МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА»
Навчально-науковий інститут електронних та інформаційних технологій
Кафедра кібербезпеки та математичного моделювання

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ

МЕТОДИЧНІ ВКАЗІВКИ

до практичних занять
для здобувачів першого (бакалаврського) рівня вищої освіти
спеціальності 262 – Правоохоронна діяльність

Обговорено і рекомендовано
на засіданні кафедри кібербезпеки
та математичного моделювання
протокол № 5
від 16.11.2020р.

Чернігів – 2020

Інформаційна безпека держави. Методичні вказівки до практичних занять для здобувачів першого (бакалаврського) рівня вищої освіти спеціальності 262 – Правоохоронна діяльність // Укл.: Ю.М.Ткач, С.М.Семендяй – Чернігів: НУ «Чернігівська політехніка», 2020. – 112 с.

Укладачі: Ткач Юлія Миколаївна
доктор педагогічних наук, завідувач кафедри кібербезпеки та математичного моделювання, доцент

Семендяй Сергій Матвійович
викладач кафедри кібербезпеки та математичного моделювання

Відповідальний за випуск: Ткач Юлія Миколаївна
доктор педагогічних наук, завідувач кафедри кібербезпеки та математичного моделювання, доцент

Рецензент: Мехед Дмитро Борисович
кандидат педагогічних наук, доцент кафедри кібербезпеки та математичного моделювання, доцент

Вказівки підготовлено відповідно до навчального плану підготовки бакалаврів спеціальності 262 – Правоохоронна діяльність. Методичні рекомендації містять загальні положення щодо організації підготовки практичних занять, теоретичний матеріал та завдання на роботу. Є керівним документом для здобувачів вищої освіти освітнього ступеню «бакалавр», спеціальності 262 – Правоохоронна діяльність.

ЗМІСТ

ВСТУП

Практичне заняття – це вид навчального заняття, передбачений навчальним планом освітньо-кваліфікаційного рівня «бакалавр» спеціальності 262 – «Правоохоронна діяльність», на якому викладач організує детальний розгляд студентами окремих теоретичних положень навчальної дисципліни «Інформаційна безпека держави» та формує вміння і навички їх практичного застосування шляхом індивідуального виконання студентами відповідно сформульованих завдань.

Практичні заняття проводяться в аудиторіях або в навчальних лабораторіях, оснащених необхідними технічними засобами навчання, комп’ютерною технікою.

Перелік тем практичних занять визначається робочою навчальною програмою дисципліни. Проведення практичного заняття починається з опитування студентів (за допомогою попередньо підготовлених контрольних питань, наведених у кінці кожної практичної роботи) для виявлення ступеня оволодіння ними необхідними теоретичними положеннями, і грунтується на наборі завдань різної складності для розв'язування їх студентами під час занять.

Практичне заняття № 1

2 години

Тема заняття: Небезпеки для інформаційної безпеки держави, суспільства та особи.

Мета заняття: ознайомитися із загрозами для інформаційної безпеки держави, суспільства та особи.

Теоретичні відомості

Загрози інформаційній безпеці – сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства і держави в інформаційній сфері. Основні загрози інформаційній безпеці можна розділити на три групи:

– загрози впливу неякісної інформації (недостовірної, фальшивої, дезінформації) на особистість, суспільство, державу;

– загрози несанкціонованого і неправомірного впливу сторонніх осіб на інформацію і інформаційні ресурси (на виробництво інформації, інформаційні ресурси, на системи їхнього формування і використання);

– загрози інформаційним правам і свободам особистості (праву на виробництво, розповсюдження, пошук, одержання, передавання і використання інформації; праву на інтелектуальну власність на інформацію і речову власність на документовану інформацію; праву на захист честі і гідності і т.ін.).

Аналіз і виявлення загроз інформаційної безпеки є важливою функцією забезпечення інформаційної безпеки. Багато в чому вигляд розроблюваної системи захисту і склад механізмів її реалізації визначається потенційними загрозами, виявленими на цьому етапі. Наприклад, якщо користувачі мають доступ в Інтернет, то кількість загроз інформаційній безпеці різко зростає, відповідно, це відбивається на методах і засобах захисту і т. д.

Загроза інформаційній безпеці - це потенційна можливість порушення режиму інформаційної безпеки. Навмисна реалізація загрози називається атакою на інформаційну систему. Особи, які навмисно реалізують загрози, є зловмисниками.

Найчастіше загроза є наслідком наявності вразливих місць в захисті інформаційних систем, наприклад, неконтрольований доступ до персональних комп'ютерів або неліцензійне програмне забезпечення (на жаль навіть ліцензійне програмне забезпечення не позбавлене уразливостей).

Історія розвитку інформаційного середовища показує, що нові вразливі місця з'являються постійно. З такою ж регулярністю, але з невеликим відставанням, з'являються і засоби захисту. В більшості своїй засоби захисту з'являються у відповідь на виникаючі загрози, так, наприклад, постійно з'являються виправлення до програмного забезпечення фірми Microsoft, що усувають чергові його вразливі місця. Такий підхід до забезпечення безпеки малоефективний, оскільки завжди існує проміжок часу між моментом виявлення загрози та її усуненням. Саме в цей проміжок часу зловмисник може завдати непоправної шкоди інформації.

У цьому зв'язку більш прийнятним є інший спосіб - спосіб попереджувального захисту, що полягає в розробці механізмів захисту від можливих, передбачуваних і потенційних загроз. Але деякі загрози не можна вважати наслідком цілеспрямованих дій шкідливого характеру. Існують загрози, викликані випадковими помилками або

техногенними явищами.

Знання можливих загроз інформаційній безпеці, а також вразливих місць системи захисту, необхідне для того, щоб вибрати найбільш економічні і ефективні засоби забезпечення інформаційної безпеки.

Види загроз інформаційній безпеці

За ступенем гіпотетичної шкоди: загроза - явні чи потенційні дії, які ускладнюють або унеможливлюють реалізацію національних інтересів в інформаційній сфері та створюють небезпеку для системи державного управління, життєзабезпечення її системоутворюючих елементів; небезпека - безпосередня дестабілізація функціонування системи державного управління.

За повторюваністю вчинення: повторювані - такі загрози, які раніше вже мали місце; продовжувані - неодноразове здійснення загроз, що складається з ряду тотожних, які мають спільну мету.

За сферами походження: екзогенні - джерело дестабілізації системи лежить поза її межами; ендогенні - алгоритм дестабілізації системи перебуває у самій системі.

За ймовірністю реалізації: імовірні - такі загрози, які за виконання певного комплексу умов обов'язково відбудуться. Прикладом може слугувати оголошення атаки інформаційних ресурсів суб'єкта забезпечення національної безпеки, яке передує самій атаці; неможливі - такі загрози, які за виконання певного комплексу умов ніколи не відбудуться. Такі загрози зазвичай мають більше декларативний характер, не підкріплений реальною і, навіть, потенційною можливістю здійснити проголошені наміри, вони здебільшого мають залякуючий характер; випадкові - такі загрози, які за виконання певного комплексу умов кожного разу протікають по-різному. Загрози даного рівня доцільно аналізувати за допомогою методів дослідження операцій, зокрема теорії ймовірностей і теорії ігор, які вивчають закономірності у випадкових явищах.

За джерелами походження: природного походження - включають в себе небезпечні геологічні, метеорологічні, гідрологічні морські та прісноводні явища, деградацію ґрунтів чи надр, природні пожежі, масове ураження сільськогосподарських рослин і тварин хворобами чи шкідниками, зміна стану водних ресурсів і біосфери тощо; техногенного походження - транспортні аварії (катастрофи), пожежі, неспровоковані вибухи чи їх загроза, раптове руйнування каналів зв'язку, аварії на інженерних мережах і спорудах життєзабезпечення, аварії головних серверів органів державного управління тощо; антропогенного походження - вчинення людиною різноманітних дій з руйнування інформаційних систем, ресурсів, програмного забезпечення об'єкта тощо. До цієї групи за змістом дій належать: ненавмисні, викликані помилковими чи ненавмисними діями людини (це, наприклад, може бути помилковий запуск програми, ненавмисне інсталяція закладок тощо); навмисні (інспіровані), що стали результатом навмисних дій людей (наприклад: навмисна інсталяція програм, які передають інформацію на інші комп'ютери, навмисне введення вірусів тощо).

За значенням: допустимі - такі загрози, які не можуть призвести до колапсу системи. Прикладом можуть слугувати віруси, які не пошкоджують програми шляхом їх знищення; недопустимі - такі загрози, які: 1) можуть у разі їх реалізації

призвести до колапсу і системної дестабілізації системи; 2) можуть призвести до змін, не сумісних із подальшим існуванням системи.

За структурою впливу: системні - загрози, що впливають одразу на всі складові елементи суб'єкта ЗНБ; структурні - загрози, що впливають на окремі структури системи. Дані загрози є також небезпечними, водночас вони стосуються структури окремих органів державної влади або їх компонентів; елементні - загрози, що впливають на окремі елементи структури системи. Дані загрози носять постійний характер і можуть бути небезпечними лише за умови неефективності або не проведення їх моніторингу.

За характером реалізації: реальні - активізація алгоритмів дестабілізації є неминучою і не обмежена часовим інтервалом і просторовою дією; потенційні - активізація алгоритмів дестабілізації можлива за певних умов середовища функціонування органу державного управління; здійснені - такі загрози, які втілені у життя; уявні - псевдоактивізація алгоритмів дестабілізації, або ж активізація таких алгоритмів, що за деякими ознаками схожі з алгоритмами дестабілізації, але такими не є.

За ставленням до них: об'єктивні - такі загрози, які підтверджуються сукупністю обставин і фактів, що об'єктивно характеризують навколишнє середовище. При цьому ставлення до них суб'єкта управління не відіграє вирішальної ролі через те, що об'єктивні загрози існують незалежно від волі та свідомості суб'єкта; суб'єктивні - така сукупність чинників об'єктивної дійсності, яка вважається суб'єктом управління системою безпеки загрозою.

За об'єктом впливу: на державу; на людину; на суспільство.

Крім того, загрози можуть мати або об'єктивну природу, наприклад, зміна умов фізичного середовища (пожежі, повені і т.п.) чи відмовлення елементів обчислювальної системи, або суб'єктивну, наприклад, помилки персоналу. Загрози, що мають суб'єктивну природу, можуть бути випадковими або навмисними.

Отже, на будь-якому об'єкті повинні здійснюватися деякі дії чи фактори, що будуть перешкоджати реалізації конкретних захисних механізмів і заходів, створюючи тим самим відзначені вище загрози. При цьому вони будуть безпосередньо пов'язані з цими загрозами і будуть, власне кажучи, їхніми причинами. Ці події чи фактори можна охарактеризувати в такий спосіб:

– вони об'єктивно існують і можуть реалізуватися в будь-який момент часу на будь-якому об'єкті, де обробляється інформація, що підлягає захисту;

– вони не зводяться до загроз; один і той самий процес чи подія в одному випадку призводить до загроз, а в іншому не являє собою ніякої небезпеки для інформації;

– для кожного такого фактора існує можливість явно установити, з якими видами загроз він пов'язаний;

– виникає можливість здійснювати конкретні дії по протидії загрозам.

Таким чином, виявляється, що загрози виникають внаслідок здійснення цих факторів, тобто є їх результатом. Надалі ці фактори будемо називати дестабілізуючими факторами (ДФ). Як показує подальший аналіз, введення поняття ДФ цілком логічно виправдане і дозволяє одержати дуже просту, зрозумілу і наочну схему для створення моделі загроз.

Дестабілізуючі фактори загроз

Дестабілізуючі фактори - явища та процеси природного і штучного походження, що породжують інформаційні загрози.

Джерелами дестабілізуючих факторів можуть бути як окремі особи, так і організації та їхні об'єднання. До найбільш сильних із них відносяться ворожі держави або коаліції ворожих держав, в яких для формування інформаційних загроз створюються і функціонують спеціальні органи і служби.

Особливу групу джерел складають інформаційні системи і засоби, оскільки вони одночасно є знаряддям приведення в дію інформаційних загроз, каналом їхнього проникнення у свідомість особистості або суспільну свідомість і генератором спонтанних загроз, що виникають внаслідок технічних несправностей і інших причин.

Джерелом дестабілізуючих факторів може бути також природне середовище. Кожному джерелу властиві певні види дестабілізуючих факторів, які можна представити двома групами: міждержавні дестабілізуючі фактори і внутрішньодержавні дестабілізуючі фактори.

Сукупність джерел разом із властивими їм видами дестабілізуючих факторів формують цілий спектр інформаційних загроз, що впливають на стан інформованості особистості, суспільства і держави. До них відносяться: викрадення, знищення, втрата, приховування, спотворення, розголошення, фальсифікація, компрометація корисної (істинної) інформації, а також фабрикування, розповсюдження і впровадження дезінформації.

До внутрішньодержавних дестабілізуючих факторів відносять:

– правовий вакуум у більшості питань забезпечення інформаційної безпеки;

– навмисне або ненавмисне порушення законодавства з питань інформаційної безпеки;

– політичні конфлікти;

– зловмисні дії злочинних елементів або груп;

– відмови, збої, технічні помилки інформаційних систем (засобів);

– природні явища (процеси), що ускладнюють одержання, передачу, прийом і зберігання інформації або руйнують інформаційні системи.

Міждержавні дестабілізуючі фактори - це конфлікти різноманітних масштабів і проявів (в економіці, політиці, ідеології, дипломатії і т.ін.).

Фактори загроз інформаційній безпеці

Фактори загроз за видовою ознакою поділяються на політичні, економічні та організаційно-технічні**.**

Під політичними факторами загроз інформаційній безпеці розуміють:

– зміни геополітичної обстановки внаслідок фундаментальних змін у різноманітних регіонах світу, зведення до мінімуму ймовірності світової ядерної війни;

– інформаційна експансія розвинених країн, які здійснюють глобальний моніторинг світових політичних, економічних, воєнних, екологічних та інших процесів, та розповсюджують інформацію з метою здобуття односторонніх переваг;

– становлення нової державності в пострадянських країнах на основі принципів демократії, законності, інформаційної відкритості;

– знищення колишньої командно-адміністративної системи державного управління, а також системи забезпечення безпеки;

– порушення інформаційних зв'язків внаслідок утворення на території колишнього СРСР нових держав;

– прагнення пострадянських країн до більш тісного співробітництва із закордонними країнами в процесі проведення реформ на основі максимальної відкритості сторін;

– низька загальна правова та інформаційна культура сторін.

Основними економічними факторами загроз безпеці інформації є:

– перехід на ринкові відносини в економіці, поява на ринку великої кількості вітчизняних та зарубіжних комерційних структур - виробників та споживачів інформації, засобів інформатизації та захисту інформації, включення інформаційної продукції в систему товарних відносин;

– критичний стан вітчизняних галузей промисловості, яка виробляє засоби інформатизації та захисту інформації;

– розширення кооперації із зарубіжними країнами в розвитку інформаційної інфраструктури.

Основними організаційно-технічними факторами загроз інформаційній безпеці є:

– недостатня нормативно-правова база у сфері інформаційних відносин, у тому числі в галузі забезпечення інформаційної безпеки;

– недостатнє регулювання державою процесів функціонування та розвитку ринку засобів інформатизації, інформаційних продуктів та послуг;

– широке використання у сфері державного управління та кредитно-фінансової сфери незахищених від витоку інформації імпортних технічних та програмних засобів для зберігання, обробки та передавання інформації;

– зростання обсягів інформації, яка передається відкритими каналами зв'язку;

– загострення криміногенної обстановки, зростання числа комп'ютерних злочинів, особливо в кредитно-фінансовій сфері.

Джерела загроз інформаційній безпеці

Виходячи з визначення загроз інформаційній безпеці, можна виділити декілька основних джерел загроз, які можуть торкатися інтересів особистості, суспільства і держави.

Джерела загроз інформаційній безпеці особистості.

Інтереси особистості, які необхідно охороняти в інформаційному суспільстві, полягають насамперед у реальному забезпеченні конституційних прав і свобод людини і громадянина на доступ до відкритої інформації, на використання інформації в інтересах здійснення не забороненої законом діяльності, а також у захисту інформації, що забезпечує особисту безпеку, духовний та інтелектуальний розвиток.

Найбільш небезпечним джерелом загроз цим інтересам вважається суттєве розширення можливості маніпулювання свідомістю людини за рахунок формування навкруг неї індивідуального «віртуального інформаційного простору», а також можливість використання технологій впливу на її психічну діяльність.

Важливою особливістю способу життя людини в інформаційному суспільстві є

суттєве скорочення «інформаційних» відстаней (часу доступу до необхідної інформації), що веде до появи нових можливостей - як з формування особистості, та і з реалізації її потенціалу. Людство впритул підходить до рубежів, за якими інформаційна інфраструктура стає, по суті, основним джерелом інформації для людини, здійснює безпосередній вплив на її психічну діяльність, на формування її соціальної поведінки.

Проблема формування розумових потреб і мотивації соціальної поведінки поки не має загального вирішення навіть для індустріального суспільства і ще більше ускладнюється стосовно інформаційного суспільства. Вона є однією з найбільш складних у сучасній психологічній науці.

В цілому структура споживчо-мотиваційної сфери особистості утворюється базовими потребами, зумовленими його генотипом (у їжі, особистій безпеці, потреба у продовженні роду, довголітті, а також потребами у спілкуванні з іншими людьми), похідними потребами, що формуються діючою системою виховання. Способи і форми задоволення цих потреб у значній мірі залежать від інформації і знань, що одержуються з навколишнього світу і, зокрема, надходять через інформаційну інфраструктуру. Спрямованість використання одержаної інформації і результати, що одержуються, визначаються, насамперед, особою людини та її духовним потенціалом.

Складність процедур, що реалізуються в сучасних технологіях доступу до необхідних інформаційних ресурсів, критично збільшують залежність окремої людини від інших людей, які здійснюють розробку інформаційних технологій, визначення алгоритмів пошуку необхідної інформації, її попередньої обробки, приведення до виду, зручного для сприйняття, доведення до споживача. По суті, ці люди формують для людини інформаційний фон його життя, визначають умови, в яких він живе і діє, вирішує свої життєві проблеми. Саме тому вважається виключно важливим забезпечити безпеку взаємодії людини з інформаційною структурою.

Іншим небезпечним джерелом загроз інтересам особистості є використання на шкоду її інтересам персональних даних, що нагромаджуються різноманітними структурами, в тому числі органами державної влади, а також розширення можливості прихованого збирання інформації, що складає його особисту і сімейну таємницю, відомості про її приватне життя.

Це зумовлено, у першу чергу, труднощами реалізації механізмів охорони цих відомостей, подальшими досягненнями у мікромініатюризації засобів прихованого збирання і передавання інформації.

Джерела загроз інформаційній безпеці суспільства.

Інтереси суспільства, що вступило у стадію постіндустріального розвитку, полягають у захисті життєво важливих інтересів у цій сфері, забезпечення реалізації конституційних прав і свобод людини і громадянина в інтересах зміцнення демократії, досягнення і підтримування суспільної злагоди, підвищення творчої активності населення.

Одним із джерел загроз інтересам суспільства в інформаційній сфері є безперервне ускладнення інформаційних систем і мереж зв'язку критично важливих інфраструктур забезпечення життя суспільства.

Ці загрози можуть проявлятися і вигляді як навмисних, так і ненавмисних помилок, збоїв і відмов техніки і програмного забезпечення, шкідливого впливу зі

сторони злочинних структур і кримінальних елементів. Об'єктами реалізації таких структур можуть виступати системи енергетичної, транспортної, трубопровідної і деяких інших інфраструктур.

Небезпечним джерелом загроз виступає можливість концентрації засобів масової інформації (ЗМІ) в руках невеликої групи власників.

Ці загрози можуть проявлятися у вигляді маніпуляції суспільною думкою по відношенню до тих чи інших суспільно значимих подій, а також руйнування моральних устоїв суспільства шляхом нав'язування чужорідних цінностей.

Нарешті, небезпечним джерелом загроз є розширення масштабів вітчизняної і міжнародної комп'ютерної злочинності.

Ці загрози можуть проявлятися у вигляді спроб здійснення шахрайських операції з використанням глобальних або вітчизняних інформаційно-телекомунікаційних систем, відмивання фінансових коштів, одержаних протиправним шляхом, одержання неправомірного доступу до фінансової, банківської та іншої інформації, яка може бути використаною з корисливою метою.

Джерела загроз інформаційній безпеці держави

Інтереси держави в інформаційній сфері полягають у створенні умов для гармонійного розвитку інформаційної інфраструктури держави, реалізації конституційних прав і свобод людини і громадянина в інтересах зміцнення конституційного ладу, суверенітету і територіальної цілісності країни, встановлення політичної і соціальної стабільності, економічного процвітання, безумовного виконання законів і підтримки міжнародного співробітництва на основі партнерства.

У першу чергу загрози інтересам держави також можуть проявлятися у вигляді отримання протиправного доступу до відомостей, що складають державну таємницю, до іншої конфіденційної інформації, розкриття якої може нанести збитки.

Проте найбільш небезпечними джерелами загроз інтересам держави в інформаційному суспільстві може стати неконтрольоване розповсюдження інформаційної зброї та розгортання гонки озброєнь у цій галузі, спроби реалізації концепції ведення інформаційних війн.

Серед найбільш серйозних завдань, які можуть вирішуватися за допомогою сучасної інформаційної зброї, можна виділити наступні:

– створення атмосфери бездуховності та аморальності, негативного відношення до культурної спадщини противника;

– маніпулювання суспільною свідомістю та політичною орієнтацією соціальних груп населення держави з метою створення політичної напруги та хаосу;

– дестабілізація політичних відносин між партіями, об'єднаннями та рухами з метою провокації конфліктів, розпалювання недовіри, загострення політичної боротьби, провокування репресій проти опозиції, провокація взаємного знищення;

– зниження інформаційного забезпечення влади та управління, інспірація помилкових управлінських рішень;

– дезінформація населення про роботу державних органів, підрив їхнього авторитету, дискредитація органів управління;

– провокування соціальних, політичних, національних і релігійних сутичок;

– ініціювання страйків, масових заворушень та інших акцій економічного протесту;

– ускладнення прийняття органами важливих рішень;

– підрив міжнародного авторитету держави, її співробітництва з іншими країнами;

– нанесення втрат життєво важливим інтересам держави в політичній, економічній, оборонній та інших сферах.

Руйнівний вплив інформаційних загроз в інформаційному суспільстві може бути більш потужним та ефективним, ніж це уявляється. Особливо небезпечним це є в умовах існування майже монопольного положення компаній невеликої кількості країн на ринку інформаційних продуктів, оскільки це здатне спровокувати бажання використати наявну перевагу для досягнення тієї чи іншої політичної мети.

Хід роботи

1. Ознайомитися з теоретичними матеріалами по темі.
2. Проаналізувати загрози, що проявляються у вигляді маніпуляції суспільною думкою по відношенню до тих чи інших суспільно значимих подій, а також руйнування моральних устоїв суспільства шляхом нав'язування чужорідних цінностей, викликані можливістю концентрації засобів масової інформації (ЗМІ) України в руках невеликої групи власників.
3. За результатами роботи підготувати звіт
4. Зробити висновки.

