Рівненський державний гуманітарний університет
Факультет історії, політології та міжнародних відносин
Кафедра міжнародних відносин та політології

Термінологічний мінімум з дисципліни «Інформаційна безпека»

для здобувачів вищої освіти першого (бакалаврського) рівня спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії».

Рівне-2024 рік

УДК 327: 316.77 (03)
Т.35
Термінологічний мінімум з дисципліни «Інформаційна безпека» для здобувачів вищої освіти першого (бакалаврського) рівня спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії». Рівне: РДГУ, 2024. 14 с.

Укладач: к.політ. наук, доц. кафедри міжнародних відносин та політології **Кундеус О. М.**

Рецензенти:

Вівчар І.В. кандидат політичних наук, доцент кафедри міжнародних відносин та політології РДГУ.

Чернюк І.А. кандидат політичних наук, доцент кафедри суспільних наук Національного університету водного господарства та природокористування.

Термінологічний мінімум укладено на основі тематики навчального курсу. Містить основні визначення, які формують понятійний апарат курсу «Інформаційна безпека».

Затверджено на засіданні кафедри міжнародних відносин та політології
Протокол від 26 серпня 2024 № 1

Завідувач кафедри міжнародних відносин та політології _____ (доц.. Крет Р.М.)

Схвалено навчально-методичною комісією факультету історії, політології та міжнародних відносин
Протокол від 26 серпня 2024р. № 7

Голова методичної комісії _____ (проф..каф...Галуха Л.Ю)

Активне забезпечення інформаційної безпеки спрямоване на завчасне виявлення та попередження загроз.

Безпека – стан, при якому кому-небудь, чому-небудь не загрожує небезпека будь-якого виду, існує захист від небезпеки.

Безпека держави – положення, при якому державі не загрожує небезпека. Досягається наявністю ефективного механізму управління і координації діяльності політичних сил та громадських груп, а також активних інститутів (органів) їхнього захисту.

Безпека особистості – положення, при якому особистості не загрожує небезпека. Безпека особистості полягає у формуванні комплексу правових і моральних норм, суспільних інститутів та організацій, що дозволили розвивати й реалізовувати соціально значущі здібності й потреби, не зазнаючи при цьому протидії держави й суспільства.

Безпека суспільства – наявність суспільних інститутів, норм, розвинених форм суспільної свідомості, які дозволяють реалізувати права та свободи всіх груп населення і протистояти діям, що ведуть до розколу суспільства (зокрема і з боку держави).

Гриф секретності – реквізит матеріального носія секретної інформації, що засвідчує ступінь секретності даної інформації.

Держава – сукупність офіційних органів влади в цій чи іншій країні, основний заклад і спосіб політико-правової організації життя суспільства на чолі з одноособовим або колективним правителем, органами виконавчої та інших видів влади й вертикальною системою управління, за допомогою якої здійснюється влада, охороняється існуючий лад, забезпечується нормальне життя людей.

Державна система забезпечення інформаційної безпеки держави являє собою організаційне об’єднання державних органів, а також сил та засобів інформаційної безпеки, що виконують свої функції на основі закону під контролем і захистом судової влади. Державна система становить найважливішу ланку системи інформаційної безпеки особистості, суспільства й держави в правовій державі.

Державна таємниця – вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки й техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані в порядку, встановленому Законом України «Про державну таємницю», і підлягають охороні державою.

Дестабілізуючі фактори – явища та процеси природного й штучного походжень, що породжують інформаційні загрози.

Допуск до державної таємниці – процедура оформлення права громадян на доступ до відомостей, що становлять державну таємницю, а підприємств, установ і організацій – на проведення робіт з використанням таких відомостей.

Доступ до відомостей, що становлять державну таємницю – надання уповноваженою посадовою особою дозволу громадянину на ознайомлення з конкретною секретною інформацією та провадження діяльності, пов’язаної з державною таємницею, або ознайомлення з конкретною секретною інформацією та провадження діяльності, пов’язаної з державною таємницею, цією посадовою особою відповідно до її службових повноважень.

Життєво важливі інтереси – сукупність потреб, задовольняння яких надійно забезпечує існування і можливості прогресивного розвитку особистості, суспільства й держави.

Забезпечення інформаційної безпеки – сукупність заходів, призначених для досягнення стану захищеності потреб особистостей, суспільства й держави в інформації.

Загроза – можлива небезпека, тобто здатність заподіяти будь-яку шкоду, призвести до будь-якого нещастя.

