Книги, які можуть вас зацікавити



Кібернологія: цифрова віртуальність та воєнна реальність



Воєнна комп'ютерна інженерія: логіка та криптосистема



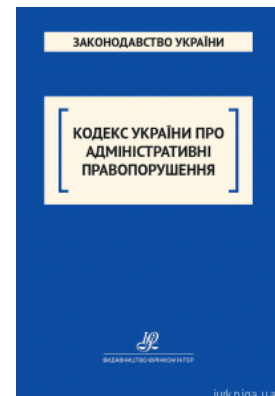
Психодіагностика лідерських якостей військовослужбовців



Кримінальний кодекс України. Юрінком Інтер



Кримінальний процесуальний кодекс України. Юрінком Інтер



Кодекс України про адміністративні правопорушення. Юрінком Інтер

Перейти до галузі права
Інформаційне право



[Перейти на сайт →](#)