Контрольні питання

1. Яким чином розрізняються групи загроз інформації?
2. Назвіть основні характеристики загроз інформаційній безпеці України.
3. Які основні підходи до визначення дестабілізуючих факторів ви знаєте?
4. Дайте визначення поняттям «загроза», «небезпека».
5. Як співвідносяться категорії «небезпека» та «загроза»?
6. Визначте види загроз за певними критеріями.
7. Визначте фактори загроз за певними критеріями.
8. Назвіть джерела загроз інформаційній безпеці.
9. Назвіть базові загрози інформаційній безпеці держави.
10. Назвіть базові загрози інформаційній безпеці суспільству.
11. Назвіть базові загрози інформаційній безпеці людині, громадянину.
12. Які існують етапи розвитку засобів інформаційних комунікацій?
13. Які завдання можуть вирішуватися за допомогою сучасної інформаційної зброї?

Практичне заняття № 2

2 години

Тема заняття: Методи та засоби забезпечення інформаційної безпеки держави.

Мета заняття: ознайомитися із методами та засобами забезпечення інформаційної безпеки держави.

Теоретичні відомості

Держава здійснює свої заходи через відповідні органи, а громадяни, суспільні організації і об'єднання, що мають відповідні повноваження, - у відповідності із законодавством. В основу забезпечення інформаційної безпеки держави повинні

бути покладені наступні принципи:

– законність, дотримання балансу інтересів особистості, суспільства і держави;

– взаємна відповідальність суб'єктів забезпечення інформаційної безпеки;

– інтеграція систем національної і міжнародної безпеки.

Специфічними принципами забезпечення інформаційної безпеки є:

– превентивний характер проведення її заходів по відношенню до заходів інших видів безпеки;

– адекватна інформованість об'єктів безпеки, в тому числі і міжнародних.

Превентивність (лат. praeventio від praevenio – «попереджую») зумовлена властивою людині послідовністю виконання операцій, що складає будь-яку елементарну дію. Усе починається з приймання (добування) інформації, а закінчується активною дією: реакцією на одержану інформацію. Оскільки це справедливо по відношенню до будь-якого виду діяльності, то можна стверджувати, що даний принцип є загальним, і його дія розповсюджується на всі сфери безпеки особистості, суспільства та держави.

Адекватна інформованість об'єктів безпеки означає, що всі вони мають право володіти інформацією про явища і процеси, що їх цікавлять, яке обмежене тільки законодавчо з метою охорони особистої, сімейної, професійної, комерційної та державної таємниці, а також моралі. Права та свободи суспільства в питаннях пошуку, володіння та розповсюдження інформації повинні регулюватися законодавчими актами, які видаються, щодо специфіки діяльності суспільних об'єднань та організацій або змісту інформації. Наприклад, адекватна інформованість суспільства про його матеріальні цінності досягається у сфері нормотворчості та правозастосування законодавства про захист комерційної таємниці. Права та свободи суспільства в духовній сфері повинні захищати законодавчі акти, які визначають порядок освіти та функціонування освітніх, просвітницьких, культурних, релігійних організацій, а також засобів масової інформації. В основі прав і свобод держави у сфері її інформованості з питань світової політики, економіки, науки, ресурсів, екології, оборони і т.ін. лежать діючі норми та принципи міждержавного права. Головним слід вважати принцип рівної безпеки. Стосовно до інформаційної сфери можна говорити про його трансформацію в принцип адекватної інформованості держав світового співтовариства, який передбачає право кожної держави на інформаційну безпеку, забезпечення інформаційної безпеки усіх членів співтовариства в рівній мірі, врахування інтересів усіх сторін без будь-якої дискримінації, виключення односторонніх переваг, відмова від дій, що наносять шкоду іншій державі.

Законодавча база, яка визначає перелік відомостей, що віднесені до державної таємниці, механізм та порядок її захисту повинні розроблятися, виходячи із наведеного принципу, а також багатосторонніх угод держав, які входять до міжнародної системи інформаційної безпеки. Формування останньої буде, очевидно, справою далекої перспективи, яка ознаменує собою вищий рівень прояву довіри та зацікавленості держав світового співтовариства в забезпеченні виконання на практиці принципу адекватної інформованості. Така система повинна стати підсистемою у системі колективної безпеки.

Система забезпечення інформаційної безпеки держави

Забезпечення інформаційної безпеки держави - це сукупність заходів,

призначених для досягнення стану захищеності потреб особистостей, суспільства і держави в інформації.

Відсутність системи забезпечення інформаційної безпеки унеможливлює надійне забезпечення не лише інформаційної, а й національної безпеки. Головне призначення цієї системи полягає у досягненні цілей національної безпеки в інформаційній сфері, а отже основною функцією даної системи є забезпечення збалансованого існування інтересів особи, суспільства і держави в інформаційній сфері.

Забезпечення інформаційної безпеки досягається у процесі свідомої цілеспрямованої діяльності органів державного управління, по запобіганню можливого порушення їх нормального функціонування в результаті дії загроз та небезпек. Метою забезпечення інформаційної безпеки є створення нормальних умов функціонування конкретного органу державного управління, а також проведення моніторингу стану інформаційної безпеки для розроблення оптимальної моделі функціонування системи забезпечення інформаційної безпеки.

Державна система забезпечення інформаційної безпеки країни 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 складає найважливішу ланку системи інформаційної безпеки особистості, суспільства і держави в правовій державі. Основними завданнями такої системи є:

− виявлення і прогнозування дестабілізуючих факторів і інформаційних загроз життєво важливим інтересам особистості, суспільства та держави;

− здійснення комплексу оперативних і довготривалих заходів з їхнього попередження і усунення;

− створення і підтримання в готовності сил та засобів забезпечення інформаційної безпеки.

Органи (служби) інформаційної безпеки можуть створюватися (на законодавчих засадах) і в недержавних структурах для захисту своїх потреб в забезпеченні необхідною інформацією. Дані органи на основі укладення відповідних угод можуть бути приєднані до єдиної державної системи інформаційної безпеки.

Таким чином, управління в сфері інформаційної безпеки має здійснюватися на підставі принципу доступності та безпеки. Система забезпечення інформаційної безпеки в першу чергу має гарантувати доступність і цілісність інформації, а її конфіденційність у випадку необхідності.

Основні форми забезпечення інформаційної безпеки держави

Форми і способи забезпечення інформаційної безпеки утворюють власне інструмент, з допомогою якого сили інформаційної безпеки вирішують весь комплекс завдань із захисту життєво важливих інтересів особистості, суспільства та держави. Тому необхідне чітке юридичне оформлення при розробці нормативних актів, які регулюють діяльність органів інформаційної безпеки. Найважливіша вимога до обґрунтування способів, форм і механізмів їхньої реалізації полягає в абсолютному верховенстві права у будь-якій, в тому числі і політичній діяльності. У свою чергу, кожний суб'єкт інформаційного процесу повинен мати відповідну правову свідомість, бути законослухняним, добре уявляти наслідки своїх дій для

інших суб'єктів та міру відповідальності на випадок порушення їхніх життєво важливих інтересів. Це є принциповим, оскільки застосування тих чи інших форм і способів залежить від того, чи є інформаційні загрози наслідком ненавмисних або навмисних дій суб'єктів інформаційного процесу. У першому випадку забезпечення інформаційної безпеки здійснюється відповідно у формах інформаційного патронату та інформаційної кооперації, у другому - у формі інформаційного протиборства

Інформаційний патронат (лат. patronatys від patronys - "захисник") - форма забезпечення інформаційної безпеки фізичних і юридичних осіб з боку держави. Він припускає забезпечення органів управління системи інформаційної безпеки держави відомостями про дестабілізуючі фактори і загрози стану інформованості фізичних і юридичних осіб (інформаційне забезпечення інформаційної безпеки) і власне захист життєво важливих інтересів цих осіб від інформаційних загроз або, як ще кажуть, - інформаційний захист.

При цьому інформаційне забезпечення інформаційної безпеки включає збирання (добування) відомостей про дестабілізуючі фактори та інформаційні загрози, їхню обробку, обмін інформацією між органами керування і силами та засобами системи інформаційної безпеки. Його основу складає збирання (добування) необхідних відомостей, здійснюване в процесі розвідувальної, оперативно-розшукової і оперативно-інформаційної діяльності.

Інформаційний захист досягається шляхом внесення в порядку законодавчої ініціативи законопроектів, здійснення судового захисту, проведення оперативних заходів силами і засобами інформаційної безпеки.

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

Інформаційне протиборство - форма забезпечення інформаційної безпеки при здійсненні навмисних деструктивних дій суб’єктів інформаційного процесу.

Інформаційне протиборство - суперництво соціальних систем (країн, блоків країн) в інформаційній сфері з приводу впливу на ті або інші сфери соціальних відносин і встановлення контролю над джерелами стратегічних ресурсів, у результаті якого одна група учасників суперництва отримує переваги, необхідні їм для подальшого розвитку.

Для конкретної особистості такими способами і засобами можуть бути:

- судовий захист прав і свобод у використанні інформації;
- адміністративний захист її життєво важливих інтересів у інформованості з боку територіальних або відомчих органів інформаційної безпеки;
- автономний захист своїх прав і свобод в основному із застосуванням технічних засобів захисту, особистої, сімейної і професійної таємниці.

Це ж характерно і для суспільних об'єднань, організацій (підприємств). Разом із тим, при наявності у них власних органів інформаційної безпеки, їхні можливості у сфері автономного захисту суттєво розширюються.

Методи забезпечення інформаційної безпеки

Під інформаційною безпекою слід розуміти захищеність від будь-яких

випадкових або зловмисних дій, результатом яких може з'явитися нанесення збитку самої інформації або її власникам .

Завдання забезпечення інформаційної безпеки повинно вирішуватися системно, це означає, що різні засоби повинні застосовуватися одночасно і під централізованим управлінням. При цьому всі складові системи повинні «знати» про існування один одного, взаємодіяти і забезпечувати захист як від зовнішніх, так і від внутрішніх загроз.

Існує багато методів забезпечення інформаційної безпеки:

- засоби антивірусного захисту;
- засоби шифрування інформації, що зберігається на комп'ютерах і переданої мережами;
- інструменти перевірки цілісності вмісту дисків;
- віртуальні приватні мережі;
- міжмережеві екрани;
- засоби аутентифікації користувачів;
- системи виявлення уразливостей мереж і аналізатори мережевих атак.

Кожен з перерахованих методів може бути використаний як самостійно, так і в інтеграції з іншими.

Сучасні антивірусні технології дозволяють виявити практично всі вже відомі вірусні програми через порівняння коду підозрілого файлу із зразками, що зберігаються в антивірусній базі. Виявлені об'єкти можуть піддаватися лікуванню, та можуть бути видалені. Захист від вірусів може бути встановлений на робочі станції, файлові і поштові сервери, міжмережеві екрани, що працюють під практично будь-якою з поширених операційних систем (Windows, Unix-і Linux системи, Novell).

Значно зменшують непродуктивні трудові витрати фільтри спаму, пов'язані з розбором спаму, знижують трафік і завантаження серверів, покращують психологічний фон в колективі і зменшують ризик залучення співробітників компанії на шахрайські операції. Крім того, фільтри спаму зменшують ризик зараження новими вірусами, оскільки повідомлення, що містять віруси часто мають ознаки спаму і фільтруються.

Резервне копіювання є одним з основних методів захисту від втрати даних з чітким дотриманням методів зберігання копій та регулярності .

Ідентифікація та авторизація - це ключові елементи інформаційної безпеки. Функція авторизації відповідає за те, до яких ресурсів конкретний користувач має доступ. Функція адміністрування наділяє користувача певними ідентифікаційними особливостями в рамках даної мережі та визначенні обсягу допустимих для нього дій.

Системи шифрування дозволяють мінімізувати втрати у разі несанкціонованого доступу до даних, що зберігаються на жорсткому диску або іншому носії, а також перехоплення інформації при її пересиланні по електронній пошті або передачу з мережних протоколів. Завдання даного засобу захисту - забезпечення конфіденційності.

Міжмережевий екран являє собою систему або комбінацію систем, що утворить між двома або більше мережами захисний бар'єр, що оберігає від несанкціонованого потрапляння в мережу або виходу з неї пакетів даних. Таким чином, міжмережеві

екрани значно розширюють можливості сегментування інформаційних мереж.

Ефективний засіб захисту від втрати конфіденційної інформації - фільтрація вмісту вхідної та вихідної електронної пошти. Перевірка самих поштових повідомлень і вкладень в них на основі правил, встановлених в організації, дозволяє також убезпечити компанії від відповідальності за судовими позовами і захистити їх співробітників від спаму. Засоби тематичної фільтрації дозволяють перевіряти файли всіх поширених форматів, у тому числі стислі і графічні. При цьому пропускна здатність мережі практично не змінюється.

Всі зміни на робочій станції або на сервері можуть бути відстеженні адміністратором мережі або іншим авторизованим користувачем завдяки технології перевірки цілісності вмісту жорсткого диску (integrity checking). Це дозволяє виявляти будь-які дії з файлами та ідентифікувати активність вірусів, несанкціонований доступ або крадіжку даних авторизованими користувачами.

Хід роботи

1. Ознайомитися з теоретичними матеріалами по темі.
2. Проаналізувати методи забезпечення інформаційної безпеки, що використовуються у вашому університеті.
3. За результатами роботи підготувати звіт
4. Зробити висновки.

Контрольні питання

1. Поняття системи забезпечення інформаційної безпеки держави.
2. У чому полягає відмінність системи інформаційної безпеки від системи забезпечення інформаційної безпеки?
3. Що таке превентивність?
4. Дати визначення інформаційного протиборства.
5. Що таке інформаційна кооперація?
6. Що таке інформаційний патронат?
7. Як можна тлумачити поняття адекватної інформованості?

Практична робота № 3

2 години

Тема роботи: Поняття та зміст інформаційного протиборства. Основи теорії інформаційної боротьби.

Мета роботи: ознайомитися з основними формами інформаційного протиборства та основами теорії інформаційної боротьби.

Теоретичні відомості

Основні форми інформаційного протиборства

Інформаційне протиборство - суперництво соціальних систем (країн, блоків країн) в інформаційній сфері з приводу впливу на ті або інші сфери соціальних відносин і встановлення контролю над джерелами стратегічних ресурсів, у результаті якого одна група учасників суперництва отримує переваги, необхідні їм для подальшого розвитку.

Інформаційне протиборство у наукових колах також розрізняють у широкому й вузькому розумінні.

Інформаційне протиборство (у широкому розумінні) - це форма боротьби, що становить сукупність спеціальних (політичних, економічних, дипломатичних, технологічних, військових та інших) методів, способів і засобів вигідного впливу на інформаційну сферу об'єкта зацікавленості та захисту власної інформаційної сфери в інтересах досягнення поставлених цілей.

Інформаційне протиборство (у вузькому розумінні - у військовій, оборонній сферах) - це комплекс заходів інформаційного характеру, здійснюваних з метою захоплення й утримання стратегічної ініціативи, досягнення інформаційної переваги над противником і створення сприятливого пропагандистського підґрунтя при підготовці й веденні бойової й іншої діяльності збройних сил.

Види інформаційного протиборства: *інформаційно-технічне* й *інформаційно-психологічне*. Головними об'єктами впливу інформаційно-технічного протиборства є системи телекомунікації і зв'язку, радіоелектронні засоби тощо. Об'єктом інформаційно-психологічного протиборства залишаються свідомість і психіка населення й особового складу збройних сил, спецслужб противника та системи формування суспільної думки і прийняття стратегічних рішень.

Концепція інформаційного протиборства передбачає його ведення на воєнному та державному рівнях. На державному рівні метою інформаційного протиборства є послаблення позицій конкуруючих держав, підрив їх національно-державних основ, порушення системи національного управління за рахунок інформаційного впливу на політичну, дипломатичну, економічну та соціальну сфери життєдіяльності країни, проведення психологічних операцій, підривних та інших деморалізуючих пропагандистських акцій. Воно спрямовано на забезпечення національних інтересів держави, упередження міжнародних конфліктів, терористичних акцій, забезпечення інформаційної безпеки країни та розглядається як вид стратегічного протиборства країн.

За інтенсивністю, масштабами та засобами, які використовуються, виділяють наступні ступені інформаційного протиборства: інформаційна експансія, інформаційна агресія та інформаційна війна.

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 їх власними цінностями й ідеологічними установками; збільшення ступеня свого впливу та присутності, встановлення контролю над стратегічними інформаційними ресурсами, інформаційно-телекомунікаційною структурою і національними ЗМІ; нарощування присутності власних ЗМІ в інформаційній сфері об'єкта проникнення і т.п.

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.

Ознаки інформаційної агресії: виключення із засобів інформаційної дії самих небезпечних видів, що не дозволяють надійно контролювати розміри, завданого збитку; обмеження розмірів простору, об'єктів інформаційної інфраструктури та соціальних груп, що піддаються ураженню інформаційною дією (агресія зачіпає

інформаційний простір держави не цілком, а тільки його частину); обмеження за метою (переслідує локальну, приватну мету) і часу (як правило, агресія припиняється після повного досягнення агресором усієї поставленої конкретної мети й рідко набуває затяжного характеру), а також по силах і засобах, що залучаються.

Інформаційна війна - найвищий ступінь інформаційного протиборства, спрямований на розв'язання суспільно-політичних, ідеологічних, а також національних, територіальних та інших конфліктів між державами, націями, класами й соціальними групами шляхом широкомасштабної реалізації народами, засобів і методів інформаційного насильства (інформаційної зброї). Можна вважати, що в інформаційній сфері агресія переростає у війну в тому випадку, якщо одна зі сторін конфлікту починає широко застосовувати проти своїх супротивників інформаційну зброю. Цей критерій дозволяє виділити з усього різноманіття процесів і явищ, що відбуваються в інформаційному суспільстві такі, які представляють для його нормального (мирного) розвитку найбільшу небезпеку. Нині відсутні міжнародні та національні правові норми, які дозволяють в мирний час (за відсутності офіційного оголошення війни з боку агресора) юридично кваліфікувати ворожі дії іноземної держави в інформаційній сфері, що супроводжуються нанесенням збитку інформаційній або іншій безпеці країни, як акції інформаційної агресії або інформаційної війни. Крім того, відсутні чіткі, однозначні, закріплені юридично критерії оцінки отриманого в результаті інформаційної агресії або інформаційної війни матеріального, морального, іншого збитку.

Це дозволяє в мирний час активно використовувати самий небезпечний і агресивний арсенал сил і засобів інформаційної війни - як основний засіб досягнення політичної мети.

Інформаційна війна ведеться не тільки у фізичному просторі, де знаходяться фізичні інформаційні системи і засоби, але і у деякій віртуальній зоні (віртуальному або кібернетичному просторі). Інформаційна війна розширює простір ведення війн, глибинами у світовому океані.

До особливостей інформаційної війни відноситься те, що вона ведеться як під час фактичних бойових дій, так і у мирний час і у кризових ситуаціях без офіційного оголошення. Початок інформаційної війни неможливо визначити однозначно. В інформаційній війні відсутня лінія фронту; проведення противником операцій інформаційної війни практично неможливо виявити, а якщо факти проведення таких операцій виявляються, то вони залишаються анонімними.

Будь-які міжнародні юридичні і моральні норми ведення інформаційної війни відсутні. Та чи інша країна може стати об'єктом інформаційної дії, не знаючи про це. Невисока вартість технічних засобів, які можуть бути використані у інформаційній війні, суттєво розширюють коло можливих її учасників. Ними можуть бути окремі країни та їхні органи розвідки, злочинні, терористичні і наркобізнесові угруповання, комерційні фірми і навіть особи, які діють без злочинних намірів.

Завданнями інформаційної війни є:

– створення атмосфери бездуховності, негативного ставлення до культури та історичної спадщини в суспільстві конкурента чи ворога;

– маніпулювання громадською думкою й політичною орієнтацією населення держави з метою створення політичного напруження та стану, близького до хаосу;

– дестабілізація політичних відносин між партіями, об'єднаннями й рухами для розпалення конфліктів, стимулювання недовіри, підозри, загострення ворожнечі, боротьби за владу;

– провокування та застосування репресій із боку влади щодо опозиції;

– зниження рівня інформаційного забезпечення органів влади й управління, інспірація помилкових управлінських рішень;

– уведення населення в оману щодо роботи державних органів влади, підрив їхнього авторитету, дискредитація їхніх дій;

Концепція інформаційної війни - це система поглядів на інформаційну війну та шляхи її ведення. За останніми оцінками, концепція інформаційної війни повинна передбачати:

– заглушення (у воєнний час) елементів інфраструктури державного і воєнного управління (ураження центрів командування і управління);

– електромагнітний вплив на елементи інформаційних і телекомунікаційних систем (радіоелектронна боротьба);

– одержання розвідувальної інформації шляхом перехоплення і декодування (дешифрування) інформаційних потоків, що передаються каналами зв'язку, а також побічним випромінюванням і за рахунок спеціально впроваджених у приміщення технічних засобів і електронних пристроїв перехоплення інформації (радіоелектронна розвідка);

– здійснення несанкціонованого доступу до інформаційних ресурсів (шляхом використання програмно-апаратних засобів зламу систем захисту інформаційних і телекомунікаційних мереж противника) із наступним їхнім спотворенням, знищенням або викраденням чи порушенням нормального функціонування цих систем (так звана "хакерна війна");

– формування і масове розповсюдження інформаційними каналами противника або глобальними мережами інформаційної взаємодії дезінформації або тенденційної інформації для впливу на оцінки, наміри і орієнтацію населення і осіб, що приймають рішення (психологічна війна);

– одержання необхідної інформації шляхом перехоплення і обробки відкритої інформації, що передається незахищеними каналами зв'язку або циркулює в інформаційних системах, а також опублікованої у засобах масової інформації.

Органи інформаційної війни - це органи керування інформаційною війною та люди (фахівці, офіцери, підрозділи) для її ведення. До органів інформаційної війни можуть відноситись:

– органи планування й координації з питань інформаційної війни, які здійснюють розробку системи планування діяльності з усіх питань, що пов'язані з інформаційною війною;

– органи стратегічного рівня з відслідковування ознак початку інформаційної війни, які займаються збиранням і аналізом розвідувальної інформації, визначенням ознак початку інформаційних атак (акцій);

– органи проведення операцій із захисту від інформаційної зброї, які здійснюють попередження про інформаційні атаки тактичного рівня і займаються ліквідацією наслідків інформаційного нападу;

– підрозділи розробки конструкцій та архітектури автоматизованих систем управління (АСУ), що здійснюють розробку єдиної архітектури й технічних стандартів у галузі засобів і систем захисту від інформаційної зброї;

– групи незалежних експертів, що здійснюють аналіз уразливості АСУ, у тому числі через здійснення експериментальних атак на АСУ та їхні окремі елементи.