Загрози інформаційній безпеці – 1. сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства й держави в інформаційній сфері; 2. дія чи подія, що може призвести до руйнування, спотворення чи несанкціонованого власником чи володільцем доступу до інформаційних ресурсів.

Найбільшу загрозу інформаційній безпеці становить: можливість утрати, порушення цілісності або блокування інформації; відкриття конфіденційної інформації; несанкціоноване використання ресурсів; помилкове використання ресурсів; несанкціонований обмін інформацією; відмова від інформації; відмова від обслуговування.

Закони інформаційної боротьби визначаються як суттєві, необхідні відношення, що характеризують впорядкованість будови і функціонування, тенденції зміни й розвитку тих чи інших явищ інформаційної боротьби. Закони інформаційної боротьби являють собою більш менш точне відображення у свідомості людей тих об'єктивних зв'язків і відносин, які існують і діють в інформаційному просторі. Якщо вони пізнані, відображені, описані, то стають основою для практичної діяльності з підготовки і ведення інформаційної боротьби.

Засекречування відомостей та їх носіїв – введення в передбаченому порядку для відомостей, що становлять державну таємницю, обмежень на їх поширення.

Інженерно-технічний захист – це сукупність спеціальних органів, технічних засобів та заходів для їхнього використання в інтересах захисту конфіденційної інформації.

Інтелектуальні способи інформаційної боротьби реалізують рефлексне управління противником. Застосування таких способів дозволяє досягти інформаційної переваги в якості інформації, яка використовується для управління військами (силами).

Інтереси особистості в інформаційній сфері полягають у:

- реалізації конституційних прав особи й громадянина на доступ до інформації, а також на використання інформації в інтересах здійснення діяльності, яка не заборонена законом;
- у захисті інформації, що забезпечує особисту безпеку.

Інтереси держави в інформаційній сфері полягають у:

- створенні умов для гармонічного розвитку інформаційної інфраструктури України;
- реалізації конституційних прав і свобод людини й громадянина в галузі одержання інформації й користування нею з метою забезпечення непорушності конституційного ладу, суверенітету й територіальної цілісності України, політичної, економічної та соціальної стабільності;
- забезпеченні законності та правопорядку, розвитку рівноправного й взаємовигідного міжнародного співробітництва.

Інформація:

1) документовані або публічно проголошені відомості про події та явища, що відбуваються в суспільстві, державі та навколишньому природному середовищі;

2) відомості про осіб, предмети, технології, засоби, ресурси, події та явища, що відбуваються в усіх сферах діяльності держави, життя суспільства, та навколишньому природному середовищі, незалежно від форми їх представлення, будь-які знання про предмети, факти, поняття і т. ін. проблемної сфери, якими обмінюються користувачі системи оброблення даних.

Інформатизація:

1) сукупність взаємопов'язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, які спрямовані на створення умов для задоволення інформаційних потреб громадян та суспільства на основі створення, розвитку й використання інформаційних систем, мереж, ресурсів та інформаційних технологій, які побудовані на основі застосування сучасної обчислювальної та комунікаційної техніки;

2) діяльність, спрямована на створення та широкомасштабне використання в усіх сферах життя суспільства інформаційних технологій.

Інформаційна агресія – незаконні дії однієї зі сторін в інформаційній сфері, спрямовані на нанесення супротивнику конкретної, відчутної шкоди в окремих областях його діяльності шляхом обмеженого та локального по своїх масштабах застосування сили.

Інформаційна безпека – це стан захищеності інформаційного середовища суспільства, що забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави.

Під інформаційною безпекою варто розуміти єдність захисту наступних компонентів:

- системи виробництва інформаційних продуктів;
- системи доставки інформаційних продуктів до споживача;
- системи виробництва засобів виробництва інформаційних продуктів та їх доставки;
- системи виробництва інформаційних технологій;
- системи накопичення і збереження інформаційних продуктів;
- системи сервісного обслуговування елементів інформаційної інфраструктури;
- системи підготовки кадрів.

Інформаційна безпека держави (суспільства) характеризується мірою захищеності держави (суспільства) та стійкості основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи тощо) відносно небезпечних (дестабілізуючих, деструктивних, уражаючих державні інтереси тощо) інформаційних впливів, причому як з упровадження, так і добування інформації.

Інформаційна безпека особистості – це захищеність психіки і свідомості людини від небезпечних інформаційних впливів: маніпулювання свідомістю, дезінформування, спонукання до самогубства, образ тощо.