Основні форми інформаційної війни

Усі форми інформаційної війни зводяться до впливу на інформаційну інфраструктуру противника, його інформаційні системи та інформаційні ресурси із проведенням будь-яких дій, що мають за мету спотворення інформації, що він одержує, позбавлення його можливостей одержання нової інформації або фізичне знищення його інформаційних засобів, а також до захисту інформації власних збройних сил від аналогічних дій противника.

Спеціалісти пропонують ведення інформаційної війни на державному та воєнному рівнях. Якщо в мирний час метою інформаційної війни на державному рівні є схилення воєнно-політичного керівництва противника до прийняття вигідних для протилежної сторони рішень, то у воєнний час - повний параліч інформаційної інфраструктури противника при забезпеченні стійкого функціонування своєї. У цьому випадку на державному рівні основне завдання інформаційної війни полягає в забезпеченні гарантованої безпеки та стійкості національної інформаційної інфраструктури держави, намаганні завоювання інформаційної переваги над противником.

На державному рівні інформаційна війна ведеться з використанням політичних, дипломатичних, економічних, інформаційно-психологічних, інформаційно-технічних і воєнних способів.

Основною формою інформаційної війни на державному рівні є спеціальна інформаційна операція, яка може носити одночасно і наступальний, і оборонний характер, відповідає передбаченій мірі ризику та очікуваному потенційному ефекту, спрямована на забезпечення національних інтересів і національної безпеки держави. Операції даного типу можуть проводитися проти будь-яких держав, у тому числі й тих, що не є потенційними противниками. Визначення мети операції, завдань, часу та місця проведення потребує безпосереднього затвердження воєнно-політичним керівництвом держави.

Для погодження запланованих дій і заходів у галузі інформаційного протиборства при керівництві державою створюють спеціальний міжвідомчий орган із забезпечення інформаційної безпеки та об’єднаний центр інформаційних операцій. Їхніми завданнями є:

– організація цілеспрямованого інформаційно-психологічного впливу на воєнно-політичне керівництво союзних держав та держав, що є потенційними противниками;

– розробка єдиної національної стратегії ведення інформаційної війни;

– координація дій усіх органів, сил та засобів, що беруть участь у інформаційній війні;

– організація та проведення спеціальної інформаційної операції.

На воєнному рівні інформаційна війна планується вестись всебічно забезпеченими силами та засобами, що виділяються для боротьби з силами бойового управління противника. Метою даної боротьби є "обезголовлення" противника, позбавлення його надійної системи управління, захоплення ініціативи та примус противника реагувати на обстановку, що склалася, бажаним для командування чином при забезпеченні високої стійкості, безперервності та оперативності функціонування своїх систем управління військами (силами).

Інформаційна війна на воєнному рівні ведеться на основі використання інформаційно-насичених засобів розвідки, зв'язку, автоматизації, радіоелектронної та психологічної війни, високоточної зброї та звичайних засобів ураження, а також із застосуванням спеціально створеної інформаційної зброї, проведення комп'ютерних атак та захисту своїх комп'ютерних мереж.

Для ведення інформаційної війни у збройних силах створюються спеціальні бойові формування та органи управління ними. Цим формуванням приписується виконання наступних функцій:

– підготовка і забезпечення планування інформаційних дій, координація зусиль у ході інформаційної операції;

– здійснення доступу до інформації противника та досягнення контролю над нею;

– використання у випадку необхідності інформаційної зброї, участь в операціях із введення воєнно-політичного керівництва в оману;

– придушення або дезорганізація частини інформаційної інфраструктури противника з одночасним надійним захистом аналогічної структури своїх збройних сил та держави.

Основними формами інформаційної війни на воєнному рівні (ведення боротьби із системами бойового управління противника) є наступальні та оборонні інформаційні операції.

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).

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

Інформаційні операції повинні проводитися в умовах комплексного, погодженого у часі використання сил та засобів, які залучаються для боротьби із системами бойового управління противника: оперативної безпеки, радіоелектронної війни, воєнної дезінформації, психологічної війни, комп'ютерної атаки та захисту мереж та фізичного знищення. Наступальні та оборонні операції можуть вестися одночасно або послідовно як у мирний, так і у воєнний час.

По контексту **оперативна безпека** являє собою не бажаний стан, а комплекс заходів із виявлення критичної інформації, проведення аналізу дій своїх збройних сил із метою:

– виявлення демаскуючих ознак своїх військ (сил) і критичних елементів інформації, яка могла стати відомою противникові;

– вибір заходів, які зменшують уразливість своїх збройних сил та збройних сил союзників;

– протидія усім видам розвідки противника.

Окрім цього оперативна безпека включає в себе;

– інформаційну безпеку;

– безпеку систем управління, зв'язку та автоматизації;

– безпеку об'єктів і бойової техніки;

– фізичну безпеку особового складу.

Радіоелектронна війна включає комплекс заходів із застосуванням засобів електромагнітного випромінювання, спрямованих на зменшення ефективності або запобігання застосування противником електромагнітного спектру, а також на забезпечення ефективного використання електромагнітного спектру своїми військами.

Інтерпретація терміну «радіоелектронна війна» набагато ширше аналогічного терміну «радіоелектронна боротьба», оскільки вона включає в себе, окрім впливу на радіоелектронні засоби (РЕЗ), їхній захист та забезпечення, а також вплив на бойову техніку, системи озброєння, об'єкти та особовий склад та їхній захист.

Радіоелектронна війна є основоположним елементом впливу як на системи управління противника в оперативній і тактичній ланках, так і у цілому на інформаційну інфраструктуру противника. Вона включає три основних елементи:

– радіоелектронне забезпечення;

– радіоелектронна атака;

– боротьба з електронною протидією або радіоелектронна контрпротидія.

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 усіх рангів, а також виконання додаткових функцій, таких як ухилення від загрози з боку противника і високоточна цілевказівка системам озброєння.

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

– неруйнівні впливи, які включають електронне придушення і електронну дезінформацію;

– руйнівні впливи на основі застосування протирадіолокаційних ракет, зброї спрямованої енергії (лазерної, надвисокочастотної) і т.ін.

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

Необхідні умови для досягнення інформаційної переваги

Інформаційна перевага є одним із центральних понять у сфері інформаційного

протиборства. Воно являє собою здатність складної саморегулюючої системи управління та інформаційного забезпечення держави або воєнного відомства забезпечити стійкий безперервний процес своєчасного одержання достовірної інформації та доведення її до відповідних споживачів при одночасному отриманні можливості використання у своїх інтересах такої ж системи ймовірного противника або пониження ефективності роботи (виведення з ладу) останньої. При цьому під саморегулюючою системою розуміють особовий склад та компоненти збирання, обробки, аналізу, кореляції, зберігання в пам'яті ЕОМ, відображення на дисплеях, запису на магнітних та інших носіях інформації, систематичного своєчасного оновлення та уточнення, розподілу за мірою пріоритетності, передавання інформації споживачам та здійснення іншого впливу на інформацію.

На думку командування збройних сил США, щоб створити необхідні умови для досягнення інформаційної переваги над противником, необхідно вирішити п'ять взаємозалежних завдань.

По-перше, створити та ефективно використовувати інтегровану автоматизовану систему управління, зв'язку, розвідки та спостереження (C4ISR), що повинно значно підвищити фундаментальні можливості вирішення наступних завдань.

Друге завдання - це забезпечення примусового циркулярного доведення до виконавців важливої інформації в реальному масштабі часу та видобування конкретної інформації за запитами виконавців із баз даних вищих командних інстанцій (завдання User Pull/Producer Push).

Третє завдання спрямоване на вирішення питань адекватного співробітництва у розподілі Інформації (Distributed Collaboration), тобто на забезпечення командного складу штабів і військ (сил) за погодженою домовленістю необхідними засобами сполучення, приймання та розподілу інформації.

Після вирішення четвертого завдання збройні сили отримають можливість спільного та взаємно узгодженого, єдиного сприйняття та відображення різноманітними командними інстанціями реальної оперативної (бойової) та радіоелектронної обстановки (Consistent Situation Perception), що дозволить полегшити своєчасне прийняття оперативних рішень, адекватних реальній обстановці, організацію та підтримання взаємодії у ході операції.

Вирішення п'ятого завдання, що полягає у можливості повномасштабного використання системи C4ISR в інтересах радіоелектронної війни зокрема, та усіх сил і засобів боротьби з системами бойового управління противника в цілому, повинне дати можливість досягнення інформаційної переваги при проведенні інформаційних операцій за рахунок побудови та функціонування автоматизованих складних саморегулюючих систем (C4IEW,C4I2 та ін.).

Інформаційна зброя в інформаційній війні

До інформаційної зброї відноситься широкий клас засобів і способів інформаційного впливу на противника: від дезінформації і пропаганди до засобів радіоелектронної боротьби**.**

Інформаційну зброю від звичайних засобів ураження відрізняє:

– скритність - можливість досягнення мети без видимої підготовки та оголошення війни;

– масштабність - можливість наносити непоправні збитки не визначаючи державних кордонів і суверенітетів, без звичного обмеження простору в усіх середовищах життєдіяльності людини;

– універсальність - можливість багатоваріантного використання як воєнними, так і цивільними структурами країни, що нападає, як проти воєнних, так і цивільних об'єктів країни ураження.

Сфера застосування інформаційної зброї включає як воєнну галузь, так і економічну, банківську, соціальну та інші галузі потенційного використання з метою:

– дезорганізації діяльності управлінських структур, транспортних потоків та засобів комунікації;

– блокування діяльності окремих підприємств та банків, а також цільових галузей промисловості шляхом порушення багатоланкових технологічних зв'язків та системи взаєморозрахунків, проведення валютно-фінансових махінацій і т.ін.;

– ініціювання великих техногенних катастроф на території противника в результаті порушення штатного управління технологічними процесами та об'єктами, які мають справу із значними кількостями небезпечних речовин та високими концентраціями енергії;

– масового розповсюдження та впровадження у свідомість людей певних уявлень, звичок та поведінкових стереотипів;

– виклику невдоволення або паніки серед населення, а також провокування деструктивних дій різноманітних соціальних груп.

Слід відзначити, що **основними об’єктами застосування інформаційної зброї** як к у мирний, так і у воєнний періоди можуть виступати:

– комп'ютерні та телекомунікаційні системи, які використовуються державними організаціями при виконанні своїх управлінських функцій;

– воєнна інформаційна інфраструктура, яка виконує завдання управління військами та бойовими засобами збирання та обробки інформації в інтересах збройних сил;

– інформаційні та управлінські структури банків, транспортних та промислових підприємств;

– засоби масової інформації, і у першу чергу електронні (радіо, телебачення і т.ін.).

Інформаційна зброя воєнного застосування.

За галузями застосування інформаційну зброю можна розділити на інформаційну зброю воєнного та невоєнного (загального) застосування. Інформаційна зброя, застосування якої можливе у воєнних умовах (радіоелектронна боротьба), включає в себе засоби з наступними функціями:

– ураження звичайними боєприпасами за цілевказівками засобів радіо - та радіотехнічної розвідки з частковим самонаведенням на кінцевій ділянці;

– ураження високоточними боєприпасами нового покоління - інтелектуальними боєприпасами із самостійним пошуком цілі та самонаведенням на її уразливі елементи;

– радіопридушення засобів зв'язку маскувальними завадами;

– створення завад імітації, які ускладнюють входження у зв'язок, синхронізацію в каналах передавання даних, що ініціюють функції перезапиту та дублювання повідомлень;

– придушення за допомогою засобів силової радіоелектронної боротьби (за допомогою потужного електромагнітного випромінювання, яке створює завади за рахунок паразитних каналів прийому);

– силовий вплив імпульсом високої напруги через мережі живлення;

– порушення властивостей середовища розповсюдження радіохвиль;

– за допомогою спеціальних методів впливу на системи зв'язку;

– засоби генерації природної мови конкретної людини.

Інформаційна зброя воєнного та невоєнного застосування.

Особливу небезпеку інформаційна зброя представляє сьогодні для інформаційних комп'ютерних систем органів державної влади, управління військами та зброєю, фінансами та банками, економікою держави, а також для людей при інформаційно-психологічному впливі на них з метою зміни та управління їхньою індивідуальною та колективною поведінкою.

При цьому за своєю результативністю інформаційна зброя прирівнюється до зброї масового ураження.

До інформаційної зброї, застосування якої можливе як у воєнний, так і у мирний час, можуть бути віднесені засоби ураження інформаційних комп'ютерних систем та засоби ураження людей (їхньої психіки).

Засоби ураження комп'ютерних інформаційних систем.

Засоби ураження інформаційних комп'ютерних систем являють собою сукупність спеціально організованої інформації та інформаційних технологій, яка дозволяє цілеспрямовано змінювати (знищувати, спотворювати), копіювати, блокувати інформацію, долати системи захисту, обмежувати допуск законних користувачів, здійснювати дезінформацію, порушувати функціонування носіїв інформації, дезорганізовувати роботу технічних засобів комп'ютерних систем та інформаційно-обчислювальних мереж, що застосовується в ході інформаційної війни (боротьби) для досягнення поставлених цілей.

За метою використання така інформаційна зброя поділяється на інформаційну зброю атаки та інформаційну зброю забезпечення.

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

У складі інформаційної зброї атаки виділяють чотири основних види засобів інформаційних впливів:

– засоби порушення конфіденційності інформації;

– засоби порушення цілісності інформації;

– засоби порушення доступності інформації;

– засоби психологічного впливу на абонентів ІОМ.

Застосування інформаційної зброї атаки спрямоване на зрив виконання ІОМ цільових завдань.

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.

Успішне застосування інформаційної зброї забезпечення дозволяє здійснювати деструктивні впливи на інформацію, що зберігається, обробляється й передається в мережах обміну інформацією, з використанням інформаційної зброї атаки.

За способом реалізації інформаційну зброю поділяють на три великих класи:

- інформаційна алгоритмічна (математична) зброя;
- інформаційна програмна зброя;
- інформаційна апаратна зброя.

Інформаційна алгоритмічна (математична) зброя - це вид інформаційної зброї до якої, зазвичай, відносять:

- алгоритми, що використовують сполучення санкціонованих дій для здійснення несанкціонованого доступу до інформаційних ресурсів;
- алгоритми застосування санкціонованого (легального) програмного забезпечення і програмні засоби несанкціонованого доступу для здійснення незаконного доступу до інформаційних ресурсів.

До **інформаційної програмної зброї** відносять програми з потенційно небезпечними наслідками своєї роботи для інформаційних ресурсів мережі обміну інформацією.

Програми з потенційно небезпечними наслідками - це окремі програми (набори інструкцій) які мають спроможність виконувати будь-яку непусту множину наступних функцій:

- приховування ознак своєї присутності в програмно-апаратному середовищі мережі обміну інформацією;
- здатність до самодублювання, асоціювання себе з іншими програмами і (або) перенесення своїх фрагментів в інші ділянки оперативної або зовнішньої пам'яті;
- руйнування (спотворення довільним чином) кодів програм в оперативній пам'яті;
- збереження фрагментів інформації з оперативної пам'яті в деякій ділянці зовнішньої пам'яті прямого доступу (локальної або віддаленої);
- спотворення довільним чином, блокування і (або) підміна масивів інформації, що виводиться у зовнішню пам'ять або в канал зв'язку, утворених в результаті роботи прикладних програм, або масивів даних, що уже знаходяться у зовнішній пам'яті;
- придушення інформаційного обміну в телекомунікаційних мережах, фальсифікування інформації в каналах державного й воєнного управління;
- нейтралізація роботи тестових програм і систем захисту інформаційних ресурсів.

Програми з потенційно небезпечними наслідками умовно поділяють на наступні класи:

- (бойові) комп'ютерні віруси;
- засоби несанкціонованого доступу;

– програмні закладки.

Комп'ютерні віруси (від лат. virus - "отрута")] - це спеціальні програми, які здатні самочинно розмножуватися, створюючи свої копії, і поширюватися, модифікуючи (заражаючи) інші програми шляхом приєднання до них для наступного одержання управління та відтворення нових копій.

Після запуску заражених програм вірус може виконувати різні небажані дії, що порушують цілісність інформації та (або) режим роботи засобів обчислювальної техніки:

– псування файлів та каталогів;
– модифікування програмного забезпечення;
– спотворення результатів обчислень;
– засмічування або стирання пам'яті;
– створення завад при роботі комп’ютера, наприклад, різних аудіо - та відео-ефектів.

Програми вірусів складаються (виконуються, пишуться), в основному, на мові програмування Асемблер і при виконанні не створюють ніяких аудіовізуальних відображень у комп'ютерній системі.

Особливістю комп'ютерних вірусів є їхня не спрямованість на конкретні програми та властивість **самодублювання**. **Самодублювання програми з потенційно небезпечними наслідками** - це процес відтворення програмою з потенційно небезпечними наслідками свого власного коду в оперативній або зовнішній пам'яті персонального комп’ютера.

Комп'ютерні віруси можуть розмножуватися, впроваджуватися у програми, передаватися лініями зв'язку, мережами обміну інформацією, виводити з ладу системи керування і т.ін.

Засоби несанкціонованого доступу відносяться до класу програм з потенційно небезпечними наслідками, для яких обов'язковим є виконання наступних функцій:

– руйнування (спотворення довільним чином) кодів програм в оперативній пам'яті;
– збереження фрагментів інформації з оперативної пам'яті в деякій ділянці зовнішньої пам'яті прямого доступу (локальної або віддаленої);
– спотворення довільним чином, блокування і (або) підміна масивів інформації, що виводиться у зовнішню пам'ять або в канал зв'язку, утворених в результаті роботи прикладних програм, або масивів даних, що уже знаходяться у зовнішній пам'яті;
– нейтралізація роботи тестових програм і систем захисту інформаційних ресурсів.

До засобів несанкціонованого доступу відноситься всіляке позаштатне програмне забезпечення, яке противник може використати для порушення цілісності операційної системи або обчислювального середовища. Часто цей тип програмного забезпечення використовується для аналізу систем захисту з метою їхнього подолання і реалізації несанкціонованого доступу до інформаційних ресурсів мереж обміну інформацією.

Відмінною ознакою (відносно програмних закладок) засобів несанкціонованого доступу є наявність функцій подолання захисту.

Програмні закладки відносяться до таких програм з потенційно небезпечними наслідками, для яких обов'язковим є виконання наступних функцій:

- руйнування (спотворення довільним чином) кодів програм в оперативній пам'яті;
- збереження фрагментів інформації з оперативної пам'яті в деякій ділянці зовнішньої пам'яті прямого доступу (локальної або віддаленої);
- спотворення довільним чином, блокування і (або) підміна масивів інформації, що виводиться у зовнішню пам'ять або в канал зв'язку, утворених в результаті роботи прикладних програм, або масивів даних, що уже знаходяться у зовнішній пам'яті.

Відмінною ознакою (відносно засобів несанкціонованого доступу) є відсутність функцій подолання захисту.

Виділяють декілька видів програмних закладок:

- троянські програми;
- логічні бомби;
- логічні люки;
- програмні пастки;
- програмні черв'яки.

Особливості застосування інформаційної зброї.

На основі аналізу застосування інформаційної зброї в інформаційній війні можна скласти перелік особливостей, що характеризують основні риси застосування інформаційної зброї:

- **низька вартість** - на відміну від традиційних воєнних технологій, розробка інформаційної зброї не потребує значних фінансових ресурсів - достатньо мати досвід роботи в інформаційних системах і доступ у глобальні та відомчі мережі;
- **відсутність традиційних кордонів** - відмінності між суспільним і особистим, воєнною і кримінальною поведінкою, а також географічні кордони, які історично складалися між націями, розмиваються зростаючою взаємопов'язаністю інформаційних інфраструктур;
- **нові можливості для керування суспільною думкою** - сучасні інформаційні технології надають широкі можливості для маніпулювання свідомістю людей і ускладнюють державі роботу з політичної підтримки ініціатив у галузі забезпечення безпеки;
- **нові завдання перед органами розвідки** - неправильне розуміння ролі, можливостей і цілей інформаційної зброї знижує ефективність традиційної розвідувальної діяльності; необхідні нові форми розвідки, що концентруються на інформаційній стратегічній зброї;
- **складність оцінки загроз і формування системи попередження** - на даний час не існує систем попередження, які дозволили б їй відрізнити стратегічну атаку з використанням інформаційної зброї від інших форм діяльності в інформаційному просторі, включаючи шпигунство і випадкові помилки;
- **труднощі при створенні й підтримці коаліцій** - коаліції тільки збільшують уразливість їхніх учасників від інформаційної поразки;

– **уразливість власних територій** - оскільки інформаційні технології не обмежені в географічному плані, то інформаційною зброєю можуть уражатися цілі як на віддаленому театрі воєнних дій, так і усередині країни.

Зміст теорії інформаційної боротьби

Основні визначення теорії інформаційної боротьби

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 і ведення повинні носити плановий, систематичний характер, заснований на глибоких знаннях законів і закономірностей інформаційної боротьби.

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

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

Мета і завдання інформаційної боротьби визначають її зміст, а також і структуру теорії інформаційної боротьби. При цьому на зміст інформаційної боротьби великий вплив здійснює ряд факторів, серед яких виділяють політичний, економічний, духовний, власне воєнний та інформаційний.

Політичний фактор відіграє найважливішу роль у формуванні змісту інформаційної боротьби. Саме він визначає:

- її мету та завдання;
- причини виникнення та шляхи запобігання;
- способи і особливості ведення;
- розмах та тривалість;
- забезпечення матеріальними та фінансовими ресурсами.

Економічний фактор здійснює великий вплив на зміст і розвиток інформаційної боротьби. Від економіки залежить рівень інформатизації суспільства та держави, а значить, і ефективність ведення інформаційної боротьби як у мирний, так і у воєнний час. Науково-технічний прогрес, що безпосередньо впливає на вдосконалення засобів інформаційної боротьби, викликає глибокі, революційні зміни і в її теорії. Економічний розвиток на базі науково-технічного прогресу створює необхідні передумови для розробки ефективних способів виконання завдань інформаційної боротьби.

Духовний фактор здійснює вирішальний вплив на реалізацію положень теорії інформаційної боротьби. Загальна та професійна підготовка обслуговуючого персоналу інформаційних систем, його морально-політичний та психологічний стан, готовність до самовідданого захисту своєї країни мають першорядне значення при

виконанні завдань інформаційної боротьби і повинні враховуватися в її теорії.

Воєнний фактор лежить в основі розвитку інформаційної боротьби. Положення воєнної доктрини держави, воєнні концепції протилежної сторони, стан та перспективи розвитку засобів інформаційної боротьби, історичний досвід та нагромаджені знання в даній галузі - саме ця база є головною при розробці фундаментальних положень теорії інформаційної боротьби та визначенні напрямків її розвитку.

Інформаційний фактор нерозривно пов'язаний з інформаційною боротьбою, оскільки остання ведеться в інформаційному середовищі та залежить від рівня інформатизації сторін. Даний фактор визначає розмах боротьби, порядок і способи її ведення, вибір напрямку ударів, структуру сил та засобів, можливості їхнього маневру при проведенні впливу на інформаційне середовище противника.