Інформаційна безпека України – стан захищеності її національних інтересів у інформаційній сфері, що визначаються сукупністю збалансованих інтересів особистості, суспільства й держави.

Інформаційна битва являє собою сукупність узгоджених і взаємопов'язаних за метою, завданнями, місцем і часом інформаційних дій та ударів, об'єднаних загальним задумом, які здійснюються спеціально виділеними силами і засобами та спрямовані для вирішення одного оперативного завдання інформаційної боротьби. Залежно від масштабу й виду інформаційної операції в ній може бути одна або декілька інформаційних битв, що здійснюються одночасно або послідовно.

Інформаційна блокада – це узгоджене за завданнями, місцем і часом застосування сил і засобів з метою найбільш повного зниження можливостей противника з одержання і використання інформації, необхідної для ефективного ведення операцій (бойових дій).

Інформаційна боротьба – це боротьба з використанням спеціальних способів і засобів для впливу на інформаційну сферу (середовище) конфронтуючої сторони, а також для захисту власної інформаційної сфери в інтересах досягнення поставленої мети. Інформаційна боротьба може бути як самостійним видом, так і складовою частиною будь-якого іншого різновиду боротьби (збройної, ідеологічної, економічної і т. ін.). Вона ведеться постійно як у мирний, так і у воєнний час. Масштаби інформаційної боротьби настільки великі, що її підготовка й ведення повинні носити плановий, систематичний характер, заснований на глибоких знаннях законів і закономірностей інформаційної боротьби.

Інформаційні відносини – відносини, які виникають у всіх сферах життя й діяльності держави, суспільства і людини при одержанні, використанні, поширенні та зберіганні інформації.

Інформаційна війна – комплекс заходів і операцій, спрямованих на забезпечення інформаційної переваги щодо потенційного або реального противника.

Інформаційні дії (акції) – це сукупність узгоджених за метою, завданнями, місцем і часом заходів, що проводяться силами і засобами, залученими для ведення інформаційної боротьби, протягом певного часу в певному районі (напрямку). Під час інформаційних дій можуть здійснюватися інформаційні удари.

Інформаційна експансія – діяльність із досягнення національних інтересів методом безконфліктного проникнення в інформаційну сферу з метою: поступової, плавної, непомітної для суспільства зміни системи соціальних відносин за зразком системи джерела експансії; витіснення положень національної ідеології і національної системи цінностей і заміщення їхніми власними цінностями й ідеологічними установками; збільшення ступеня свого впливу та присутності, встановлення контролю над стратегічними інформаційними ресурсами.

Інформаційне забезпечення: підтримка засобами систем баз даних і баз знань процесів виробництва, торгівлі, керування, навчання, наукових досліджень та будь якої іншої діяльності в усіх сферах життя суспільства, які спрямовані на створення умов для задоволення інформаційних потреб людини, суспільства та держави.

Інформаційне забезпечення інформаційної безпеки включає збирання (добування) відомостей про дестабілізуючі фактори та інформаційні загрози, їхнє оброблення, обмін інформацією між органами управління і силами та засобами системи інформаційної безпеки. Його основу складає збирання (добування) необхідних відомостей, здійснюване в процесі розвідувальної, контррозвідувальної, оперативно-розшукової і оперативно-інформаційної діяльності.

Інформаційна зброя – сукупність засобів, методів і технологій, що забезпечують можливість силового впливу на інформаційну сферу протилежної сторони з метою руйнування її інформаційної інфраструктури, системи управління державою, зниження духовного потенціалу суспільства.

Інформаційна зброя атаки – це інформаційна зброя, за допомогою якої здійснюється вплив на інформацію, що зберігається, обробляється й передається в інформаційно-обчислювальних мережах (ІОМ) і (або) порушуються інформаційні технології, що застосовуються в ІОМ.

Інформаційна зброя забезпечення – це інформаційна зброя, за допомогою якої здійснюється вплив на засоби захисту інформації об’єкта атаки, наприклад, інформаційно-обчислювальну систему. До складу інформаційної зброї забезпечення входять засоби

комп'ютерної розвідки та засоби подолання системи захисту інформаційно-обчислювальної системи.

Інформаційні злочини можуть вчинятися із використанням як інформаційно комп'ютерних, так й інформаційно психологічних методів впливу.

Інформаційна інфраструктура: сукупність взаємодіючих систем виробництва, накопичення, збереження і розвитку інформаційних продуктів та їх доставки, виробництво інформаційних технологій, сервісного обслуговування інфраструктури й системи підготовки кадрів.