Для визначення структури теорії інформаційної боротьби, ролі та місця її складових частин використовувались принципи наукової логіки. Складові частини теорії є відносно самостійними і, разом з тим, взаємопов'язаними галузями знань - такими, що виключають їхнє дублювання, але повністю охоплюють її зміст.

Оскільки основними завданнями інформаційної боротьби є ураження об'єктів інформаційного середовища противника та захист власної інформації, то структура теорії інформаційної боротьби повинна включати загальні основи теорії інформаційної боротьби, теорію ураження інформації і теорію захисту інформації.

Загальні основи теорії інформаційної боротьби - найважливіші спільні вихідні положення теорії інформаційної боротьби. У загальних основах визначаються:

- апарат понять інформаційної боротьби;
- напрямки і методи досліджень інформаційної боротьби;
- тенденції розвитку інформатизації і її роль у різноманітних галузях життя суспільства;
- роль і місце інформаційної боротьби в мирний і воєнний час;
- об'єкт, предмет, цілі, завдання і структура теорії інформаційної боротьби;
- категорії, закони, закономірності та принципи інформаційної боротьби.

Теорія ураження інформації як складова частина теорії інформаційної боротьби включає загальні положення і теорію сил і засобів ураження інформації. Загальні положення визначають предмет, завдання і зміст теорії ураження інформації, форми і способи ураження інформації, основні фактори, що впливають на зміст і ефективність ураження інформації.

Теорія сил і засобів ураження інформації визначає та вивчає показники оцінки ефективності ураження інформації, математичну модель ураження інформації, стан підготовки і вирішення завдань ураження інформації.

Теорія захисту інформації, як складова частина теорії інформаційної боротьби, включає загальні положення, що визначають: предмет, завдання і зміст теорії; об'єкти і елементи захисту інформації; основні фактори, що впливають на зміст і ефективність захисту інформації, а також визначає та вивчає загрози інформації і методологічні основи її захисту, систему показників оцінки ефективності захисту інформації, загальну математичну модель захисту інформації, організаційно-технічні і правові основи захисту інформації.

Найважливішими логічними елементами змісту загальних основ теорії

інформаційної боротьби є категорії, закони, закономірності і принципи інформаційної боротьби.

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

Розрізняють загальні і часткові категорії. Загальні категорії мають відношення до всіх галузей теорії інформаційної боротьби. Головні з них – «інформація» та «інформаційна боротьба». Часткові категорії формуються у складових частинах теорії. Так, теорія захисту інформації має свої категорії, наприклад, «захист інформації» та «інформаційна безпека», теорія ураження інформації - свої, наприклад, «ураження інформації».

1.5.2.Закони та закономірності інформаційної боротьби

Закони інформаційної боротьби визначаються як суттєві, необхідні відношення, що характеризують впорядкованість будови і функціонування, тенденції зміни і 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.

Оскільки інформаційна сфера є частиною соціальної діяльності суспільства, то в ній проявляють себе:

- загальні закони діалектики;
- загальні і специфічні закономірності соціального розвитку;
- власні закони, закономірності війни, інформаційної боротьби (наприклад, закон визначальної ролі політичних цілей війни);
- закони залежності ходу і кінця війни (інформаційної боротьби) від економічних, соціально-політичних, науково-технічних і воєнних можливостей протиборчих сторін.

Особливістю законів (закономірностей) війни, а також інформаційної боротьби є те, що, на відміну від законів і закономірностей природи, вони проявляються тільки через діяльність людей.

В теорій інформаційної боротьби постійно нагромаджуються знання про загальні закони та закономірності війни, проте основні зусилля спрямовуються на осмислення закономірностей, властивих інформаційній боротьбі. Вони тісно пов'язані із загальними законами війни, разом з тим їм властиві свої особливості.

Універсальний характер має наступна закономірність: кількість і якість засобів інформаційної боротьби, а також особового складу обумовлюють форми та способи інформаційної боротьби та її ефективність. Наведена закономірність проявляється в тому, що винайдення нових засобів інформаційної боротьби та їхнє впровадження в практику неминуче призводить до виникнення нових форм і способів інформаційної боротьби. Це підтверджує винайдення "комп'ютерних вірусів", "логічних бомб" та інших засобів ведення інформаційної боротьби. Ефективність останньої не в меншій мірі залежить від рівня професійної та морально-психологічної підготовки особового складу. Чим вона вища, тим більше можливостей для активних та рішучих дій приймається при захисті власності інформації та ураженні інформації

противника.

Закономірна також залежність цілей інформаційної боротьби від наявних засобів та можливостей для її ведення. Досвід свідчить, що постановка надмірних завдань, як і їхнє заниження, мають однаково негативні наслідки.

В галузі інформаційної боротьби можна визначити наступні закономірності:

− обумовленість масштабів та спрямованості характером створення воєнно-політичної та економічної обстановки, а також цілями воєнної політики держави, суспільних та економічних структур, які приймають участь в інформаційній боротьбі;

− відповідність змісту та масштабів створення до характеру та особливостей суспільного та державного устрою;

− залежність масштабу та якості створення від матеріальних та духовних можливостей держави (інших суспільних та економічних структур). На основі знання законів та закономірностей, а також набутого досвіду в результаті практичної діяльності розроблюються принципи інформаційної боротьби.

Принципи інформаційної боротьби - це науково обґрунтовані положення, правила, рекомендації з підготовки і ведення інформаційної боротьби, керівництва її силами і 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.

Воєнна наука керується насамперед принципами, що витікають із законів діалектики, із загальних законів і закономірностей соціального розвитку. Разом із тим, вона опрацьовує свої специфічні принципи, що відображають, головним чином, закономірності інформаційної боротьби. До таких принципів відносяться:

− принцип відповідності (підпорядкованості) цілей і завдань інформаційної боротьби політичним цілям;

− принцип необхідності зосередження сил та засобів інформаційної боротьби у вирішальному місці у вирішальний момент;

− принцип завчасної підготовки сил і засобів інформаційної боротьби;

− принцип постійної готовності сил і засобів інформаційної боротьби до захисту власної інформації і до руйнівного впливу на інформаційне середовище противника;

− принцип високої активності і рішучості дій;

− принцип узгодженого спільного застосування всіх сил і засобів інформаційної боротьби;

− принцип безперервності інформаційної боротьби;

− принцип ведення інформаційної боротьби з напруженням, необхідним для вирішення поставлених завдань;

− принцип своєчасного маневру силами і засобами інформаційної боротьби;

− принцип раптовості, застосування несподіваних для противника способів виконання завдань;

− принцип врахування духовного фактору в інтересах виконання поставлених

завдань;

– принцип всебічного забезпечення, підтримки боєздатності і своєчасності відновлення сил і засобів інформаційної війни;

– принцип твердості і безперервності управління силами і засобами інформаційної боротьби, непохитності в досягненні поставленої мети, виконанні прийнятих рішень і поставлених завдань.

Заходи інформаційної боротьби

Інформаційна боротьба розглядається як одна з форм забезпечення інформаційної безпеки від інформаційних навмисних загроз. Вона ведеться державними органами інформаційної безпеки з формуваннями, що мають різноманітний (суспільний) стан (фізичні особи, юридичні особи, суб'єкти міжнародного права) і зловмисно створюють інформаційні загрози життєво важливим інтересам особистості, суспільства і держави.

Інформаційна боротьба включає комплекс заходів інформаційного забезпечення, інформаційного захисту і інформаційної протидії, що здійснюються за єдиним задумом і планом з метою захоплення і утримання інформаційної переваги.

Інформаційне забезпечення в умовах інформаційної боротьби являє собою комплекс заходів добування інформації про противника в умовах протиборства, збирання інформації про свої сили і засоби, обробка інформації і обмін нею між органами керування з метою організації і ведення бойових дій. Результативність інформаційного забезпечення залежить від багатьох факторів і умов, які, кінець кінцем, здійснюють вплив на два основних елементи: інформування органу керування і сприйняття одержаної ним інформації.

Інформування - акт передавання органу керування певної поточної інформації. В залежності від змісту інформації, інформування можна класифікувати наступним чином:

– правильне інформування;

– правильне дезінформування;

– трансінформування;

– трансдезінформування.

Правильне інформування - це передавання органу керування неспотвореної інформації про істинну обстановку.

Правильне дезінформування - це передавання органу керування неспотвореної інформації про неправдиву обстановку.

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

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

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

Ступінь відповідності уявлень органу керування про ці характеристики їхнім

вихідним величинам створює передумови для виникнення різноманітних ситуацій інформаційної боротьби. Ці передумови реалізуються в залежності від того, наскільки інформація, що поступає, співвідноситься з образами істинних і неправдивих елементів обстановки, які зберігаються в інформаційному кадастрі.

Різноманітність ситуацій інформаційної боротьби буде визначатися ступенем відповідності апріорної і поточної інформації про обстановку. Оцінка ступеня такої відповідності повинна проводитися на моделі прийняття органом керування інформаційного рішення.

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

Інформаційний кадастр (франц. cadastre) - 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.

Процес прийняття інформаційного рішення передує усім іншим етапам процесу мислення людини або етапам обробки інформації у сучасних інформаційних системах. При моделюванні інформаційного рішення орган керування описується у вигляді інформаційної системи із самонавчанням, що сприймає поточну інформацію про обстановку.

Процедура прийняття інформаційного рішення полягає в послідовній селекції і класифікації поточної інформації. Селекція і класифікація здійснюється з використанням тезауруса апріорної інформації, основу якого складає інформаційний кадастр. Одержана в результаті прийняття інформаційного рішення інформація доповнює тезаурус і змінює ступінь інформованості органу управління про обстановку.

Інформаційна протидія - сукупність заходів інформаційної боротьби, спрямованих на протидію інформаційному забезпеченню протиборчої сторони. Інформаційна протидія включає блокування добування, обробки і обміну інформацією та впровадження дезінформації на всіх етапах інформаційного забезпечення. Завдання інформаційної протидії вирішуються шляхом маскування, контррозвідки, радіоелектронного придушення і руйнування інформаційних систем противника.

Інформаційний захист - це сукупність заходів захисту від інформаційної протидії противника, які включають дії з деблокування інформації, необхідної для вирішення завдань управління, і блокування дезінформації, що розповсюджується і упроваджується в систему управління. Інформаційний захист досягається проведенням контрольної розвідки, перевіркою інформації, захистом від вогневого ураження (захоплення) елементів інформаційних систем, а також радіоелектронним захистом. Інформаційний захист підвищує ефективність інформаційного забезпечення в умовах інформаційної протидії противника.

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

Способи інформаційної боротьби

Способи інформаційної боротьби визначають порядок і прийоми застосування сил і засобів інформаційної боротьби для захоплення і утримання інформаційної переваги над противником при підготовці і проведенні бойових дій.

Способи інформаційної боротьби включають:

– вид і послідовність інформаційних впливів на противника;

– об'єкти впливу;

– склад сил і засобів, що виділяються для ведення інформаційної боротьби, їхнє оперативне шикування (бойовий порядок).

Усі способи інформаційної боротьби можна поділити на три основні категорії: силові, інтелектуальні і комбіновані, - а також за аналогією із збройною боротьбою виділити дві основні групи способів: наступальні і оборонні.

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).

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

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

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

Спосіб блокування інформації полягає в тому, що на етапі підготовки і в ході бойових дій шляхом виконання комплексу заходів інформаційної протидії повністю або частково припиняється добування (збирання) інформації про обстановку і обмін інформацією в системах управління військами і зброєю противника. Для реалізації цього способу застосовується вогневе, радіоелектронне і 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 сковування сил противника є різновидом способу відвернення уваги. При його застосуванні у противника створюється переконання в наявності загрози для одного з його уразливих місць, запобігання якій потребує виділення частини сил та засобів.

Спосіб вимотування противника полягає в проведенні комплексу заходів

інформаційної протидії з метою примусити противника здійснювати невигідні і марні дії і, як наслідок, вступити в бій з розтраченими ресурсами і зниженою боєздатністю. При цьому можуть проводитися обмежені бойові або відволікаючі дії.

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. При виникненні справжньої загрози він також сприйме її як фальшиву і зможе діяти у відповідності до реальної обстановки.

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 обстановку у голів держав, що беруть участь у конфлікті. Крім того, можуть проводитися заходи, які сприяють загостренню реально існуючих або штучно створюваних протиріч у стані ворога з метою зменшити його воєнну і 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 провокування противника призначений для спонукання противника до здійснення будь-яких дій, корисних протилежній стороні.

Спосіб перевантаження противника полягає в тому, щоб на етапі підготовки і у ході бойових дій довести до противника таку кількість суперечливої інформації, яка перевантажує його систему управління і змушує приймати і реалізовувати рішення в умовах підвищеної невизначеності обстановки.

Спосіб навіювання на противника полягає у формуванні і наступному використанні інформаційного стереотипу конфронтуючої сторони. Для цього на етапі підготовки і 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 будь-яких дій, вигідних конфронтуючій стороні.

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.

Оборонні способи інформаційної боротьби реалізують деблокування та ототожнення інформації.

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 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.

Форми ведення інформаційної боротьби

До основних форм ведення інформаційної боротьби звичайно відносять наступні:

- інформаційна операція;
- інформаційна битва;
- інформаційна дія (акція);
- інформаційний удар.

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 і утримання інформаційної переваги над противником або зниження його інформаційної переваги) на театрі воєнних дій, стратегічному або оперативному напрямах. Інформаційні операції можуть бути наступальними та оборонними.

Наступальна інформаційна операція має за мету завоювання інформаційної переваги над противником. В 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, що проводяться в межах інформаційної боротьби, повинні забезпечувати сприятливі умови для бойових дій своїх військ (сил).

Оборонна інформаційна операція проводиться в умовах великої інформаційної переваги противника і має за мету зниження цієї переваги. В 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.

Мета інформаційної операції досягається вирішенням наступних завдань: інформаційним впливом на противника, інформаційним захистом і ефективним використанням інформаційних ресурсів власного угруповання військ (сил). Інформаційна операція, звичайно, проводиться в межах відповідної загальновійськової, самостійної, спільної або спеціальної операції.

За масштабами інформаційні операції можна класифікувати як стратегічні, оперативно-стратегічні, оперативні і оперативно-тактичні і характеризувати наступними основними показниками: просторовим розмахом, тривалістю, а також кількісним і якісним складом сил і засобів. В той же час необхідно відзначити, що ця специфічна галузь протиборства не передбачає використання таких чітко визначених для бойових дій понять, як фронт і тил (інформаційний вплив може здійснюватися на всю глибину території противника).

В деяких умовах обстановки не виключена можливість проведення в рамках інформаційної операції **інформаційної битви**, в ході якої вирішується одне з найважливіших оперативних завдань. Вона 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. В залежності від масштабу і виду інформаційної операції в ній може бути одна або декілька інформаційних битв, що здійснюються одночасно або послідовно.

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.

Для ефективного проведення заходів інформаційної боротьби інформаційні впливи на противника необхідно починати ще у мирний час, нерідко заздалегідь до початку воєнних (бойових) дій. Такі інформаційні впливи звичайно називають **інформаційними акціями**, оскільки вони виходять за межі власне інформаційної боротьби в область інформаційного протиборства геополітичних суб'єктів.

Інформаційні дії (акції) можна класифікувати за видами (наступальні і оборонні), масштабом (стратегічні, оперативно-стратегічні, оперативні, оперативно-тактичні і тактичні) і об'єктами впливу (інформаційні системи, морально-психологічний стан особового складу та їхня комбінація). До наступальних інформаційних дій відносяться інформаційний вплив (інформаційна акція) та інформаційна блокада, до оборонних - дії (акції) з інформаційного захисту.

Наступальний інформаційний вплив - це активний, цілеспрямований, узгоджений за завданнями, місцем і часом вплив залучених до ведення інформаційної боротьби сил і засобів протягом певного часу в заданому районі по окремих інформаційних об'єктах системи управління противника або його інформаційного ресурсу в цілому. При цьому можуть здійснюватися різноманітні інформаційні удари.

Інформаційна наступальна акція здійснюється в межах інформаційного протиборства (наприклад, маніпуляція засобами масової інформації, культури, мистецтва і т. ін.).

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). В рамках інформаційної блокади можуть також проводитися інформаційні удари різного виду та масштабу. Одним з основних способів досягнення мети інформаційної блокади у воєнній час є радіоелектронне **блокування** [electronic blocking] - узгоджений вплив засобами радіоелектронного придушення і функціонального ураження на технічні елементи систем розвідки і канали передавання інформації.

Необхідно також відзначити, що мета інформаційної блокади противника у воєнних конфліктах не може бути повністю реалізована без спеціальних заходів (акцій), які проводяться на рівні керівництва держави.

До оборонних відносяться **дії (акції)** з **інформаційного захисту** - узгоджені за завданнями, місцем і часом застосування залучених до ведення інформаційної

боротьби сил і засобів з метою забезпечення стійкості функціонування системи управління військами (силами) в умовах інформаційного впливу противника.

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).

Інформаційні удари можна класифікувати за масштабом (стратегічні, оперативно-стратегічні, оперативні, оперативно-тактичні, тактичні), типами (радіоелектронні, радіоелектронно-вогневі, комп'ютерні, спеціальні і комбіновані) і ступенем зосередження сил і засобів (вибіркові, зосереджено-масовані і масовані).

Радіоелектронний удар - це узгоджений за часом, глибиною та завданнями масований комплексний вплив різноманітних сил і засобів радіоелектронного придушення і функціонального ураження радіоелектронних об'єктів системи керування противника з метою зриву управління на окремих напрямках (або з окремих пунктів управління) на певний час.

Радіоелектронно-вогневий удар - це узгоджений за часом, глибиною та завданнями масований комплексний (радіоелектронний і вогневий) вплив сил і засобів радіоелектронної боротьби, ракетних військ і артилерії, авіації та інших сил і засобів, виділених для боротьби з системами керування противника, з метою зриву управління на окремих напрямках на певний час.

Комп'ютерний (програмний) удар - це узгоджений за часом, глибиною і завданнями масований комплексний вплив атакуючих сил і засобів деструктивного програмно-математичного впливу на об'єкти автоматизованих систем керування противника з метою зриву управління на окремих напрямках (або з окремих пунктів) на певний час.

Спеціальний удар - це узгоджений за часом, глибиною завданнями масований комплексний морально-психологічний вплив залучених до ведення інформаційної боротьби сил і засобів на особовий склад (насамперед на персонал органів управління) угруповання противника з метою зриву (ускладнення) управління на окремих напрямках на певний час.

Для досягнення мети інформаційних ударів, впливів, битв і операцій застосовується вся сукупність способів інформаційної боротьби.

Методологія оцінки ефективності інформаційної боротьби

Ефективність інформаційної боротьби виражається ступенем реалізації мети інформаційної боротьби.

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

Методологія оцінки ефективності інформаційної боротьби - одна з ключових проблем розвитку теорії інформаційної боротьби, вирішення якої надає теорії необхідну фундаментальність і відносну завершеність.

Стосовно до збройної боротьби в методології оцінки ефективності можна виділити два основних рівні. Перший (вищий) рівень включає оцінку ефективності у війнах і збройних конфліктах у цілому, другий - окремі методології оцінки ефективності в операціях (бойових діях).

Крім того, методологія (на кожному з рівнів) має загальну і спеціальну частину. Загальний рівень, призначений для оцінки ефективності власне інформаційної боротьби (як самостійного виду боротьби), спеціальний - для оцінки ефективності дій, в інтересах яких ведеться інформаційна боротьба.

До загальної частини методології повинні входити метод і методика оцінки ефективності інформаційної боротьби, а також показники і критерії її ефективності.

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 у відповідності до мети інформаційної боротьби. В основу методу може бути покладене математичне моделювання процесу забезпечення інформацією органів управління протидіючих сторін.

Методика оцінки ефективності інформаційної боротьби включає ряд взаємозв'язаних етапів оцінки ефективності інформаційної боротьби:

– формування інформаційного кадастру органів керування протиборчих сторін;

– оцінку характеристик інформації про обстановку, що поступає в органи керування, її селекцію і класифікацію;

– порівняльну оцінку величини показника інформованості органів керування своїми силами і засобами і силами і засобами противника.

Критерій ефективності інформаційної боротьби - це кількісна міра відображення ступеня інформаційної переваги однієї з протиборчих сторін. Визначається співвідношенням інформованості протиборчих сторін. Числове значення критерію визначається за формулою:

$$F = K_1 / K_2 .$$

В чисельнику формули - показник інформованості першої, а в знаменнику - другої конфронтуючої сторони. Перевага першої сторони над другою досягається у випадку, якщо $F > 1$.

Хід роботи

1. Ознайомитися з теоретичними матеріалами по темі.
2. Проаналізувати інформаційне протиборство, здійснюване Російською Федерацією у відношенні до України у період часу, заданий викладачем.
3. За результатами роботи підготувати звіт
4. Зробити висновки.

Контрольні питання

1. Дайте визначення поняття «інформаційне протиборство».
2. Назвіть рівні проведення інформаційного протиборства.
3. Назвіть основні ступені інформаційного протиборства.
4. Дайте визначення поняттям «інформаційна експансія», «інформаційна агресія» та «інформаційна війна».
5. Що відноситься до органів інформаційної війни?
6. Назвіть основні форми інформаційної війни.
7. Що являє собою оперативна безпека?
8. Яким чином відрізняється інформаційна зброя від звичайних засобів ураження?
9. Назвіть сферу застосування інформаційної зброї.

10. Назвіть основні об’єкти застосування інформаційної зброї.
11. Яким чином розрізняються засоби ураження інформаційних комп'ютерних систем?
12. Які функції мають спроможність виконувати програми з потенційно небезпечними наслідками?
13. Що таке комп’ютерні віруси?
14. Які існують види програмних закладок?
15. Дати визначення інформаційної боротьби.
16. Яка мета інформаційної боротьби?
17. Які фактори впливають на зміст інформаційної боротьби?
18. Які існують заходи інформаційної боротьби?
19. Охарактеризувати принципи інформаційної боротьби**.**
20. Дати визначення метода оцінки ефективності інформаційної боротьби.
21. Які існують форми ведення інформаційної боротьби?
22. Які існують способи інформаційної боротьби?
23. Що таке радіоелектронно-вогневий удар?
24. Формула для обчислення числового значення критерію ефективності інформаційної боротьби.

Практичне заняття № 4

2 години

Тема заняття: Захист інформаційних систем.

Мета заняття: ознайомитися із основними принципами захисту інформаційних систем.

Теоретичні відомості

Джерела конфіденційної інформації

Джерело інформації - це матеріальний об'єкт, що володіє певними відомостями (інформацією), що представляють конкретний інтерес для сторонніх осіб.

В загальному плані джерелами конфіденційної інформації можна вважати наступні категорії:

1. Люди (співробітники, обслуговуючий персонал, продавці, клієнти та ін.).
2. Документи будь-якого призначення.
3. Публікації: доповіді, статті, інтерв'ю, проспекти, книги та ін.
4. Технічні носії інформації й документів.
5. Технічні засоби обробки інформації.
6. Продукція, що випускається.
7. Виробничі й промислові відходи.

Люди, в якості джерел конфіденційної інформації займають особливе місце, як активні елементи, здатні виступати не тільки власниками конфіденційної інформації, але й суб'єктами зловмисних дій. Люди є і власниками і розповсюджувачами інформації в рамках своїх функціональних обов'язків. Крім того, що люди володіють важливою інформацією, вони ще здатні її аналізувати, узагальнювати, робити відповідні висновки, а також, за певних умов, приховувати, красти, продавати та виконувати інші кримінальні дії, аж до вступу в злочинні зв'язки зі зловмисниками.

Документи. Документи - це найпоширеніша форма обміну інформацією, її нагромадження та зберігання. Під документом розуміють матеріальний носій інформації (папір, кіно- і фотоплівка, магнітна стрічка й т.п.) із зафіксованої на ньому інформацією, призначеної для її використання в часі й просторі. Документ має досить різноманітне функціональне призначення. Він може бути представлений не тільки різним змістом, але й різними фізичними формами.

По спрямованості розрізняють організаційно-розпорядницькі, планові, статистичні, бухгалтерські й науково-технічні документи, що містять, по суті, всю масу відомостей про склад, стан і діяльність будь-якої організаційної структури від державного до індивідуального рівня, про будь-який виріб, товар, задум, розробку.

Публікації. Публікації - це інформаційні носії у вигляді різноманітних видань, вони діляться на первинні і вторинні. До первинних відносять книги, статті, періодичні видання, збірники, науково-технічні звіти, дисертації, рекламні проспекти, доповіді та ін. До вторинних - інформаційні карти, реферативні журнали, експрес-інформацію, огляди, бібліографічні покажчики, каталоги та ін.

Технічні носії. Інформація може бути фіксованою та нефіксованою. Фіксована інформація - це відомості, закріплені на якому-небудь фізичному носії, а нефіксована - це знання, якими володіють вчені, фахівці, працівники, які так чи інакше беруть участь у виробництві та здатні передавати ці знання іншим. Фіксована інформація різниться залежно від виду носія, на якому вона перебуває. До технічних носіїв інформації відносяться паперові носії, кіно- і фотоматеріали (мікро- і кінофільми), магнітні носії (дискети, жорсткі диски, стримери), відеозапис, інформація на екранах ПЕОМ, на табло колективного користування, на екранах промислових телевізійних установок і інших засобів.

Технічні засоби обробки інформації. Технічні засоби як джерела конфіденційної інформації є досить широкою і ємною в інформаційному плані групою джерел. По специфіці призначення й виконання їх можна розділити на дві великі групи:

- технічні засоби забезпечення виробничої і трудової діяльності;
- технічні засоби автоматизованої обробки інформації.

До групи засобів забезпечення виробничої і трудової діяльності входять всілякі технічні засоби, такі, наприклад, як телефонні апарати й телефонний зв'язок; телеграфний, фототелеграфний і факсимільний зв'язок; системи радіозв'язку (автономні, територіальні, релейні, супутникові й ін.); телевізійні (у тому числі і засоби промислового телебачення); радіоприймачі та радіотрансляційні системи; системи гучномовного зв'язку, підсилювальні системи різного призначення; засоби магнітного та відеозапису; засоби неполіграфічного розмноження документів (друкарські машинки, ксерокопіювальні апарати, факси) та інші засоби і системи. Всі ці засоби можуть бути джерелами перетворення акустичних сигналів, що містять комерційні секрети, в електричні й електромагнітні поля, здатні утворити електромагнітні канали витоку охоронюваних відомостей.

Особливу групу технічних засобів становлять автоматизовані системи обробки інформації (АСОІ). Привабливість ПЕОМ і інформаційних систем як джерел конфіденційної інформації обумовлена рядом об'єктивних особливостей, до числа яких відносяться:

- різке розширення сфери застосування інформаційної й обчислювальної

техніки (ПЕОМ, локальні й розподілені інформаційні мережі національного й міжнародного масштабу);
- збільшення обсягів оброблюваної й збереженої інформації в локальних і розподілених банках даних;
- збільшення числа користувачів ресурсами ПЕОМ та мереж: багатокористувальницький режим вилученого доступу до баз даних.

Привабливість полягає ще і в тому, що АСОІ містить досить значні асортименти інформації. У її базах даних є вся інформація про конкретне підприємство від досьє на співробітників до конкретної продукції, її характеристиках, вартості та інші відомості.

Продукція. Продукти праці виступають джерелами інформації, за якою досить активно полюють конкуренти. Особливу увагу звертають конкуренти на нову продукцію, що перебуває на стадії підготовки до виробництва. Виробництво будь-якої продукції визначається етапами «життєвого циклу»: ідеєю, макетом, дослідним зразком, випробуваннями, серійним виробництвом, експлуатацією, модернізацією та зняттям з виробництва. Кожен із цих етапів супроводжується специфічною інформацією, що проявляється різними фізичними ефектами, які у вигляді характеристик (демаскуючих ознак) можуть розкрити охоронювані відомості про вироблений товар.

Промислові та виробничі відходи. Відходи виробництва, так званий непридатний матеріал, можуть багато чого розповісти про використовувані матеріали, їх склад, особливості виробництва, технології. До них можливий доступ через смітники, місця збору металобрухту, ящики відходів дослідницьких лабораторій, сміттєві кошики кабінетів. Не менш серйозними джерелами конфіденційної інформації є промислові відходи: стружка, обрізки, зіпсовані заготівлі, поламані комплектуючі і т.д. Аналіз відходів допоможе довідатися про особливості виробництва, технології.

Як кожне окремо, так і в сукупності джерела конфіденційної інформації містять досить повні відомості про склад, стан і напрямки діяльності підприємства.

Інформаційна система як об’єкт захисту інформації

Загалом, інформація являє собою незамінну сировину для вироблення будь-якого рішення, яку необхідно добути, переробити та поставити до закінчення терміну придатності тому, кому вона потрібна, тобто цінні відомості, що добуваються на превелику силу, повинні вчасно надійти тому, кому вони необхідні, оскільки інформація корисна тільки тоді, коли її можна використовувати для прийняття серйозних рішень. Все це визначає необхідність впровадження складних систем збору, обробки й аналізу різної інформації.

При вирішенні проблеми задоволення інформаційної потреби необхідно мати на увазі три компоненти: людину (споживача інформації), що формулює свої задачі; інформаційний фонд (інформаційний ресурс), у якому зосереджена необхідна людині інформація, і відповідний пристрій, що є посередником між споживачем і інформаційним масивом. Набір перелічених компонент і являє собою інформаційну систему.

Інформаційна система (ІС), як і будь-яка інша, має певну структуру, склад, фахівців, засоби, обладнання і порядок функціонування.

Продуктом інформаційної системи є інформація, властивості якої змінюються відповідно до заданої технології за допомогою комплексу різних технічних засобів і людей, що виконують певні технологічні операції. Відомо, що технологічні операції - це сукупність дій, спрямованих на зміну стану предмета виробництва. В інформаційній системі предметом виробництва є інформація, що на виході системи набуває потрібного користувачу вигляду та змісту.

У структуру інформаційної системи входять наступні складові:

1. Користувачі.

2. Інформаційні ресурси , документи та масиви документів в різних формах та видах (бібліотеки, архіви, фонди, бази даних, бази знань, а також інші форми організації та зберігання інформації), які містять інформацію по всім напрямкам життєдіяльності суспільства.

3. Носії інформації:

- на паперовій основі;
- звуконосії;
- фото носії;
- відео носії;
- магнітні носії;
- спеціальні технічні носії.

4. Засоби збору, зберігання та обробки інформ-традиційні технічні засоби (:телефон, радіо, звукопідсилювальні системи, поліграфія) та автоматизовані системи збору та обробки інформації.

5. Засоби передачі інформації (дротові, радіо, волоконно-оптичні)

Вихідною матеріальною основою роботи інформаційної системи виступають інформаційні ресурси. Ресурсами, як відомо, називають елементи економічного потенціалу, які перебувають у власності суспільства і які при необхідності можуть бути використані для досягнення конкретних цілей господарського й соціального розвитку.

Інформаційні ресурси можуть бути фіксованими й нефіксованими. Фіксовані інформаційні ресурси являють собою інформацію, закріплену на якому-небудь фізичному носії, а нефіксовані - знання, якими володіють люди (учені, фахівці, працівники), що беруть участь у суспільному виробництві та здатні передавати ці знання іншим учасникам виробничого процесу.

Об’єктом захисту виступає інформаційна система, предметом захисту інформації в інформаційній системі є інформація.

Для інформаційних систем як об’єктів безпеки властиві наступні характеристики: конфіденційність, доступність та цілісність інформації (даних) в інформаційній системі.

Конфіденційність (від лат. confidential - довір’я) - це властивість не підлягати розголошенню.

Конфіденційність інформації (даних) в інформаційній системі – це властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і (або) процесом інформаційної системи. Інформація зберігає конфіденційність, якщо дотримуються встановлені правила ознайомлення з нею.

Доступність у загальному сенсі представляється як можливість доступу до

інформаційних ресурсів при їх обробці, зберіганні та передачі.

Для інформаційної системи - це властивість ресурсу системи, яка полягає в тому, що користувач і (або) процес, який володіє відповідними повноваженнями, може використовувати ресурс відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого (малого) проміжку часу, тобто коли він знаходиться у вигляді, необхідному користувачеві, і в той час, коли він йому необхідний.

Доступність даних в інформаційній системі - це властивість даних, що полягає у можливості їхнього отримання користувачем або програмою. Визначається рядом факторів: можливістю працювати за терміналом, володінням паролем, знанням мови запитів та ін.

Цілісність - це внутрішня єдність, зв'язаність усіх частин інформаційних ресурсів при їх обробці, зберіганні та передачі, як одного цілого в інформаційній системі. Тобто, це стан даних, або інформаційної системи, коли дані та програми використовуються встановленим чином, що забезпечує:

– стійку роботу системи;

– автоматичне відновлення у випадку виявлення системою потенційної помилки;

– автоматичне використання альтернативних компонентів замість тих, що вийшли з ладу.

Для інформаційної системи можна розглядати такі поняття як цілісність даних, цілісність інформації, цілісність бази даних, цілісність інформаційної системи.

Цілісність даних в інформаційній системі - це стан, при якому дані, що зберігаються в системі, в точності відповідають даним у вихідних документах; властивість, що має відношення до набору даних і означає, що дані не можуть бути змінені або зруйновані без санкції на доступ. Цілісність даних вважається збереженою, якщо дані не спотворені і не зруйновані (стерті).

Семантична цілісність даних - це стан даних, коли вони зберігають свій інформаційний зміст та однозначність інтерпретації в умовах випадкових впливів.

Цілісність інформації - це властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і (або) процесом.

Цілісність бази даних - це стан бази даних, коли всі значення даних правильні в тому сенсі, що відображають стан реального світу (в межах заданих обмежень по точності та часовій узгодженості) і підпорядковуються правилам взаємного не протиріччя. Підтримка цілісності бази даних містить перевірку цілісності і відновлення з будь-якого неправильного стану, яке може бути виявлено; це входить у функції адміністратора бази даних.

Цілісність системи - це властивість системи, яка полягає в тому, що жоден її компонент не може бути усунений, модифікований або доданий з порушенням політики безпеки.

Захищена інформаційна система - інформаційна система, яка для певних умов експлуатації забезпечує безпеку (конфіденційність, цілісність) інформації, що функціонує в системі, та підтримує свою працездатність в умовах впливу на неї заданої множини загроз.

Рівні захисту інформаційних систем

Побудова надійного захисту інформаційної системи неможлива без попереднього аналізу можливих загроз безпеки системи. Цей аналіз повинен складатися з таких етапів:

– виявлення характеру інформації, яка зберігається в системі;

– оцінки цінності інформації, яка зберігається в системі;

– побудови моделі зловмисника;

– визначення та класифікації загроз інформації в системі (несанкціоноване зчитування, несанкціонована модифікація і т.д.);

– визначення затрат часу і матеріальних ресурсів на злам системи, припустимих для зловмисників;

– оцінки припустимих витрат часу, засобів і ресурсів системи на організацію її захисту.

Проблеми інформаційної безпеки вирішуються, як правило, з допомогою створення спеціалізованих систем захисту інформації, які повинні забезпечувати безпеку інформаційної системи від несанкціонованого доступу до інформаційних ресурсів. Система захисту інформації є інструментом адміністраторів інформаційної безпеки, які виконують функції із забезпечення захисту інформаційної системи і контролю її захищеності.

Система захисту інформації повинна виконувати такі функції:

– реєстрація і облік користувачів, носіїв інформації, інформаційних масивів;

– забезпечення цілісності системного та прикладного програмного забезпечення та інформації яка оброблюється;

– захист комерційної таємниці, включаючи використання сертифікованих засобів криптографічного захисту;

– створення захищеного електронного документообігу з використанням сертифікованих засобів криптографічні перетворення і електронного цифрового підпису;

– централізоване управління системою захисту інформації;

– управління доступом;

– забезпечення ефективного антивірусного захисту, тощо.

Комплекс вимог, які висуваються до системи безпеки, передбачає функціональне навантаження на кожний з наведених на рис. 1. рівнів.

Організація захисту на фізичному рівні повинна зменшити можливість несанкціонованих дій сторонніх осіб і персоналу підприємства, а також понизити вплив техногенних джерел.

Захист на технологічному рівні (програмний продукт і технічні засоби обробки інформації). Система захисту на цьому рівні повинна бути автономною, але забезпечувати реалізацію єдиної політики безпеки і будуватись на основі використання сукупності вбудованих систем захисту операційної системи і систем управління базами даних та знань.

Рис. 1. Рівні захисту інформаційної системи

На локальному рівні зорганізується розподілення інформаційних ресурсів ІС на сегменти за рівнями конфіденційності по територіальному і функціональному принципах, а також виділяється в окремий сегмент засоби обробки конфіденційної інформації. Підвищенню рівня захищеності сприяє обмеження і мінімізація кількості точок входу/виходу (точок взаємодії) між сегментами, створення надійної оболонки по периметру сегментів і інформаційної системи в цілому, організація захищеного обміну інформацією між сегментами.

На мережевому рівні зорганізується захищений інформаційний обмін даними між автоматизованими робочими місцями, а також створюється надійна оболонка фізичного захисту периметра розташування ІС в цілому. Система захисту на цьому рівні повинна будуватись з урахуванням реалізації захисту на попередніх рівнях.

На рівні користувача повинно бути забезпечено допуск тільки авторизованих абонентів до роботи в інформаційний системі, створено захисну оболонку навколо її елементів, а також організовано індивідуальне захищене середовище діяльності кожного користувача.

Залежно від призначення і характеру задач з обробки інформації можна виділити три основні види експлуатації інформаційних систем, що мають принципове значення для складу посадовців і характеру доступу до інформації з:

– **закритим доступом** - організація - споживач використовує інформаційну систему повністю в своїх інтересах, при цьому обслуговуючий персонал, включаючи технічний і оперативний склад, є співробітниками даної організації;

– **обмеженим доступом** - організація - споживач обчислювальної системи поєднує свої інтереси з інтересами інших організацій і приватних осіб;

– **відкритим доступом** - організація - споживач обчислювальної мережі надає послуги населенню.

Назва «Система з відкритим доступом» умовна в тому значенні, що будь-яка людина може скористатися послугами даної системи. Насправді ж кожна інформаційна система має і внутрішню частину, яка стосується обробки її власної інформації, яка може бути закритою для сторонніх осіб.

Усі загрози безпеки, спрямовані проти програмних і технічних засобів інформаційної системи, впливають на безпеку інформаційних ресурсів і призводять до порушення основних властивостей інформації, яка зберігається і обробляється в системі. Як правило, загрози інформаційній безпеці розрізняються за способом їх реалізації.

Дослідження і аналіз численних випадків впливів на інформацію і несанкціонованого доступу до неї показують, що їх можна розділити на випадкові і навмисні.

Навмисні загрози можуть бути реалізовані шляхом довготривалої масованої атаки несанкціонованими запитами або вірусами тощо. Наслідки такі: руйнування (втрата) інформації, модифікація (зміна інформації на помилкову, яка коректна за формою і змістом, але має інший сенс) і ознайомлення з нею сторонніх осіб. Ціна вказаних подій може бути досить високою. Попередження зазначених наслідків в інформаційній системі є основною метою створення системи безпеки інформації, розроблення та вдосконалення існуючих методів захисту інформації.

Для вирішення поставленої задачі доцільно навести найбільш повну класифікацію загроз і шляхів їх реалізації в ІС.

Можна виділити такі основні класи загроз безпеці, які спрямовані проти інформаційних ресурсів:

– загрози конфіденційності даних і програм;

– загрози цілісності даних, програм, апаратури;

– загрози доступності даних;

– загрози відмови від виконання трансакцій.

Оцінка вразливості інформаційної системи і побудова моделі впливів припускають вивчення всіх варіантів реалізації перерахованих вище загроз і виявлення наслідків, до яких вони призводять.

Аналіз вразливостей корпоративних інформаційних систем

Корпоративна інформаційна система (КІС) - це інформаційна система, яка підтримує автоматизацію функцій управління на підприємстві (в корпорації) і постачає інформацію для прийняття управлінських рішень. У ній реалізована управлінська ідеологія, яка об'єднує бізнес-стратегію підприємства і прогресивні інформаційні технології. В загальному випадку КІС - це система з можливістю масштабування, призначена для комплексної автоматизації всіх видів господарської діяльності великих і середніх підприємств, в тому числі корпорацій, що складаються з групи компаній, які потребують єдиного управління. Об'єднує систему управління персоналом, матеріальними, фінансовими та іншими ресурсами компанії, використовується для підтримки планування і управління компанією, для підтримки прийняття управлінських рішень її керівниками. Під КІС можна розуміти управлінську ідеологію, яка об'єднує бізнес-стратегію та інформаційні технології.

До основних принципів побудови КІС належать:

- інтелектуальність (управління організацією - реєстрація та накопичення інформації);
- інтегрованість (наскрізне проходження документів через різні служби);
- модульність (можливість поетапного впровадження системи);
- доступність;
- відкритість (можливість взаємодіяти з іншими програмами);
- адаптивність (потужність механізму налаштувань).

Основні вимоги КІС:

- використання архітектури клієнт-сервер з можливістю застосування промислових СУБД;

- забезпечення безпеки методами контролю і розмежування доступу до інформаційних ресурсів;
- підтримку розподіленої обробки інформації;
- модульний принцип побудови з оперативно-незалежних функціональних блоків з розширенням за рахунок відкритих стандартів (API, COM і інші).

Корпоративні інформаційні системи діляться на наступні класи:

- ERP (Enterprise Resource Planning System);
- CRM (Customer Relationship Management System);
- MES (Manufacturing Execution System);
- WMS (Warehouse Management System);
- EAM (Enterprise Asset Management);
- HRM (Human Resource Management);
- СЕД (Системи електронного документообігу).

Підходи побудови КІС:

- орієнтація на споживача;
- процесний підхід;
- збалансована система показників (відношення клієнта до компанії, ступінь його задоволеності, інноваційний потенціал компанії і співробітників, якість бізнес-процесів та ін.);
- комплексний підхід до управління;
- системний підхід;
- адаптивне управління (вибір оптимального способу досягнення мети, це спосіб управління, при якому зберігаються незмінними цільові показники).

Головними особливостями сучасного підходу до побудови корпоративної інформаційної системи підприємства є:

- всебічний аналіз бізнес-процесів, на основі якого проводиться розробка проекту інформаційної системи і обґрунтування закладених в ньому рішень;
- використання широкої палітри сучасних методологій та інструментальних засобів моделювання та проектування систем;
- підтримка міжкорпоративного бізнесу;
- детальне опрацювання та узгодження з замовником всіх етапів розробки проекту, контрольних точок, необхідних ресурсів.

Корпоративні інформаційні системи великих компаній регулярно зазнають змін - оновлюється конфігурація обладнання, змінюється топологія мереж, з'являються нові вузли і цілі системи. Для більшості корпорацій з розподіленою інфраструктурою процес безперервного забезпечення комплексного захисту інформаційних активів стає непростим завданням через високу складності архітектури і великого числа взаємозв'язків всередині окремих підсистем. За результатами аналітики в 2019 році найбільш поширені уразливості на мережевому периметрі корпоративних інформаційних систем розподілені наступним чином:

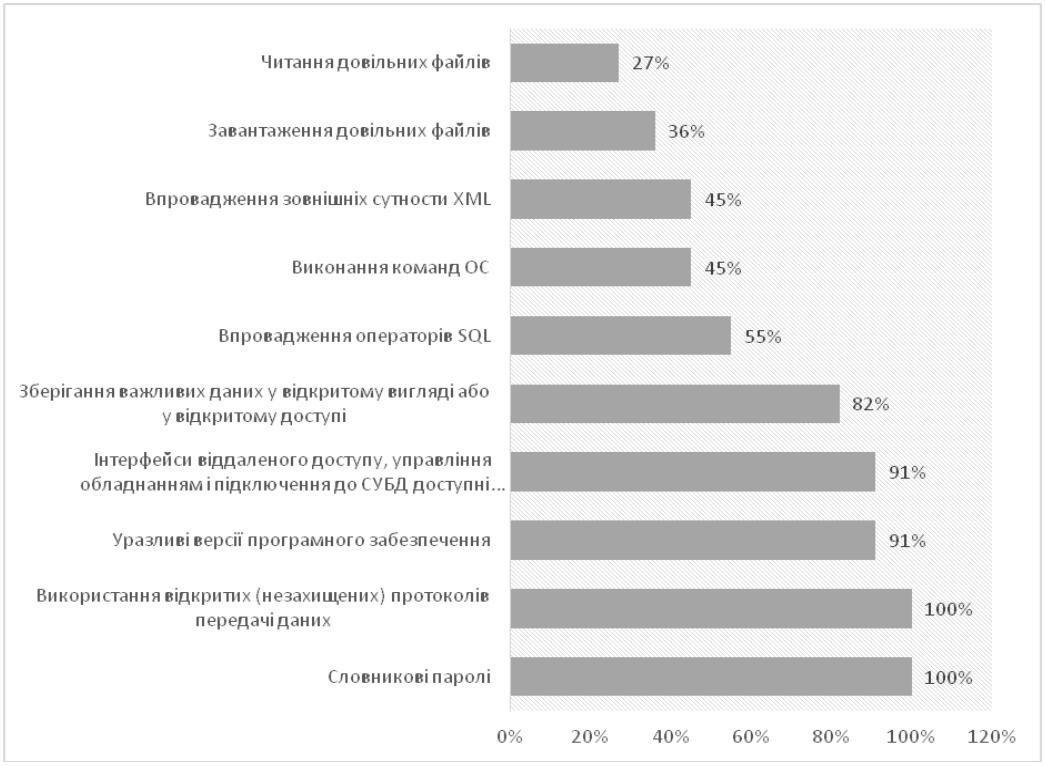

Рис. 2. Найбільш поширені уразливості на мережевому периметрі (частка систем)*

**Джерело за даними аналітики компанії Positive Technologies 2019 рік.*

Локальна обчислювальна мережа є основою функціонування будь-якої КІС. До найбільш поширених загроз інформаційної безпеки даного типу мереж належать:

10. Недоліки захисту службових протоколів, що призводять до перенаправлення трафіку і перехоплення інформації про конфігурацію мережі.
11. Словникові паролі.
12. Недостатній рівень захисту привілейованих облікових записів.
13. Зберігання важливої інформації у відкритому вигляді.
14. Недоліки захисту протоколів NBNS і LLMNR.
15. Недостатньо ефективна реалізація антивірусного захисту.
16. Використання слабких алгоритмів шифрування при зберіганні паролів.
17. Уразливі версії програмного забезпечення.
18. Надлишкові привілеї додатків або СУБД.
19. Використання відкритих (незахищених) протоколів передачі даних.