Інформаційна інфраструктура включає в себе:

- ***організаційні структури***, що забезпечують функціонування і розвиток єдиного інформаційного простору (зокрема, збирання, обробку, збереження, поширення, пошук і передачу інформації). Забезпечувальну частину складають науково-методичне, інформаційне, лінгвістичне, технічне, кадрове забезпечення;
- ***інформаційно-телекомунікаційні структури*** – територіально розподілені державні й корпоративні комп'ютерні мережі, телекомунікаційні мережі й системи спеціального призначення та загального користування, мережі й канали передачі даних, засоби комутації і керування інформаційними потоками;
- ***телекомунікаційні технології;***
- ***системи засобів масової інформації***.

Інформаційний кадастр – сукупність відомостей, необхідних для прийняття рішення органом керування. Інформаційний кадастр може мати вигляд двомірної матриці, стовпці якої відповідають тематичним розділам кадастру, а рядки – їхнім характеристикам.

Інформаційна кооперація – форма забезпечення інформаційної безпеки між рівноправними суб'єктами інформаційного процесу (фізичними, юридичними, міжнародними), що включає сукупність їхніх взаємоузгоджених дій, спрямованих на одержання відомостей про дестабілізуючі фактори, дестабілізуючі та інформаційні загрози й захист від них доступними законними способами й засобами.

Під **інформаційним ударом** розуміють короткочасний потужний узгоджений інформаційний вплив сил і засобів на найбільш важливий елемент (елементи) системи управління (керування) противника для досягнення рішучих цілей із завоювання інформаційної переваги (зниження інформаційної переваги противника).

Інформаційна операція (від лат. operatio – «дія») – це сукупність узгоджених за метою, завданнями, місцем і часом дій (акцій), ударів і битв, що проводяться за єдиним задумом і планом для вирішення завдань інформаційної боротьби (завоювання й утримання інформаційної переваги над противником або зниження його інформаційної переваги) на театрі воєнних дій, стратегічному або оперативному напрямах.

Інформаційний патронат (захисник) є формою забезпечення інформаційної безпеки фізичних і юридичних осіб із боку держави. Він припускає забезпечення органів управління системи інформаційної безпеки держави відомостями про дестабілізуючі фактори й загрози стану поінформованості фізичних і юридичних осіб (інформаційне забезпечення інформаційної безпеки) та власне захист життєво важливих інтересів цих осіб від інформаційних загроз, або, як ще кажуть, інформаційний захист.

Інформаційне протиборство, яке характеризується, з однієї сторони, впливом на системи добування, оброблення, розповсюдження та зберігання інформації противника, а з іншої — застосуванням заходів захисту своїх подібних систем від деструктивного та керуючого впливу.

Інформаційна перевага розуміють ситуацію, що надає можливість змінити уявлення противника про дійсну обстановку й позбавити його здатності прогнозувати подальші події та впливати на них.

Інформаційне поле:

1) сукупність енергетичних субстанцій окремих об'єктів, які є елементами інформаційного поля Землі та Всесвіту;

2) просторово-часові вібрації (інформаційно-розпорядницькі структури), що містять відомості про минуле, сьогодення і майбутнє Всесвіту.

Інформаційна політика держави – це головні напрями й предмет діяльності держави в галузі інформації.

Інформаційний продукт (продукція):

1) документована інформація, яка підготовлена і призначена для задоволення потреб користувачів;

2) документована інформація, яку підготовлено відповідно до потреб користувачів і яка призначена для задоволення потреб користувачів;

3) створена виробником сукупність документованої інформації, відомостей, даних і знань, яка призначена для забезпечення інформаційних потреб користувача.

Інформаційний простір (національний):

1) інформаційне середовище, в якому здійснюються інформаційні процеси та інформаційні відносини щодо створення, збирання, відображення, реєстрації, накопичення, збереження, захисту та поширення інформації, інформаційних продуктів і ресурсів, на яке поширюється юрисдикція держави;

2) сукупність національних інформаційних ресурсів та інформаційної інфраструктури, які дозволяють на основі єдиних принципів і загальних правил забезпечувати інформаційну взаємодію громадян, суспільства і держави з їх рівним правом доступу до відкритих інформаційних ресурсів та максимально повним задоволенням інформаційних потреб суб'єктів держави на всій її території з додержанням балансу інтересів на входження у світовий інформаційний простір і забезпечення інформаційної безпеки відповідно до Конституції України та міжнародних правових норм.

Інформаційні ресурси:

1) сукупність документів у інформаційних системах (бібліотеках, архівах, банках даних тощо);

2) організована сукупність інформаційних продуктів певного призначення, що необхідні для забезпечення інформаційних потреб громадян, суспільства, держави в певній сфері життя чи діяльності.

Інформаційне рішення – це одиничний акт сприйняття органом керування поточної інформації про ситуацію та її віднесення до будь-якої відомості інформаційного кадастру.

Інформаційний ринок: система економічних, організаційних і правових відносин щодо продажу і купівлі інформаційних ресурсів, технологій, продукції та послуг.

Інформаційне середовище: усталене поєднання окремих суб'єктів національного інформаційного простору України, інформаційної інфраструктури та інформаційних ресурсів, що взаємодіють в інформаційних процесах.

Інформаційна система: організаційно впорядкована сукупність інформаційних ресурсів та інформаційних технологій і засобів забезпечення інформаційних процесів.

Інформаційна сфера – сфера діяльності суб'єктів, пов'язана зі створенням, перетворенням і споживанням інформації.

Інформаційний суверенітет – здатність держави контролювати й регулювати потоки інформації поза межами держави з метою дотримання законів України, прав і свобод громадян, забезпечення національної безпеки держави.

Інформаційне суспільство:

1) суспільство, в якому більшість робітників займаються створенням, збиранням, відображенням, реєстрацією, накопиченням, збереженням і поширенням інформації, особливо її вищої форми – знань;

2) суспільство, в якому діяльність людей ґрунтується на використанні послуг, що надаються за допомогою інформаційних технологій і технологій зв'язку.

Інтереси суспільства в інформаційній сфері полягають у:

- забезпеченні інтересів особистості в цій сфері;
- зміцненні демократії;
- створенні правової соціальної держави;
- досягненні й підтримці суспільної злагоди;
- у духовному відновленні України.

Інформаційні технології:

1) цілеспрямована організована сукупність інформаційних процесів із використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування;

2) цілеспрямовано організована сукупність інформаційних процесів для створення і використання інформаційних продуктів або надання інформаційних послуг;

3) технологічний процес, предметом перероблення й результатом якого є інформація;

4) процес матеріалізації знань у продукцію і послуги за допомогою комп'ютерно-телекомунікаційних систем;

5) система методів і способів використання комп'ютерної техніки та систем зв'язку для створення, пошуку, одержання, відображення, реєстрації, накопичення, збереження, захисту й поширення інформаційних продуктів.

Інформування – акт передавання органу керування певної поточної інформації.

Ефективність інформаційної боротьби виражається ступенем реалізації мети інформаційної боротьби.

Категорії інформаційної боротьби являють собою фундаментальні поняття, що відображають найбільш загальні, суттєві предмети, процеси і властивості інформаційної боротьби.

Комбіновані способи інформаційної боротьби забезпечують досягнення інформаційної переваги як за кількістю, так і за якістю інформації.

Комерційна таємниця – відомості, що не є державними секретами, пов'язані з виробництвом, технологіями, фінансами, процесами управління та іншою діяльністю організацій або фірм, розголошування яких може завдати шкоди їхнім інтересам.

Концепція слугує юридичним актом, що містить керівні принципи та цільові настанови щодо шляхів, засобів та методів захисту життєво важливих інтересів людини, групи, суспільства та держави.

Концепція інформаційної безпеки держави – це систематизована сукупність відомостей про інформаційну безпеку держави та шляхи її забезпечення.

Концепція інформаційної війни – система поглядів на інформаційну війну та шляхи її ведення.

Критерій ефективності інформаційної боротьби – це кількісна міра відображення ступеня інформаційної переваги однієї з протиборчих сторін. Визначається співвідношенням інформованості протиборчих сторін.

Ліцензія (від лат. licentia – «свобода, право») – це дозвіл, виданий державою на проведення деяких видів господарської діяльності, включаючи зовнішньоторговельні операції (ввезення та вивезення) та надання права використовувати захищені патентами винаходи, технології, методики. Ліцензійні дозволи надаються на певний час і на певні види товарів.

Матеріальні носії секретної інформації – матеріальні об'єкти, у тому числі фізичні поля, в яких відомості, що становлять державну таємницю, відображені у вигляді текстів, знаків, символів, образів, сигналів, технічних рішень, процесів тощо.