В той же час корпоративні інформаційні системи мають свої характерні вразливості інформаційної безпеки. До них можна віднести:

1. Помилки в коді веб-додатків і відсутність оновлень безпеки.
2. Недоліки конфігурування.

За даними результатів аналітики провідних компаній, які займаються інформаційною безпекою підприємств останніми роками зберігається тенденція до підвищення загального рівня захищеності мережевого периметра корпоративних інформаційних систем. В середньому, у 27% випадків фахівцям не вдається подолати мережевий периметр і отримати доступ до ресурсів внутрішньої локальної обчислювальної мережі. Дані результати пов'язані з тим, що деякі замовники регулярно проводять тестування на проникнення і усувають виявлені вразливості. Однак важливо пам'ятати, що конфігурація мережевої інфраструктури регулярно змінюється, тому тестування на проникнення необхідно проводити на регулярній

основі. Крім того, потрібно стежити за тим, які служби доступні для підключення з мережі Інтернет. Приклади подолання периметра і отримання доступу до ресурсів локальної обчислювальної мережі:

1. Тривіальна складність подолання периметра. На периметрі мережі доступний для підключення інтерфейс налагодження JDWP. Будь-який зовнішній порушник може використовувати загальнодоступний експлойт (github.com/IOActive / jdwp-shellifier) і виконати довільні команди на сервері. Використовуючи цю вразливість і надлишкові привілеї служби, вдається отримати повний контроль над сервером і доступ до ЛВС (якщо на вузлі є доступ до інтерфейсу внутрішньої мережі).

2. Низька складність подолання периметра. На тестованому вузлі виявлено веб-додаток для управління навчанням співробітників. Шляхом реєстрації нового облікового запису без підтвердження особи вдається отримати доступ до функціональності веб-додатка і завантажити веб-інтерпретатор командного рядка (веб-шелл) на сервер, що робить можливим виконання довільних команд ОС на сервері з привілеями веб-додатка. Таким чином вдається отримати доступ до ЛОМ, у випадку, коли на вузлі є доступний інтерфейс внутрішньої мережі.

3. Середня складність подолання периметра. В ході робіт по оцінці обізнаності співробітників в питаннях інформаційної безпеки була проведена масова розсилка електронних листів від внутрішньої особи з посиланням на веб-ресурс, що містить фішингову форму для введення облікових даних. Деякі співробітники ввели облікові дані в помилкову форму аутентифікації. Отримані облікові дані можуть бути використані для несанкціонованого доступу до ресурсів системи. Для використання фішингових сценаріїв атак як мінімум необхідно зареєструвати власний домен і розробити неправдиву форму аутентифікації. Більш того, важливо зробити фішинговий ресурс максимально наближеним по дизайну сторінки до того ресурсу, яким звик користуватися співробітник. Для цього необхідно проводити додаткові розвідувальні дії, що істотно підвищує складність реалізації атаки.

Після отримання доступу до внутрішньої мережі зовнішній зловмисник має можливості для розвитку атаки і отримання повного контролю над всією IT-інфраструктурою або окремими критично важливими системами.

У більшості випадків для отримання максимальних привілей в критично важливих системах від імені внутрішнього порушника досить підібрати обліковий запис з привілеями локального адміністратора на одній з робочих станцій або на сервері ЛОМ, запустити спеціалізоване ПО і отримати у відкритому вигляді облікові записи локальних адміністраторів інших вузлів. Даний вектор атаки можна розвивати аж до отримання облікових даних адміністраторів доменів.

За результатами звітів компаній, діяльністю яких є аналіз та захист інформаційної безпеки підприємств, перше місце в рейтингу найбільш поширених уразливостей захисту внутрішніх ресурсів належить недолікам захисту протоколів мережевого і канального рівнів, що призводить до перенаправлення трафіку і перехоплення інформації про конфігурацію мережі. Кожна досліджувана система містила різні недоліки захисту службових протоколів, таких як ARP, STP, BOOTP, CDP. У кожному з проектів, де проводився аналіз мережевого трафіку ЛОМ, було виявлено відсутність механізмів захисту від атак ARP Cache Poisoning. Даний недолік може бути використаний для прослуховування трафіку в мережі і проведення атак типу «людина посередині». В ході успішної реалізації атаки

порушник може перехоплювати конфіденційну інформацію, змінювати дані в процесі передачі і блокувати мережеву взаємодію.

На другому місці серед уразливостей внутрішніх мереж знаходиться використання словникових паролів. Третє місце - недостатній рівень захисту привілейованих облікових записів.

Таким чином, можна зробити наступні висновки: сучасні корпоративні інформаційні системи мають велику кількість уразливостей з боку зовнішніх і внутрішніх зловмисників, а реалізація їх атак не вимагає серйозної кваліфікації. Досить низьким є рівень захищеності бездротових мереж і рівень обізнаності користувачів в питаннях інформаційної безпеки.

Необхідно також відзначити, що вектори атак на корпоративні інфраструктури ґрунтуються на експлуатації поширених уразливостей і недоліків, для усунення яких, як правило, досить застосувати базові принципи забезпечення інформаційної безпеки:

- використовувати сувору парольну політику;
- захищати привілейовані облікові записи;
- не зберігати конфіденційну інформацію у відкритому вигляді або у відкритому доступі;
- обмежити число доступних для підключення на мережевому периметрі інтерфейсів мережевих служб;
- захищати або відключати в локальній обчислювальній мережі протоколи канального або мережевого рівня, які не використовуються та розділяти мережу на сегменти;
- мінімізувати привілеї користувачів і служб;
- регулярно оновлювати ПЗ і встановлювати оновлення безпеки ОС;
- для своєчасного виявлення атак використовувати SIEM-системи;
- для захисту веб-додатків використовувати web application firewalls;
- проводити регулярні тренінги, спрямовані на підвищення обізнаності користувачів в питаннях інформаційної безпеки (при цьому важливо проводити і оцінку ефективності таких тренінгів);
- регулярно проводити тестування на проникнення для своєчасного виявлення нових векторів атак і перевірки вжитих заходів захисту на практиці.

При цьому важливо забезпечити всі ці заходи в комплексі, тільки тоді захист буде ефективним, а витрати на різні дорогі рішення виявляться виправданими.

Основні принципи захисту інформації

Захист інформації від НСД є складовою частиною загальної проблеми забезпечення захисту інформації в ІС. В загальному випадку комплекс програмно-технічних засобів та організаційних рішень по захисту інформації в ІС реалізується в рамках системи захисту інформації від НСД, яка умовно складається з таких чотирьох підсистем:

– управління доступом до ІС, до її послуг та ресурсів;
– реєстрація і облік користувачів, послуг, інформаційних ресурсів;
– криптографічного захисту;
– забезпечення цілісності інформаційних потоків, інформаційних ресурсів та

програмного забезпечення.

Закриття каналів несанкціонованого отримання інформації повинно починатися з контролю доступу користувачів до ресурсів ІС. Ця задача вирішується на основі ряду принципів:

Принцип виправданості доступу - користувач повинен мати достатню «форму допуску» для отримання інформації того рівня конфіденційності, що він вимагає, і ця інформація дійсно необхідна йому для виконання його виробничих функцій.

Принцип достатньої глибини контролю доступу. Засоби захисту інформації повинні включати механізми контролю доступу до всіх видів інформаційних і програмних ресурсів ІС, які у відповідності з принципом виправданості доступу слід розмежовувати між користувачами.

Принцип розмежування інформаційних потоків. Для попередження порушення інформаційної безпеки, яке, наприклад, може мати місце при запису секретної інформації на несекретні носії і в несекретні файли, її передачі програмам і процесам, які не призначені для обробки секретної інформації, а також при передачі секретної інформації по незахищених каналах зв'язку, необхідно здійснювати відповідне розмежування інформаційних потоків.

Принцип персональної відповідальності. Кожний користувач повинен нести персональну відповідальність за свою діяльність в системі, включаючи будь-які операції з конфіденційною інформацією і можливі порушення її захисту.

Принцип цілісності засобів захисту. Даний принцип передбачає, що засоби захисту інформації в ІС повинні чітко виконувати свої функції у відповідності з переліченими принципами і бути ізольованими від користувачів, а для свого супроводу повинні включати спеціальний захищений інтерфейс для засобів контролю, сигналізації про спроби порушення захисту інформації і впливу на процеси в системі.

Реалізація перелічених принципів здійснюється з допомогою так званого «монітору звернень», який контролює будь-які запити до даних чи програм з боку користувачів (чи їх програм) за установленими для них видами доступу до цих даних і програм. Схематично такий монітор можна представити у вигляді, показаному на рис. 3.

Рис. 3. Структура монітору звернень

Практичне створення монітору звернень, як видно з наведеного рисунку, передбачає розробку конкретних правил розмежування доступу у вигляді так званої моделі захисту інформації.

Найбільш розповсюджена модель отримала назву - багаторівнева модель захисту Белла Ла Падула. Основою цієї моделі є поняття рівня конфіденційності (форми допуску) і категорії (прикладної області) суб'єкта і об'єкта доступу. На основі присвоєних кожному суб'єкту і об'єкту доступу конкретних рівнів і категорій в моделі визначаються їх рівні безпеки, а потім встановлюється їх взаємодія. При цьому в моделі приймається, що один рівень безпеки домінує над іншим тоді і тільки тоді, коли відповідний йому рівень конфіденційності більше чи дорівнює конфіденційності іншого, а множина категорій включає множину категорій другого.

Хід роботи

1. Ознайомитися з теоретичними матеріалами по темі.
2. Провести аналіз вразливостей корпоративної інформаційної системи, вказаної викладачем.
3. За результатами роботи підготувати звіт
4. Зробити висновки.

Контрольні питання

9. Що таке джерело інформації?
10. Які існують категорії джерел конфіденційної інформації?
11. Дайте визначення інформаційної системи.
12. Які складові має інформаційна система?
13. Що є об'єктом та предметом захисту інформації?
14. Розкрийте поняття «цілісність».
15. Розкрийте поняття «доступність».
16. Розкрийте поняття конфіденційності інформації.
17. Назвіть основні напрями забезпечення безпеки інформації.
18. Назвіть основні характеристики інформаційної системи.
19. Розкрийте зміст моделі системи захисту інформації.
20. Якими показниками може бути оцінено якість розподілу доступу?
21. Назвіть основні принципи та рівні захисту інформаційних систем.
22. Які існують основні принципи захисту інформації?

Практичне занятя № 5

2 години

Тема заняття: Інформаційно-комунікаційні системи та комп'ютерні мережі.

Мета заняття: ознайомитися з різновидами побудови комп'ютерних мереж та основними завданнями захисту інформації у мережі.

Теоретичні відомості

Впровадження та інтеграція інформаційно-комунікаційних систем та мереж потребує високого рівня технічних і соціальних вимог до якості інформаційних ресурсів та безпосередньо до систем передачі, обробки і відображення даних. Базовими властивостями інформаційних ресурсів є їх цілісність, конфіденційність і доступність. Випадкові, а також штучні завади, спотворюють інформаційні потоки, які надходять від джерела повідомлення до споживача, що призводить до втрати

цілісності даних. Спотворення основних властивостей інформації при її передачі чи обробці, веде до неякісних процедур прийняття рішень або зовсім унеможливлює цей процес у всіх сферах діяльності розвинутого суспільства.

Базовою функцією інформаційних систем передачі даних є здійснення процесів оперативного та надійного обміну інформацією між джерелом повідомлення та його користувачем, а також у забезпеченні ефективності функціонування інформаційної системи мінімізації часу передачі інформації за умов зростання її обсягів при фіксованій вірогідності інформаційного потоку. Інформаційні системи передачі даних є базовою платформою сучасного процесу інформатизації суспільства, що активно впливає на стан національної безпеки держави.

Інформаційно-комунікаційна система (та комп'ютерна мережа, ІКСМ) - це інтегрований комплекс організаційно-технічних заходів та взаємопов'язаних і взаємоузгоджених комунікаційних, програмно-апаратних і програмних компонентів, які забезпечують достовірну передачу інформації від джерела повідомлення до споживача.

Вивчення мережі в цілому потребує знання принципів роботи та характеристик її окремих елементів: комп'ютерів, комунікаційного устаткування, операційних систем, мережних додатків і т. ін.

Багаторівневою моделлю інформаційно-комунікаційної системи називається повний інтегрований комплекс середовища та комунікаційних й програмно-апаратних засобів, що застосовується з метою достовірної передачі інформаційних потоків від джерела повідомлення до споживача.

Перший (апаратний) рівень - основа будь-якої мережі, створена стандартизованими комп'ютерними платформами й використовувана з метою автоматизованої обробки даних.

Другий рівень - комунікаційне устаткування зазначеної інформаційно-комунікаційної мережі.

Не зважаючи на те, що комп'ютери і є центральними елементами обробки даних у мережах, не менш важливу роль в організації мережі відіграють комунікаційні пристрої. Кабельні системи, повторювачі, мости, комутатори, маршрутизатори й модульні концентратори - усі ці складові перетворилися з допоміжних компонентів мережі на основні як за впливом на характеристики мережі, так і за вартістю. Сьогодні комунікаційний пристрій може бути складним спеціалізованим мультипроцесором, який потрібно конфігурувати, оптимізувати й адмініструвати. Для вивчення принципів роботи комунікаційного устаткування необхідно знання великої кількості протоколів, використовуваних як у локальних, так і у глобальних мережах.

Третій рівень - операційні системи (ОС), які створюють та забезпечують програмну платформу мережі.

Від того, які концепції управління локальними та розподіленими ресурсами покладено в основу мережної ОС, залежить ефективність роботи всієї мережі. При проектуванні мережі важливо враховувати:

– оптимальність взаємодії даної операційної системи з іншими ОС мережі;

– можливість нарощувати кількість користувачів (складність мережі);

– можливість адаптації чи інсталяції на інші типи обчислювальних платформ

тощо.

Четвертий рівень - рівень мережних засобів - утворюють мережні додатки, такі як мережні бази даних, поштові системи, засоби архівації даних, системи автоматизації колективної роботи і т. ін.

Важливо уявляти діапазон можливостей, що надаються додатками для різних сфер застосування, а також знати, наскільки вони сумісні з іншими мережними додатками й операційними системами.

Мережева технологія - це узгоджений набір стандартних протоколів та програмно-апаратних засобів, що їх реалізують (наприклад, мережевих адаптерів, драйверів, кабелів і роз'ємів), достатніх для побудови та функціонування інформаційно-комунікаційної (комп'ютерної) мережі.

Однією з найбільш розвинених мережевих технологій є технологія Ethernet. Протоколи, на основі яких будується мережа певної технології (у вузькому сенсі), спеціально розроблялися для спільної роботи користувачів (абонентів), тому від розробника мережі не вимагається додаткових зусиль щодо організації її взаємодії. Іноді мережні технології називають базовими, маючи на увазі те, що на їх основі будується базис будь-якої мережі.

Головний принцип, покладений в основу Ethernet, - випадковий метод доступу до середовища передачі даних та загальних інформаційних ресурсів (CSMA/CD). Як середовище може використовуватися товстий або тонкий коаксіальний кабель, вита пара, оптоволокно або радіохвилі для передачі інформаційних потоків.

Сутність випадкового методу доступу: користувач у мережі Ethernet може передавати дані по мережі тільки тоді, коли мережа вільна, тобто коли ніякий інший користувач (комп'ютер) у даний момент не обмінюється даними. Тому важливою частиною технології Ethernet є процедура визначення доступності середовища.

При об'єднанні в мережу великої кількості користувачів постає цілий комплекс технічних та інших питань. Проектування мережі передусім передбачає в тому числі розв'язання задачі про забезпечення безпеки інформації і захищеності даних.

Захист інформації в комп'ютерних мережах

Комп'ютерна мережа - система зв'язку між двома чи більше комп'ютерами. У більш широкому розумінні комп'ютерна мережа - це система зв'язку через кабельне чи повітряне середовище, самі комп'ютери різного функціонального призначення і мережеве обладнання. Для передачі інформації можуть бути використані різні фізичні явища, як правило - різні види електричних сигналів чи електромагнітного випромінювання. Середовищами передавання у комп'ютерних мережах можуть бути телефонні кабелі, та спеціальні мережеві кабелі: коаксіальні кабелі, виті пари, волоконно-оптичні кабелі, радіохвилі, світлові сигнали. Мережа дає можливість окремим співробітникам організації взаємодіяти один з одним і звертатися до спільно використовуваних ресурсів; дозволяє їм одержувати доступ до даних, що зберігається на персональних комп'ютерах у видалених офісах, і встановлювати зв'язок з постачальниками. Мережеві операції регулюються набором правил і угод (званих мережевим протоколом), який визначає: типи роз'ємів і кабелів, види сигналів, формати даних, алгоритми роботи мережевих інтерфейсів, способи контролю та виправлення помилок, взаємодія прикладних процесів та ін.

До теперішнього часу розроблено значну кількість організаційних та

архітектурних різновидів побудови комп’ютерних мереж. Системну їх класифікацію можна здійснити за наступними критеріями:

1) за масштабом - локальні та глобальні;

2) за способом організації - централізовані і децентралізовані;

3) по топології (конфігурації) - зіркоподібні, кільцеві, шинні, змішані.

Різновиди комп’ютерних мереж по виділених значенням перерахованих критеріїв характеризуються наступним чином:

– локальні обчислювальні мережі - мережі, вузли яких розташовуються на невеликих відстанях один від одного (в різних приміщеннях однієї і тієї ж будівлі, в різних будівлях, розташованих на одній і тій же території).

– глобальні обчислювальні мережі - вузли мережі розташовані на значних відстанях один від одного (в різних частинах великого міста, у віддалених один від одного населених пунктах (які включають у себе цегляні, панельні і дерев'яні будинки), в різних регіонах країни і навіть у різних країнах).

Централізовані локальні обчислювальні мережі - мережі, в яких передбачено головний вузол, через який здійснюються всі обміни інформацією і який здійснює управління всіма процесами взаємодії вузлів.

Децентралізовані обчислювальні мережі - мережі з відносно рівноправними вузлами, управління доступом до каналів передачі даних у цих мережах розподілено між вузлами.

На основі навіть такого швидкого розгляду можливих структур обчислювальних мереж неважко зробити висновок, що для тих об'єктів (підприємств, установ, інших організацій), в яких регулярно обробляються значні обсяги інформації, найбільш доцільною буде комбінована структура комп’ютерних обчислювальних мереж.

Мережева взаємодія

Дане питання розглянемо на прикладі найбільш поширеної і визнаної еталонної моделі взаємодії відкритих систем ISO / OSI (BOC) [1].

В основу еталонної моделі покладена ідея декомпозиції процесу функціонування відкритих систем на рівнях, причому розбиття на рівні проводиться таким чином, щоб згрупувати в рамках кожного з них функціонально найбільш близькі компоненти. Крім того, потрібно, щоб взаємодія між суміжними рівнями була мінімальною, число рівнів порівняно невеликим, а зміни, вироблені в рамках одного рівня, не вимагали б перебудови суміжних.

Окремий рівень, таким чином, являє собою логічно і функціонально замкнуту підсистему, що сполучається з іншими рівнями за допомогою спеціально визначеного інтерфейсу. В рамках моделі ISO/OSI кожен конкретний рівень може взаємодіяти тільки із сусідніми. Сукупність правил (процедур) взаємодії об'єктів однойменних рівнів називається протоколом.

Еталонна модель містить сім рівнів (знизу вгору):

1. Фізичний.
2. Канальний (або передачі даних).
3. Мережевий.
4. Транспортний.
5. Сеансовий.
6. Представницький.

7. Рівень додатків.

Кожен рівень передавальної станції в цій ієрархічній структурі взаємодіє з відповідним рівнем приймаючої станції за допомогою нижчих рівнів. При цьому кожна пара рівнів за допомогою службової інформації повідомлень встановлює між собою логічне з'єднання, забезпечуючи тим самим логічний канал зв'язку відповідного рівня. За допомогою такого логічного каналу кожна пара верхніх рівнів може забезпечувати між собою взаємодію, абстрагуючись від особливостей нижніх. Іншими словами, кожен рівень реалізує строго певний набір функцій, який може використовуватися верхніми рівнями незалежно від деталей реалізації цих функцій (див. Табл.)

Таблиця. Семирівнева модель протоколів мережевого обміну ISO

№ рівня	Найменування рівня	Зміст
7	Рівень додатків	Надання послуг на рівні кінцевого користувача
6	Рівень представлення даних	Інтерпретація та стиск даних
5	Рівень сеансів	Аутентифікація та перевірка повноважень
4	Транспортний рівень	Забезпечення коректної передачі даних
3	Мережевий рівень	Маршрутизація та ведення обліку
2	Канальний рівень	Передача та прийом пакетів, визначення апаратних адрес
1	Фізичний рівень	Кабель або фізичний носій інформації

Розглянемо докладніше функціональне призначення кожного рівня.

Фізичний рівень. Фізичний рівень забезпечує електричні, функціональні та процедурні засоби встановлення, підтримки і роз'єднання фізичного з'єднання. Реально він представлений апаратурою генерації та управління електричними сигналами і каналом передачі даних. На цьому дані представляються у вигляді послідовності бітів або аналогового електричного сигналу. Завданням фізичного рівня є передача послідовності бітів з буфера відправника в буфер одержувача.

Канальний рівень. Протоколи канального рівня (або протоколи управління ланкою передачі даних) займають особливе місце в ієрархії рівнів: вони служать сполучною ланкою між реальним каналом, що забезпечує безпомилкову передачу даних. Цей рівень використовується для організації зв'язку між двома станціями за допомогою наявного (зазвичай ненадійного) каналу зв'язку. При цьому станції можуть бути пов'язані декількома каналами.

Протокол канального рівня повинен забезпечити наступне:

– незалежність протоколів вищих рівнів від використовуваного середовища передачі даних;

– кодонезалежність переданих даних;

– вибір якості обслуговування при передачі даних.

На цьому рівні дані представляються кадром, який містить інформаційне поле, а також заголовок і доповнення (трейлер), що привласнюються протоколом.

Заголовок містить службову інформацію, використовувану протоколом канального рівня приймаючої станції і служить для ідентифікації повідомлення, правильного прийому кадрів, відновлення і повторної передачі у разі помилок і т. д. Доповнення містить перевірочне поле, що служить для корекції та виправлення помилок, внесених каналом. Завдання протоколу канального рівня - складання кадрів, правильна передача і прийом послідовності кадрів, контроль послідовності кадрів, виявлення та виправлення помилок в інформаційному полі (якщо це необхідно).