Мета інформаційної боротьби – забезпечення необхідного ступеня власної інформаційної безпеки й максимальне зменшення рівня інформаційної безпеки конфронтуючої сторони. Досягнення мети інформаційної боротьби здійснюється шляхом вирішення багатьох завдань, основними з яких є ураження об'єктів інформаційної сфери конфронтуючої сторони і захист власної інформації.

Метод оцінки ефективності інформаційної боротьби – це сукупність способів, прийомів визначення кількісних значень показників інформованості протидіючих сторін та розрахунку ступеня інформаційної переваги однієї з них над іншою відповідно до мети інформаційної боротьби. В основу методу може бути покладене математичне моделювання процесу забезпечення інформацією органів управління протидіючих сторін.

Міждержавні дестабілізуючі фактори – це конфлікти різноманітних масштабів і проявів (в економіці, політиці, ідеології, дипломатії тощо).

Напрями забезпечення безпеки інформації – це нормативно-правові категорії, орієнтовані на забезпечення комплексного захисту інформації від внутрішніх та зовнішніх загроз на державному рівні, на рівні підприємства або організації, на рівні окремої особи.

Наступальна інформаційна операція має за мету завоювання інформаційної переваги над противником. У цій операції головні зусилля спрямовуються на дезорганізацію його систем управління військами і зброєю, а частина сил та засобів забезпечують стійкість власного управління. При цьому всі заходи, які проводяться в межах інформаційної боротьби, повинні забезпечувати сприятливі умови для бойових дій своїх військ (сил).

Наступальні способи інформаційної боротьби реалізують блокування інформації, відвернення уваги, сковування сил противника, вимотування противника, інсценування, дезінтеграцію, замирення, залякування противника, провокування противника, перевантаження противника, навіювання на противника і тиск на противника

Національна безпека – категорія політичної науки (політології), що характеризує стан соціальних інститутів, що забезпечує їхню ефективну діяльність для підтримки оптимальних умов існування особистості, суспільства та держави. Вона відображає зв'язок безпеки з нацією.

Національний інформаційний простір – інформаційне середовище, в якому здійснюються інформаційні процеси та інформаційні відносини щодо створення, збирання, відображення, реєстрація, накопичення, збереження, захист і поширення інформації, інформаційних продуктів та інформаційних ресурсів, на яке розповсюджується юрисдикція держави.

Національні інтереси держави відображають фундаментальні цінності та прагнення народу, його потреби в гідних умовах життєдіяльності, а також цивілізовані шляхи їх створення й способи задоволення. Національні інтереси держави та їхня пріоритетність обумовлюються конкретною ситуацією, що складається в країні та за її межами.

Нація – стійка історична спільність людей, що визначається соціальними зв'язками певної формації і характеризується специфічними етнічними рисами, зумовленими особливостями економічного й культурного розвитку, спільністю території, мови, побуту, традицій і звичаїв, а також відображенням цих факторів у суспільній свідомості та суспільній психології.

Оборонна інформаційна операція проводиться в умовах великої інформаційної переваги противника і має за мету зниження цієї переваги. У такій операції головні зусилля сил і засобів спрямовуються на забезпечення інформаційної безпеки органів управління об'єднань і з'єднань, на захист інформації в системах керування. Частина сил і засобів спрямовуються на дезорганізацію управління військами і зброєю противника.

Оборонні способи інформаційної боротьби реалізують деблокування та ототожнення інформації.

Оперативна безпека – це комплекс заходів із виявлення критичної інформації, проведення аналізу дій своїх збройних сил.

Особистість – людина як суб'єкт відносин і свідомої діяльності. До життєво важливих інтересів особистості належать, насамперед права і свободи людини й громадянина, зокрема інформаційні.

Оцінка ефективності інформаційної боротьби – це визначення ступеня відповідності результатів інформаційної боротьби її меті (цілі).

Пасивне забезпечення інформаційної безпеки передбачає реагування на вже наявні загрози, спрямоване на безпосередню протидію акціям, що є деструктивними щодо соціальної системи.

Поінформованість особистості (суспільства та держави) – задоволення в будьякій мірі потреб в інформації, що призводить до оволодіння відомостями про навколишній світ та процеси, що відбуваються у ньому.

Правильне інформування – це передавання органу керування неспотвореної інформації про істинну ситуацію.

Правильне дезінформування – це передавання органу керування неспотвореної інформації про неправдиву ситуацію.

Правовий захист інформації як ресурсу признаний на міждержавному, державному рівні та визначається міждержавними договорами, конвенціями, деклараціями та реалізується патентами, авторським правом та ліцензіями на їхній захист. На державному рівні правовий захист регулюється державними та відомчими актами.