Мережевий рівень. Мережевий рівень надає транспортному рівню набір послуг, головними з яких є наскрізна передача блоків даних між передавальною і приймальною станціями (тобто, виконання функцій маршрутизації та ретрансляції) і глобальне адресування користувачів. Іншими словами, знаходження одержувача за вказаною адресою, вибір оптимального (в умовах даної мережі) маршруту та доставка блоку повідомлення за вказаною адресою.

Таким чином, на кордоні мережевого і транспортного рівнів забезпечується незалежність процесу передачі даних від використовуваних середовищ за винятком якості обслуговування. Під якістю обслуговування розуміється набір параметрів, що забезпечують функціонування мережевої служби, що відображає робочі (транзитна затримка, коефіцієнт невиявлених помилок та ін.) Та інші характеристики (захист від НСД, вартість, пріоритет та ін.). Система адрес, використовувана на мережевому рівні, повинна мати ієрархічну структуру і забезпечувати наступні властивості: глобальну однозначність, маршрутну незалежність і незалежність від рівня послуг.

На мережевому рівні дані представляються у вигляді пакету, який містить інформаційне поле і заголовок, який присвоюється протоколом. Заголовок пакета містить керуючу інформацію, яка вказує адресу відправника, можливо, маршрут і параметри передачі пакета (пріоритет, номер пакета в повідомленні, параметри безпеки, максимум ретрансляції та ін.). Розрізняють такі види мережевої взаємодії:

– з встановленням з'єднання - між відправником та одержувачем спочатку за допомогою службових пакетів організовується логічний канал (відправник - відправляє пакет, одержувач - чекає отримання пакету плюс взаємне повідомлення про помилки), який роз'єднується після закінчення повідомлення або у разі невиправної помилки. Такий спосіб використовується протоколом X.25;

– без встановлення з'єднання (дейтаграмний режим) - обмін інформацією здійснюється за допомогою дейтаграм (різновид пакетів), незалежних один від одного, які приймаються також незалежно один від одного і збираються в повідомлення на приймальній станції. Такий спосіб використовується в архітектурі протоколів DARPA.

Транспортний рівень. Транспортний рівень призначений наскрізної передачі даних через мережу між кінцевими користувачами - абонентами мережі. Протоколи транспортного рівня функціонують тільки між кінцевими системами.

Основними функціями протоколів транспортного рівня є розбивка повідомлень або фрагментів повідомлень на пакети, передача пакетів через мережу і збір пакетів. Вони також виконують такі функції: відображення транспортного адреси в мережі, мультиплексування і розщеплення транспортних сполучень, міжкінцеве управління потоком і виправлення помилок. Набір процедур протоколу транспортного рівня залежить як від вимог протоколів верхнього рівня, так і від характеристик мережевого рівня.

Найбільш відомим протоколом транспортного рівня є TCP (Transmission Control Protocol), використовуваний в архітектурі протоколів DARPA і прийнятий в якості стандарту. Він використовується в якості високонадійного протоколу взаємодії між комп'ютерами в мережі з комутацією пакетів.

Протоколи верхніх рівнів. До протоколів верхніх рівнів відносяться протоколи **сеансового, представницького і прикладного рівнів**. Вони спільно виконують одну задачу - забезпечення сеансу обміну інформацією між двома прикладними процесами, причому інформація повинна бути представлена в тому вигляді, який зрозумілий обом процесам. Тому зазвичай ці три рівня розглядають спільно. Під прикладним процесом розуміється елемент кінцевої системи, який бере участь у виконанні одного або декількох завдань з обробки інформації. Зв'язок між ними здійснюється за допомогою прикладних об'єктів - елементів прикладних процесів, що беруть участь в обміні інформацією. При цьому протоколи верхніх рівнів не враховують особливості конфігурації мережі, каналів і засобів передачі інформації.

Протоколи представницького рівня надають послуги за погодженням синтаксису передачі (правил, які задають подання даних при їх передачі) і конкретним уявленням даних в прикладній системі. Іншими словами, на представницькому рівні здійснюється синтаксичне перетворення даних від виду, використовуваного на прикладному рівні, до виду, використовуваному на інших рівнях (і навпаки).

Прикладний рівень, будучи самим верхнім у еталонної моделі, забезпечує доступ прикладних процесів до середи взаємодії відкритих систем. Основним завданням протоколів прикладного рівня є інтерпретація даних, отриманих з нижніх рівнів, і виконання відповідних дій у кінцевій системі в рамках прикладного процесу. Зокрема, ці дії можуть полягати в передачі управління певним службам операційної системи разом з відповідними параметрами.

Крім того, прикладний рівень можуть надавати послуги з ідентифікації і аутентифікації партнерів, встановленню повноважень для передачі даних, перевірці параметрів безпеки, управлінню діалогом та ін.

Для мереж передачі даних реальну небезпеку представляють наступні **загрози.**

1. Прослуховування каналів, тобто запис і подальший аналіз всього потоку повідомлень. Прослуховування в більшості випадків не помічається легальними учасниками інформаційного обміну.

2. Умисне знищення або спотворення (фальсифікація) повідомлень в мережі, а також включення в потік помилкових повідомлень. Неправдиві повідомлення можуть бути сприйняті одержувачем як справжні.

3. Присвоєння зловмисником своєму вузлу або ретранслятору чужого ідентифікатора, що дає можливість отримувати або відправляти повідомлення від чужого імені.

4. Навмисний розрив лінії зв'язку, що призводить до повного припинення доставки всіх (або тільки, обраних зловмисником) повідомлень.

5. Впровадження мережевих вірусів. Передача по мережі тіла вірусу з його подальшою активізацією користувачем віддаленого або локального вузла.

Відповідно до цього специфічні **завдання захисту в мережах передачі даних** полягають у наступному.

1. Аутентифікація однорівневих об'єктів, що полягає у підтвердженні

справжності одного або декількох взаємодіючих об'єктів при обміні інформацією між ними.

2. Контроль доступу та захист від несанкціонованого використання ресурсів мережі.

3. Маскування даних, що циркулюють в мережі.

4. Контроль і відновлення цілісності всіх даних, що знаходяться в мережі.

5. Арбітражне забезпечення або захист від можливих відмов від фактів відправки, прийому або змісту відправлених або прийнятих даних.

Таким чином, стосовно до різних рівнів семирівневого протоколу передачі даних **завдання захисту інформації в мережі** можуть бути конкретизовані наступним чином.

1. Фізичний рівень - контроль електромагнітних випромінювань ліній зв'язку та пристроїв, підтримка комутаційного обладнання в робочому стані. Захист на даному рівні забезпечується за допомогою екрануючих пристроїв, генераторів перешкод, засобів фізичного захисту передавального середовища.

2. Канальний рівень - збільшення надійності захисту (при необхідності) за допомогою шифрування переданих по каналу даних. У цьому випадку шифруються всі передані дані, включаючи службову інформацію.

3. Мережевий рівень - найбільш вразливий рівень з точки зору захисту. На ньому формується вся маршрутизована інформація, відправник і одержувач фігурують явно, здійснюється управління потоком.

Крім того, протоколами мережевого рівня пакети обробляються на всіх маршрутизаторах, шлюзах та інших проміжних вузлах. Майже всі специфічні мережеві порушення здійснюються з використанням протоколів даного рівня (читання, модифікація, знищення, дублювання, переорієнтація окремих повідомлень або потоку в цілому, маскування під інший вузол і ін.). Захист від таких загроз здійснюється протоколами мережевого і транспортного рівнів і за допомогою засобів криптографічного захисту. На даному рівні може бути реалізована вибіркова маршрутизація.

4. Транспортний рівень - здійснює контроль за функціями мережевого рівня на приймальному і передавальному вузлах (на проміжних вузлах протокол транспортного рівня не функціонує). Механізми транспортного рівня перевіряють цілісність окремих пакетів даних, послідовності пакетів, пройдений маршрут, час відправлення і доставки, ідентифікацію та аутентифікацію відправника і одержувача та інші функції. Всі активні загрози стають видимими на даному рівні.

Гарантом цілісності переданих даних є криптозахист як самих даних, так і службової інформації. Ніхто, крім тих, що мають секретний ключ одержувача і / або відправника, не може прочитати або змінити інформацію таким чином, щоб зміна залишилася непоміченою.

Аналіз трафіку забезпечується передачею повідомлень, що не містять інформацію, які, однак, виглядають як реальні повідомлення. Регулюючи інтенсивність цих повідомлень в залежності від обсягу переданої інформації, можна постійно домагатися рівномірного трафіку. Проте всі ці заходи не можуть захистити від загрози знищення, переорієнтації або затримки повідомлення. Єдиним захистом від таких порушень може бути паралельна доставка дублікатів повідомлення по інших шляхах.

5. Протоколи верхніх рівнів забезпечують контроль взаємодії прийнятої або переданої інформації з локальною системою. Протоколи сеансового і представницького рівня функцій захисту не виконують. У функції захисту протоколу прикладного рівня входить управління доступом до певних наборів даних, ідентифікація і аутентифікація певних користувачів, а також інші функції, які визначаються конкретним протоколом. Більш складними ці функції є у разі реалізації повноважної політики безпеки в мережі.

Безпека інформаційних ресурсів у ІКСМ на базі ISO/IEC

Наприкінці 90-х рр. Британський Інститут Стандартів (BSI) розробив національний стандарт щодо управління інформаційною безпекою, який потім одержав назву BS 7799, або «Старий Британський стандарт». При розробці стандарту ставилося завдання забезпечення державних та комерційних організацій інструментом для створення і реалізації ефективних систем інформаційної безпеки на основі сучасних інформаційних технологій та методів менеджменту. У 2000 р. на базі BS 7799 був розроблений новий стандарт, що визнаний міжнародним, під назвою «International Standard ISO/IEC 17799 (Information technology - Code of practice for information security management)».

ISO (Міжнародна Організація по Стандартизації) і IEC (Міжнародна Електротехнічна Комісія) формують спеціалізовану систему всесвітньої стандартизації. Національні органи, які є членами ISO або IEC, беруть участь у розробці Міжнародних Стандартів через технічні комітети, створені відповідною організацією з метою роботи з специфічними областями технічної діяльності. Технічні комітети ISO й IEC співпрацюють в областях взаємного інтересу. Інші урядові й неурядові міжнародні організації, пов’язані з ISO й IEC, також беруть участь у цій роботі. На даний час сформовано цілий ряд стандартів ISO/IEC з урахуванням їх впровадження у галузь «Інформаційної безпеки»: ISO/IEC 15408 «Критерії оцінювання безпеки інформаційних технологій», а також стандарти серії 27000 – 27001:2005, 27005:2008, 27006:2007, 27003, 27004, 27007, 27022, 27033.

У даному розділі розглянемо стандарт ISO/IEC 17799, як найбільш поширений та загальний стандарт для організації системи захисту інформаційних ресурсів та сервісних послуг в інформаційно-комунікаційних системах та мережах.

Стандарт ISO/IEC 17799 - це модель системи менеджменту, яка визначає загальну організацію процесів, класифікацію даних, системи доступу, напрямки планування, відповідальність співробітників, використання оцінки ризику і т. ін. в контексті інформаційної безпеки.

У процесі впровадження стандарту створюється так звана система менеджменту інформаційної безпеки, мета якої - скорочення матеріальних втрат, пов’язаних з порушенням безперервності бізнесу компанії.

Основна ідея стандарту - допомогти комерційним та державним господарським організаціям вирішити достатньо складне завдання: забезпечення надійного захисту інформаційних ресурсів та організація ефективного доступу до даних й процесу їх обробки згідно визначених послуг та вимог.

Основна структура стандарту

Структура стандарту дозволяє вибрати засоби управління, які мають відношення до конкретної організації або сфери відповідальності у середині

організації. Зміст стандарту має такі розділи:

- політика безпеки;
- організація захисту;
- класифікація ресурсів та контроль;
- безпека персоналу;
- фізична безпека та безпека навколишнього середовища;
- адміністрування комп'ютерних систем та обчислювальних мереж;
- управління доступом до систем;
- розробка та супроводження інформаційних систем;
- планування безперервної роботи організації;
- виконання вимог (відповідність законодавству).

У зв'язку з цим виділяється ряд ключових елементів управління, що подаються як фундаментальні:

- політика інформаційної безпеки;
- розподіл відповідальності за інформаційну безпеку;
- освіта та тренінг з інформаційної безпеки;
- звітність за інциденти з безпеки;
- захист від вірусів;
- забезпечення безперервності роботи;
- контроль копіювання ліцензованого програмного забезпечення;
- захист архівної документації організації;
- захист персональних даних;
- реалізація політики з інформаційної безпеки.

Як видно, поряд з елементами захисту та управління для комп'ютерів та комп'ютерних мереж, стандарт велику увагу приділяє питанням розробки політики безпеки, роботі з персоналом (прийом на роботу, навчання, звільнення з роботи), забезпеченню безперервності виробничого процесу, юридичним вимогам.

Задачі організації безпеки інформації та інформаційних ресурсів

Забезпечення безпеки інформаційних мереж - запобігання ушкодженню інформаційних активів і переривання дій, пов'язаних з реалізацією безперервного процесу бізнесу. Інформаційні ресурси та засоби обробки, поширення інформації повинні бути керовані й фізично захищені.

Повинні бути встановлені відповідні експлуатаційні процедури для захисту документів, носіїв інформації (стрічок, дисків, флешек, касет), обчислювальної техніки, даних, систем введення/виводу й системної документації, які стосуються процесів ушкодження, злодійства й несанкціонованого доступу або інших зловмисних дій.

З даної точки зору необхідно розглядати такі заходи:

- фіксація попереднього змісту інформації, яка повинна бути вилучена з організації та розташована на будь-яких носіях багаторазового користування;
- дотримання строгої авторизації всіх носіїв інформації, що видаляється із організації, а також проведення реєстрації всіх видалень для підтримки процедур аудиту;
- носії інформації повинні зберігатися в надійному, безпечному середовищі, відповідно до встановлених вимог.

Всі процедури й рівні авторизації повинні бути чітко задокументовані. Процедури обробки й зберігання інформації варто встановлювати для того, щоб захистити інформацію від неавторизованого розкриття або неправильного впровадження.

Варто встановити процедури для обробки інформації, відповідно до її класифікації у документах, обчислювальних системах, мережах, мобільних засобах зв'язку, пошті, мовній пошті, мовному зв'язку взагалі, системах з комп'ютерним поданням інформації, поштових послугах/засобах обслуговування, при використанні факсів і будь-яких інших чутливих об'єктів, наприклад, чистих чеків, рахунків.

Заходи управління обробкою й зберіганням інформації :

- обробка й маркування всіх носіїв інформації;
- обмеження доступу при ідентифікації неавторизованого персоналу;
- підтримка офіційної реєстрації авторизованих одержувачів даних;
- забезпечення впевненості в тому, що введені дані є повними та обробка завершується належним чином, а також є підтвердження виводу даних;
- захист (записаних у буфер) даних, що очікують виходу на рівень сумісний з їхньою відповідністю;
- зберігання носіїв інформації в середовищі, що відповідає специфікаціям виготовлювачів;
- відомість розподілу даних до мінімуму;
- чітке маркування всіх копій даних, пропонованих увазі авторизованого одержувача.

Системна документація може містити визначений діапазон інформації, наприклад: опис процесів додатків, процедур, структур даних, процесів авторизації тощо. Необхідно розглянути такі заходи для захисту системної документації від неавторизованого доступу та використання:

- системну документацію варто зберігати згідно з визначеною політикою безпеки та встановленими стандартами;
- список осіб, що мають доступ до системної документації, варто зводити до мінімуму, а авторизацію варто забезпечувати власникові додатків;
- системну документацію, підтримувану загальнодоступною мережею, або отриману через загальнодоступну мережу, варто захищати згідно з визначеною політикою безпеки та встановленими стандартами.

Безпека обміну інформацією й програмним забезпеченням – запобігання втрат, модифікації або неправильного чи неавторизованого вживання інформації і програмного забезпечення, що підлягає обміну між організаціями та окремими користувачами.

Обмін інформацією й програмним забезпеченням між організаціями та окремими користувачами виконується згідно з встановленими процедурами управління у відповідності чинному законодавству, стандартам або внутрішнім нормативним документам. Обміни варто виконувати на основі угод, або встановлювати внутрішні процедури й стандарти по захисту інформації й носіїв інформації при їх передачі. Дані питання є базовими для процесів безперервності бізнесу і його безпеки з урахуванням питань пов'язаних з електронним обміном даних, електронною торгівлею й електронною поштою, а також вимогами до заходів управління безпекою інформаційних систем.

Угоди обміну програмним забезпеченням повинні включати:

- обов’язки персоналу по управлінню і контролю безпекою та повідомлення про передачу, відправлення й одержання інформації;
- визначені процедури для відправника про передачу, відправлення й одержання повідомлення;
- мінімальну кількість технічних стандартів по формуванню й передачу пакетів;
- стандарти по ідентифікації кур’єра;
- відповідальність й обов’язки у випадку втрати даних;
- використання погодженої системи маркування для чутливої або критичної інформації;
- володіння інформацією й програмним забезпеченням, а також обов’язки по захисту даних, узгодження з авторським правом на програмне забезпечення й аналогічні питання;
- технічні стандарти по запису й зчитуванню інформації й програмного забезпечення;
- будь-які спеціальні засоби управління, які можуть знадобитися, для захисту чутливих об’єктів, таких як криптографічні ключі тощо.

Інформація може бути вразливою до неавторизованого доступу, неправильного вживання або спотворення під час фізичного транспортування, наприклад, при пересиланні носіїв інформації через поштову службу або через кур’єра.

Хід роботи

1. Ознайомитися з теоретичними матеріалами по темі.
2. Проаналізувати завдання захисту інформації в конкретній мережі та стосовно конкретного протоколу передавання даних семирівневої моделі ISO/OSI, заданих викладачем.
3. За результатами роботи підготувати звіт
4. Зробити висновки.

Контрольні питання

1. Розкрийте поняття інформаційно-комунікаційної системи.
2. Назвіть рівні інформаційно-комунікаційних мереж.
3. Сутність випадкового методу доступу до ресурсів системи.
5. Які основні типи протоколів використовуються в моделі ISO/OSI?
6. Перерахуйте основні функції рівнів моделі ISO/OSI.
7. Дайте визначення поняттю «IP адреса»?
8. Назвіть основні вимоги для проектування більшості мережних проектів.
9. Основні завдання захисту інформації в мережі?
10. Різновиди побудови комп’ютерних мереж?
11. Що повинні включати угоди обміну програмним забезпеченням?
12. Назвіть заходи управління обробкою й зберіганням інформації.

Практичне заняття № 6

2 години

Тема заняття: Забезпечення інформаційної безпеки України.

Мета заняття: ознайомитися із основними реальними та потенційними загрозами інформаційній безпеці України.

Теоретичні відомості

Необхідною умовою нормального існування і розвитку кожного суспільства є захищеність від зовнішніх і внутрішніх загроз, стійкість до спроб зовнішнього тиску, як здатність протистояти таким спробам і нейтралізувати загрози, що виникають, так і забезпечувати такі внутрішні і зовнішні умови існування країни, які гарантують можливість стабільного і всебічного прогресу суспільства і його громадян. Для характеристики цього стану використовується поняття національної безпеки.

Під **національною безпекою** слід розуміти стан захищеності життєво важливих національних інтересів від внутрішніх і зовнішніх загроз.

Система національних інтересів України визначається сукупністю основних інтересів особи, суспільства, держави і охоплює всі сфери їх діяльності: політичну, економічну, військову, екологічну, інформаційну, науково-технічну, соціальну та інші. Тому в змісті поняття "Національна безпека" можна виділити різні структурні елементи (компоненти), до основних з яких відносяться політична, економічна, військова, екологічна і інформаційна безпека.

Суть **політичної безпеки** полягає в здатності науки створити політичну систему, що забезпечує баланс інтересів різних соціальних груп; самостійно вирішувати питання державного устрою; проводити незалежну внутрішню і зовнішню політику.

Під **економічною безпекою** розуміється стан нації, при якому вона може суверенно, без зовнішнього втручання визначати шляхи і форми свого економічного розвитку.

Військова безпека полягає в можливості забезпечення національної безпеки засобами озброєного насильства. Насамперед військова безпека характеризується здатністю нації стримувати агресію або протидіяти їй.

Екологічна безпека полягає в наявності безпечного місця існування, що забезпечує нормальну життєдіяльність людини. Баланс компонентів у системі "населення - навколишнє середовище - природні ресурси" є гарантом життєздатності людського суспільства.

Інформаційна безпека - стан захищеності інформаційних ресурсів від внутрішніх і зовнішніх загроз, здатних завдати збитку інтересам особи, суспільства, держави (національним інтересам).

Оскільки в умовах інформатизації країни, розвитку інформаційних технологій, інформаційні ресурси формуються у всіх сферах діяльності, і насамперед в політичній, військовій, економічній, науково-технічній, інформаційну безпеку слід розглядати як комплексний **показник** національної безпеки. Цим визначається її важливе місце і одна **з провідних ролей** в системі національної безпеки країни в сучасних умовах. Недарма існує ряд прислів'їв і виразів, що характеризують місце інформації в конкурентній боротьбі і в тактиці військових дій: "Хто володіє інформацією - той володіє ситуацією", "перемагає той, хто більш інформований про супротивника " та інші.

Основними загрозами інформаційній безпеці є витікання інформації і порушення її цілісності.

Забезпечення інформаційної безпеки здійснюється в рамках забезпечення

національної безпеки.

Національна безпека досягається проведенням єдиної державної політики в області забезпечення безпеки, системою заходів економічного, політичного і іншого характеру, адекватних загрозам життєво важливих інтересів особи, суспільства і держави.

Законодавчу основу забезпечення національної безпеки представляють Конституція України, закони України, укази Президента України, ухвали і розпорядження Кабінету Міністрів України, інші нормативно-правові акти державних органів влади і управління, прийняті у межах їх компетенції в даній сфері; міжнародні договори і угоди визнані Україною.

Основним суб'єктом забезпечення безпеки є **держава,** що здійснює функції в цій області через органи законодавчої, виконавчої і судової влади.

До основних **об'єктів** безпеки відносяться: **особа - її права і свободи; суспільство - його матеріальні і духовні цінності; держава - її конституційний лад, суверенітет і територіальна цілісність**.

Громадяни, суспільні і інші організації і об'єднання є суб'єктами безпеки, володіють правами і обов'язками по участі в забезпеченні безпеки.

Принципи забезпечення безпеки.

Основними принципами забезпечення безпеки є:

– законність;

– дотримання балансу життєво важливих інтересів особи, суспільства і держави;

– взаємна відповідальність особи, суспільства і держави по забезпеченню безпеки;

– інтеграція з міжнародними системами безпеки.