Принципи інформаційної боротьби – це науково обґрунтовані положення, правила, рекомендації з підготовки і ведення інформаційної боротьби, керівництва її силами й засобами. Вони створюються на основі законів і закономірностей, а також досвіду, набутого в результаті практичної діяльності в галузі інформаційної боротьби. Принципи інформаційної боротьби не тільки відображають об'єктивну сутність, але і приписують, як слід діяти в конкретних умовах. Зміст і масштаби завдань інформаційної боротьби передбачають наявність цілої множини принципів інформаційної боротьби.

Радіоелектронна атака передбачає активний вплив на радіоелектронні засоби противника. За видом впливу атаки поділяється на два компоненти:

- неруйнівні впливи, які включають електронне придушення й електронну дезінформацію;
- руйнівні впливи на основі застосування протирадіолокаційних ракет, зброї спрямованої енергії (лазерної, надвисокочастотної) і т. ін.

Радіоелектронний захист – це сукупність заходів забезпечення стійкої роботи засобів управління й розвідки в умовах ведення противником радіоелектронної боротьби, застосування розвідувально-ударних комплексів, самонавідної зброї та усунення взаємного впливу радіоелектронних засобів.

Радіоелектронне забезпечення передбачає проведення заходів пошуку, перехоплення випромінювання в електромагнітному спектрі та визначення місцеположення джерел випромінювання для оцінки ступеню можливої загрози і прийняття рішення командирами всіх рангів, а також виконання додаткових функцій, таких як ухилення від загрози з боку противника і високоточна цілевказівка системам озброєння.

Радіоелектронна контрпротидія являє собою сукупність заходів, спрямованих на підвищення живучості та зменшення втрат своїх сил і засобів від впливу керованої зброї і засобів радіоелектронної протидії противника.

Силові способи інформаційної боротьби засновані на ураженні об'єктів інформаційної боротьби різноманітними видами зброї (звичайної, радіоелектронної, інформаційної). Застосування силових способів дозволяє досягти інформаційної переваги в кількості інформації, необхідної для вирішення завдань управління військами (силами).

Система забезпечення національної безпеки – організована державою сукупність суб'єктів: державних органів, громадських організацій, посадових осіб та окремих громадян, об'єднаних цілями та завданнями щодо захисту національних інтересів, що здійснюють узгоджену діяльність у межах законодавства держави.

Система захисту державної таємниці – сукупність органів захисту державної таємниці, використовуваних ними засобів і методів захисту відомостей, що становлять державну таємницю та їх носіїв, а також заходів, що проводяться з цією метою.

Спосіб блокування інформації полягає в тому, що на етапі підготовки й у ході бойових дій шляхом виконання комплексу заходів інформаційної протидії повністю або частково припиняється добування (збирання) інформації про ситуацію й обмін інформацією в системах управління військами і зброєю противника. Для реалізації цього способу застосовується вогневе, радіоелектронне й інформаційне ураження (придушення) елементів систем управління військами (силами) і зброєю противника.

Спосіб відвернення уваги полягає в тому, що на етапі підготовки бойових дій шляхом проведення комплексу заходів інформаційної протидії намагаються створити реальну або удавану загрозу для одного з найбільш уразливих місць противника і тим самим переконати його у своїх намірах діяти на одному з можливих напрямів з метою відволікти головні сили противника на вирішення другорядних завдань.

Спосіб вимотування противника полягає в проведенні комплексу заходів інформаційної протидії з метою примусити противника здійснювати невигідні й марні дії і, як наслідок, вступити в бій із розтраченими ресурсами та зниженою боєздатністю. При цьому можуть проводитися обмежені бойові або відволікаючі дії.

Спосіб деблокування інформації передбачає проведення комплексу заходів інформаційного захисту з метою одержання інформації, яка приховується або модифікується противником. При цьому можуть застосовуватися всі можливі методи, сили і засоби, аж до проведення широкомасштабних операцій.

Спосіб дезінтеграції використовується для вирішення політичних завдань у міждержавних конфліктах. Реалізація способу полягає в проведенні комплексу заходів інформаційної протидії, що дозволяє нав'язати противникові уяву про необхідність діяти всупереч коаліційним інтересам. З цією метою може використовуватися дезінформування громадської думки, а також формування фальшивих уявлень про воєнно-політичну ситуацію у голів держав, що беруть участь у конфлікті. Крім того, можуть проводитися заходи, які сприяють загостренню реально наявних або штучно створюваних суперечностей у стані ворога з метою зменшити його воєнну й економічну могутність.

Спосіб замирення застосовується для нав'язування противникові уяви про нейтральну або союзницьку позицію конфронтуючої сторони. Суть способу полягає у проведенні комплексу заходів інформаційної протидії, основною метою яких є створення у противника уяви про те, що здійснюється не підготовка до бойових дій, а планова оперативна (бойова підготовка) або будь-які інші заходи. Противник повинен упевнитися в дружніх або мирних намірах конфронтуючої сторони і втратити пильність. Таємно ж планується і готується напад на нього при першому зручному випадку.

Спосіб інсценування полягає в тому, що на етапі підготовки до бойових дій противникові нав'язується уява про наявність удаваної загрози для одного з його уразливих місць, запобігання якій не потребує виділення сил та засобів. Це робиться з метою, щоб противник помітив обман і його пильність була б приспана. Якщо виникає справжня загроза, він також сприйме її як фальшиву і зможе діяти відповідно до реальної ситуації.

Спосіб навіювання на противника полягає у формуванні й наступному використанні інформаційного стереотипу конфронтуючої сторони. Для цього на етапі підготовки й у ході бойових дій шляхом проведення комплексу заходів інформаційної протидії до відома противника доводиться інформація, яка має юридичну, моральну, ідеологічну або іншу силу і спонукає його до здійснення будьяких дій, вигідних конфронтуючій стороні.

Спосіб ототожнення інформації передбачає проведення комплексу заходів інформаційного захисту, які забезпечують збирання і зіставлення інформації про один і той же факт (явище) від різноманітних джерел, що дозволяє виявити і блокувати дезінформацію, яка розповсюджується противником.

Спосіб провокування противника призначений для спонукання противника до здійснення будь-яких дій, корисних протилежній стороні. Спосіб перевантаження противника полягає в тому, щоб на етапі підготовки й у ході бойових дій довести до противника таку кількість суперечливої інформації, яка перевантажує його систему управління, і змушує приймати й реалізовувати рішення в умовах підвищеної невизначеності ситуації.

Спосіб сковування сил противника є різновидом способу відвернення уваги. При його застосуванні у противника створюється переконання в наявності загрози для одного з уразливих місць, запобігання якій потребує виділення частини сил.

Спосіб тиску на противника заснований на доведенні до суспільної думки відомостей, які ганьблять противника, та змушують державні, міждержавні, суспільні та інші організації здійснювати дії, які ускладнюють виконання його задумів.

Сприйняття інформації – процес формування в органі керування уявлення про ситуацію, включаючи її кількісні та якісні параметри. Найбільш суттєві характеристики при цьому – розпізнавальні ознаки істинних і неправдивих елементів ситуації.

Ступінь секретності – категорія, що характеризує важливість такої інформації, можливі збитки внаслідок її розголошування, ступінь обмеження доступу до неї та рівень її

охорони державою. Критерій визначення ступеня секретності інформації встановлює відповідний державний орган.

Суспільство – сукупність форм сумісної діяльності людей, що утворилися в процесі історичного розвитку. Життєво важливі інтереси суспільства зв'язані зі створенням і розвитком вільного, гуманного, високоосвіченого, гармонійного суспільства, заснованого на принципах демократи, бережливого ставлення до своїх традицій і національного надбання, суспільства, що підтримує і всіляко охороняє основний свій осередок – сім'ю.

Теорія інформаційної боротьби являє собою систему знань про характер, закони, закономірності, принципи, форми, способи підготовки і ведення інформаційної боротьби.

Теорія національної безпеки – наука, що поєднує у собі прикладні аспекти соціальних, воєнних, гуманітарних, технічних, психологічних, біологічних та інших наук із метою дослідження суті, змісту, методів, форм і засобів забезпечення безпеки особистості, суспільства та держави.

Тероризм – загроза або використання насильства в політичних цілях окремими особами або групами, що можуть діяти як на боці, так і проти існуючого уряду, коли такі дії, спрямовані на те, щоб уплинути на більше число людей, ніж безпосередні жертви.

Трансінформування – це передавання органу керування трансінформації (інформація про істинну ситуацію, трансформована в інформацію про неправдиву ситуацію).

Трансдезінформування – це передавання органу керування трансдезінформації (інформація про неправдиву ситуацію, перетворена в інформацію про правдиву ситуацію).