Систему національної безпеки утворюють:

– органи законодавчої, виконавчої і судової влади;

– державні, суспільні і інші організації і об'єднання;

– громадяни, що беруть участь в забезпеченні безпеки відповідно до закону;

– законодавство, що регламентує стосунки у сфері безпеки;

– сили забезпечення безпеки.

Для безпосереднього виконання функцій забезпечення національної безпеки в системі виконавчої влади створюються і діють сили і засоби забезпечення національної безпеки.

Сили забезпечення безпеки включають:

а) Збройні сили України; Службу безпеки України;Внутрішні війська; Прикордонні війська України; органи і підрозділи Міністерства внутрішніх справ України; військові підрозділи Міністерства України із питань надзвичайних ситуацій і в справі захисту населення від наслідків Чорнобильської катастрофи; інші військові формування, створені відповідно до Конституції України, які виконують свої функції в даній сфері згідно чинному законодавству;

б) органи, що забезпечують безпечне ведення робіт в промисловості, енергетиці, на транспорті і в сільському господарстві;служби забезпечення безпеки засобів зв'язку і інформації;митні служби; природоохоронні служби; органи охорони здоров'я населення і інші державні органи забезпечення безпеки, які діють згідно

законодавству України.

Для розгляду питань внутрішньої і зовнішньої політики в області забезпечення безпеки, стабільності і правопорядку створено Центральне управління Служби безпеки України, яке відповідає за стан державної безпеки, координує і контролює діяльність інших органів Служби безпеки України.

Центральне управління Служби безпеки України видає положення, накази, розпорядження, інструкції, дає вказівки, обов'язкові для виконання в системі Служби безпеки України. Вказані акти не підлягають виконанню, якщо в них встановлюються непередбачені законодавством додаткові повноваження органів і співробітників Служби безпеки України або антиконституційні обмеження прав і свобод громадян.

У межах своєї компетенції Центральне управління Служби безпеки України вносить Президентові України пропозиції що до видання актів по питаннях збереження державної таємниці, обов'язкової для виконання органами державного управління, підприємствами, установами, організаціями і громадянами.

Забезпечення інформаційної безпеки здійснюється в рамках забезпечення національної безпеки України. Воно передбачає наявність державної системи захисту інформації і законодавства в цій області.

Основні реальні та потенційні загрози інформаційній безпеці України

До головних чинників, що впливають на стан морально-ідеологічної стабільності та безпеки в Україні, належать:

- відсутність цілісної системи інформаційно-аналітичного забезпечення органів державної влади й управління;
- руйнування інтелектуального потенціалу, неготовність системи освіти до підтримання процесів випереджувального розвитку держави;
- повільність процесів усвідомлення прошарком колишньої радянської партійно-господарчої номенклатури, наукової й творчої інтелігенції. паростками нової буржуазії свого місця в суспільстві та формування власне української еліти, що призводить до неможливості сформувати керівними колами зрозумілої й привабливої для суспільства національної ідеї;
- низький загальний рівень розвитку інформаційної інфраструктури, що не виключає ймовірність експансії іноземних компаній на ринку інформаційних послуг; руйнування національного інформаційною простору та виникнення можливості його використання в антидержавних інтересах;
- недостатній професійний, інтелектуальний і творчий рівень вітчизняних виробників інформаційного продукту та послуг, їхня не конкурентоздатність на світовому інформаційному ринку;
- інформаційна експансія провідних іноземних держав, розроблення й використання ними, міжнародними чи вітчизняними злочинними організаціями різних сучасних способів безпосереднього підриву;
- малоконтрольована діяльність окремих політичних сил, ЗМІ та осіб, спрямована на руйнування моральних цінностей, підрив морального й фізичного здоров'я нації; використання ЗМІ з позицій, протилежних інтересам громадян, політичних і громадських організацій, держави:

- втрата довіри до влади з боку значної частини населення внаслідок поширення компромату, застосування «брудних» політичних технологій, особливо під час виборчих кампаній;

- конкурентна боротьба за володіння ЗМІ, процес їхньої монополізації й концентрації інформаційної та політичної влади;

- маніпулювання громадською думкою (шляхом дезінформації, перекручування даних, замовчування правдивих відомостей тощо).

Відсутність цілісної системи інформаційно-аналітичного забезпечення органів влади та управління значно ускладнює прийняття ними зважених. науково обґрунтованих рішень, що породжує конфліктні ситуації у владних структурах і суспільстві.

Недостатнє інформаційно-аналітичне забезпечення діяльності характерне для всіх державних органів - як на центральному, так і на регіональному рівнях. Владні структури не мають достатніх можливостей завчасно прогнозувати розвиток подій у державі та навколо неї, належним чином враховувати сприятливі й обмежувати несприятливі фактори, що визначають результативність прийнятих політичних рішень, здійснювати планування навіть на середньострокову перспективу.

Організація роботи інформаційно-аналітичних підрозділів дотепер не має системного характеру, а в періоди чергових скорочень чисельності державних органів діяльність деяких таких підрозділів взагалі припиняється.

Руйнування інтелектуального потенціалу, неготовність системи освіти до підтримання процесів випереджувального розвитку країни призводить до того, що з огляду на рівень розвитку цієї галузі за кордоном і той факт, що багато держав світу приділяють особливу увагу інформаційній безпеці (створенню спеціальних органів і підрозділів для ведення інформаційних війн тощо). Україна й досі не має достатньої кількості кваліфікованих фахівців. які б змогли на належному рівні ефективно протидіяти інформаційній активності іноземних партнерів щодо її інформаційного простору.

Сучасне українське суспільство, зокрема соціальний прошарок, який має репрезентувати так звану національну українську еліту, поки що перебуває в стані морально-психологічного скніння (відчуваються наслідки ідеологічних диверсій часів холодної війни), ідеологічного й політичного розколу. При цьому процес пошуку загальнонаціональних єднальних моральних та ідеологічних основ стратегії розвитку суспільства відбувається в умовах постійної жорсткої ідеологічної боротьби між іноземними конкурентами за геостратегічні позиції та вплив на правлячі кола України.

Низький загальний рівень інформаційної інфраструктури сприяє експансії іноземними компаніями ринку інформаційних послуг, що створює сприятливі умови для перерозподілу ефірного часу на користь іноземних програм, окремі з яких «засмічують» український інформаційний простір своїм баченням подій, пропагують власний спосіб життя та традиції, тим самим деструктивно впливаючи на суспільство й державу, руйнуючи морально-етичні основи генофонду української нації.

Недостатній професійний, інтелектуальний і творчий рівень вітчизняного виробника інформаційного продукту та послуг, його не конкурентоздатність не лише на світовому ринку, а й в Україні, призводить до того, що українська аудиторія

надає перевагу російським, американським, ізраїльським, польським, німецьким та іншим іноземним телесеріалам, розважальним й інформаційно-аналітичним програмам.

Недостатній контроль держави за дотриманням законів України політичними силами, ЗМІ й окремими особами, які займаються підприємницькою діяльністю в інформаційній сфері, спричиняє непоодинокі випадки надання ефірного часу теле- та радіопрограмам, спрямованим на руйнування моральних цінностей, свідомості української нації, підривання морального й фізичного здоров'я громадян.

У цьому випадку свідомо чи несвідомо ЗМІ створюють додатковий негативний вплив на психіку населення, «готуючи» його до проведення інших заходів прихованого вигідного іноземного впливу.

Втрата довіри до влади з боку значної частини населення відбувається, як уже зазначалося, внаслідок застосування «брудних» політичних технологій. Нині в Україні досить поширена практика оприлюднення «замовних» статей з метою дискредитації окремих громадян і посадових осіб, про яких свідомо розголошуються неправдиві чи конфіденційні відомості. Неправдива інформація і так званий компромат активно поширюються через Інтернет. Для цього навіть створюються спеціалізовані веб-сайти. Розмішена на них інформація поширюється дуже швидко і може завдати моральної чи політичної шкоди громадянам України.

Потенційні можливості для поширення конфіденційної інформації про особу (без її згоди) мають відповідні банки даних, сформовані в довідкових службах, житлово-експлуатаційних конторах, бібліотеках, різних державних органах, лікарнях та інших установах. Наявність таких відомостей створює передумови для протиправних дій, зокрема шантажу громадян.

Нав'язування особі, суспільству бажаних іноземній стороні рішень у життєво важливих сферах суспільної та державної діяльності відбувається шляхом застосування великого арсеналу сил і засобів від ЗМІ до звичайних благодійних організацій, культурних обмінів між державами, а також різних місіонерських структур, що поширюють нетрадиційні релігійні вірування чи окультно-містичні традиції.

Ще одним чинником, який впливає на стан забезпечення інформаційної безпеки, є конкурентна боротьба за володіння ЗМІ та процеси їх монополізації й концентрації інформаційної та політичної влади. В нинішніх умовах боротьба за вплив в електронних і друкованих мас-медіа, за контроль над кінокомпаніями, видавництвами та інформаційними агентствами спричиняє їх зосередження у руках однієї особи чи обмеженого кола людей. Саме це призводить до концентрації влади над споживачами, які одночасно є й виборцями, над політичними партіями та громадськими організаціями, профспілковими об'єднаннями (їм може бути надана підтримка, або з ними боротимуться, або зовсім обійдуть увагою), над іншими видавцями, котрих можна загнати в глухий кут та журналістами, на яких можна «натиснути». Злиття ЗМІ та виникнення монополістичних об'єднань призводить до:

- обмеження можливостей отримання інформації;
- здійснення впливу на свободу дій політичних партій:
- вигідного впливу на діяльність великих і малих видавництв.

Загрози національній безпеці України в інформаційній сфері - сукупність умов та факторів, які становлять небезпеку життєво важливим інтересам держави,

суспільства й особи у зв'язку з можливістю негативного інформаційного впливу на свідомість і поведінку громадян, а також інформаційні ресурси й інформаційно-технічну інфраструктуру.

Основними реальними та потенційними **загрозами інформаційній безпеці України** є:

1) *у зовнішньополітичній сфері:*

- поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України;
- прояви комп'ютерної злочинності, комп'ютерного тероризму, що загрожують стабільному та безпечному функціонуванню національних інформаційно-телекомунікаційних систем;
- зовнішні негативні інформаційні впливи на суспільну свідомість і засоби масової інформації, а також Інтернет;

2) у сфері державної безпеки:

- негативні інформаційні впливи, спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності й недоторканності кордонів України;
- використання засобів масової інформації, Інтернету для пропаганди сепаратизму за етнічною, мовною, релігійною й іншими ознаками;
- несанкціонований доступ до інформаційних ресурсів органів державної влади;
- розголошення інформації, яка становить державну та іншу передбачену законодавством таємницю, а також конфіденційної інформації, що є власністю держави;

3) у воєнній сфері:

- порушення встановленого регламенту збирання, оброблення й передавання інформації з обмеженим доступом в органах військового управління та на підприємствах оборонно-промислового комплексу України;
- несанкціонований доступ до інформаційних ресурсів, незаконне збирання та використання інформації з питань оборони;
- реалізація програмно-математичних заходів із метою порушення функціонування інформаційних систем у сфері оборони України;
- перехоплення інформації в телекомунікаційних мережах, радіоелектронне глушіння засобів зв'язку та управління;
- інформаційно-психологічний вилив на населення України, у тому числі особовий склад військових формувань, із метою послаблення їх готовності до оборони держави та погіршення іміджу військової служби;

4) у внутрішньополітичній сфері:

- недостатня розвиненість інститутів громадянського суспільства, недосконаліть партійно-політичної системи, непрозорість політичної та громадської діяльності, що створює передумови для обмеження свободи слова, маніпулювання суспільною свідомістю;
- негативні інформаційні впливи, в тому числі із застосуванням спеціальних засобів, на індивідуальну та суспільну свідомість;
- поширення суб'єктами інформаційної діяльності викривленої, недостовірної та упередженої інформації;

5) в економічній сфері:

- відставання вітчизняних наукоємних і високотехнологічних виробництв, особливо у сфері телекомунікаційних засобів і технологій;

- недостатній рівень інформатизації економічної сфери, зокрема кредитно-фінансової системи, промисловості, сільського господарства, сфери державних закупівель;

- несанкціонований доступ, порушення встановленого порядку роботи з інформаційними ресурсами в галузях національної економіки, викривлення інформації в таких ресурсах;

- використання не ліцензованого програмного забезпечення, засобів і комплексів оброблення інформації:

- недостатній рівень розвитку національної інформаційної інфраструктури;

6) у соціальній та гуманітарній сферах:

- відставання України від розвинутих держав за рівнем інформатизації соціальної та гуманітарної сфер, насамперед освіти, охорони здоров'я, соціального забезпечення, культури;

- недодержання прав людини і громадянина на отримання інформації, необхідної для захисту їх соціально-економічних прав;

- поширення в ЗМІ не властивих українській культурній традиції цінностей і способу життя, культу насильства, жорстокості, порнографії, зневажливого ставлення до людської й національної гідності;

- тенденція до витіснення з інформаційного простору та молодіжної культури українських мистецьких творів, народних традицій і форм дозвілля;

- послаблення суспільно-політичної, міжетнічної та міжконфесійної єдності суспільства;

- відставання розвитку українського кінематографу, книговидання, книго розповсюдження й бібліотечної справи від рівня розвинутих держав;

7) у науково-технічній сфері:

- зниження наукового потенціалу в галузі інформатизації та зв'язку;

- низька конкурентоспроможність вітчизняної інформаційної продукції на світовому ринку;

- відтік за кордон наукових кадрів та суб'єктів права інтелектуальної власності;

- недостатній захист від несанкціонованого доступу до інформації внаслідок використання іноземних інформаційних технологій і техніки;

- неконтрольована експансія сучасних інформаційних технологій, що створює передумови технологічної залежності України;

8) в екологічній сфері:

- приховування, несвоєчасне надання інформації або надання недостовірної інформації населенню про надзвичайні екологічні ситуації чи надзвичайні ситуації техногенного та природного характеру;

- недостатня надійність інформаційно-телекомунікаційних систем збору, обробки й передачі інформації в умовах надзвичайних ситуацій;

- низький рівень інформатизації органів державної влади, що унеможливлює здійснення оперативного контролю та аналізу стану потенційно небезпечних об'єктів і територій, завчасного прогнозування й реагування на надзвичайні ситуації.

Діяльність органів виконавчої влади у сфері забезпечення інформаційної безпеки України має бути зосереджена на конструктивному поєднанні діяльності

держави, громадянського суспільства та людини за трьома головними напрямами:

- інформаційно-психологічному, зокрема щодо забезпечення конституційних прав і свобод людини й громадянина, створення сприятливого психологічного клімату в національному інформаційному просторі для затвердження загальнолюдських та національних моральних цінностей;
- технологічного розвитку, зокрема стосовно розбудови та інноваційного оновлення національних інформаційних ресурсів, впровадження новітніх технологій створення, оброблення та поширення інформації;
- захисту інформації, зокрема щодо забезпечення конфіденційності, цілісності й доступності інформації, в тому числі технічного захисту інформації в національних інформаційних ресурсах від кібернетичних атак.

Стан та перспективи розвитку інформаційної безпеки України

Інформаційна безпека є одним із видів національної безпеки. Відповідно до законодавства України, інформаційна безпека має таке визначення: "стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації".

Інформаційна безпека означає:

- законодавче формування державної інформаційної політики;
- створення відповідно до законів України можливостей досягнення інформаційної достатності для ухвалення рішень органами державної влади, громадянами та об’єднаннями громадян, іншими суб’єктами права в Україні;
- гарантування свободи інформаційної діяльності та права доступу до інформації у національному інформаційному просторі України;
- всебічний розвиток інформаційної структури;
- підтримка розвитку національних інформаційних ресурсів України з урахуванням досягнень науки і техніки та особливостей духовно-культурного життя народу України;
- створення і впровадження безпечних інформаційних технологій;
- захист права власності всіх учасників інформаційної діяльності в національному просторі України;
- збереження права власності держави нестратегічні об’єкти інформаційної інфраструктури України;
- охорону державної таємниці, а також інформації з обмеженим доступом, що є об’єктом права власності або об’єктом лише володіння, користування чи розпорядження державою;
- створення загальної системи охорони інформації, зокрема охорони державної таємниці, а також іншої інформації з обмеженим доступом;
- захист національного інформаційного простору України від розповсюдження спотвореної або забороненої для поширення законодавством України інформаційної продукції;

– встановлення законодавством режиму доступу іноземних держав або їх представників до національних інформаційних ресурсів України та порядок використання цих ресурсів на основі договорів із іноземними державами;

– законодавче визначення порядку поширення інформаційної продукції зарубіжного виробництва на території України.

Державна політика інформаційної безпеки визначається пріоритетністю національних інтересів, системою небезпек і загроз та здійснюється шляхом реалізації відповідних доктрин, стратегій, концепцій і програм в інформаційній сфері відповідно до чинного законодавства.

У Законі України «Про основи національної безпеки України» визначено основні напрямки державної політики з питань національної безпеки в інформаційній сфері. До них належать:

– забезпечення інформаційного суверенітету України;

– вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері,

– наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну;

– активне залучення засобів масової інформації до боротьби з корупцією, зловживанням службовим становищем, іншими явищами, які загрожують національній безпеці України;

– забезпечення неухильного дотримання конституційного права громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції;

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

Для формування збалансованої державної політики та ефективного проведення комплексу узгоджених заходів щодо захисту національних інтересів в інформаційній сфері створення розвиненого і захищеного інформаційного середовища слугує організація функціонування системи інформаційної безпеки, складовими компонентами якої є національні інтереси в інформаційній сфері, загрози та небезпеки цим інтересам, сама інформаційна безпека як інструмент зі створення сприятливих умов для їх реалізації, які в сукупності становлять об’єкт управління органами державного управління, систему забезпечення інформаційної безпеки, тобто суб’єкт управління, більше того, основні напрямки політики національної безпеки в інформаційній сфері, а також внутрішнє та зовнішнє середовище. Інформаційна безпека забезпечується комплексом заходів системи забезпечення національної безпеки України, що включає сукупність державних органів, громадських організацій, посадових осіб та окремих громадян.

Правову основу забезпечення інформаційної безпеки України становлять Конституція України, закони України «Про основи національної безпеки України», «Про інформаційну безпеку України», «Про доступ до публічної інформації», інші

закони та інформативно-правові акти, а також ратифіковані або парафовані Україною Договір про безпеку і співробітництво в Європі, Договір «Відкрите небо», Угода про партнерство і співробітництво між європейським співтовариством і Україною, Додатковий протокол до Європейської конвенції про інформацію щодо іноземного законодавства, які зобов'язують країни-учасниці здійснювати багатосторонній обмін інформацією, потребують створення загальнодержавних механізмів зберігання та споживання отриманої інформації в національних інтересах.

Лише після революції Гідності питанням інформаційної безпеки приділяється більше уваги. Указом Президента України було оприлюднене рішення Ради національної безпеки і оборони України від 28 квітня 2014 р. «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України». Було передбачено у місячний термін розробити і внести на розгляд Верховної Ради України законопроекти про внесення змін до деяких законів України щодо протидії інформаційній агресії іноземних держав, передбачивши механізм протидії негативному інформаційно-психологічному впливу, зокрема шляхом заборони ретрансляції телевізійних каналів, а також запровадження для іноземних засобів масової інформації, системи інформування та захисту журналістів, які працюють у зоні збройних конфліктів, вчинення терористичних актів, при ліквідації небезпечних злочинних груп.

У місячний термін також було передбачено за участю Національного інституту та інших органів розробити проект Стратегії розвитку інформаційного простору України і проект стратегії кібернетичної безпеки України, а також розробити комплексні заходи організаційного, інформаційного і роз'яснювального характеру щодо всебічного висвітлення заходів із реалізації державної політики у сфері забезпечення інформаційної безпеки, а також посилення контролю за додержанням законодавства з питань інформаційно-психологічної та кібернетичної безпеки.

В листопаді 2014 р. було створено Міністерство інформаційної політики. При Міністерстві в процесі спілкування з представниками громадськості була створена Експертна Рада, метою якої стала розробка Стратегії інформаційної політики України, Концепції інформаційної безпеки України та Державної програми розвитку інформаційного простору України.

До пріоритетних напрямків забезпечення інформаційної безпеки України можна зарахувати:

– створення законодавчої та нормативної бази;

– здійснення моніторингу інформаційної безпеки України;

– стандартизація, сертифікація та ліцензування діяльності у сфері забезпечення інформаційної безпеки України;

– удосконалення та розвиток державної інформаційної інфраструктури з урахуванням вимог інформаційної безпеки України;

– удосконалення системи освіти, навчання та виховання з урахуванням вимог інформаційної безпеки України та Закону України «Про державну мову»;

– розробка міжрегіональних, державних та міждержавних програм розвитку системи інформаційної безпеки України.

На сучасному етапі інтеграційних процесів України до Європейського Союзу особливого значення набуває проблема інформаційного забезпечення політики

європейської інтеграції. Завданням інформаційної політики постала необхідність забезпечення вирішення двох основних завдань:

1. Забезпечення загальнонаціональної підтримки курсу інтеграції України в Європейський Союз широкими колами громадськості, створення про європейської більшості в суспільстві.

2.Донесення до урядів і громадськості країн-членів Європейського Союзу об'єктивної інформації про Україну, її досягнень на шляху реформ, створення позитивного іміджу України.

На шляху до вирішення цих завдань постають такі проблеми, які можна вирішити шляхом:

1. Проведення широкомасштабної інформаційної роз'яснювальної компанії серед населення України.

2. Здійснення іноземного просування України в країнах Європейського Союзу.

Проведення планомірного інформування громадськості з питань європейської інтеграції відповідає пріоритетним напрямам Програми інтеграції України до Європейського Союзу. Для забезпечення підтримки політики європейської інтеграції України серед української громадськості необхідно запровадити системи ефективних заходів інформування та освіти суспільства, налагодити механізм співпраці державних органів із засобами масової інформації з метою ефективного використання інформації, яка надходить від центральних органів виконавчої влади, забезпечити прозорість у прийнятті відповідних рішень органів виконавчої влади, налагодити постійний зворотний зв'язок.

Заходи мають охоплювати усі сфери діяльності виконавчої влади. Серед основних заходів, які здійснюються, можна виділити такі освітні заходи:

− розроблення Національної програми перепідготовки й навчання державних службовців центральних, регіональних та місцевих органів влади, спрямованої на поглиблення знань про європейську інтеграцію, забезпечення розуміння цілей інтеграції до Європейського Союзу, його основних інституцій, процесу ухвалення рішень, вміння вести переговори, використовувати європейські інформаційні ресурси, покращення володіння хоча б однією з основних європейських мов;

− інформування молоді з питань інтеграції України до ЄС;

− започаткування у вищих навчальних закладах освітніх програм із інтеграції України до ЄС.

Не менше значення мають видавничі заходи:

− підготовка та видання енциклопедії, словників, серії довідників про ЄС (його історію, законодавство, про держави-члени ЄС), листівок;

− розроблення методичних та довідкових матеріалів на допомогу викладачам, працівникам органів виконавчої влади і органів місцевого самоврядування, присвячених питанням європейської інтеграції;

− виготовлення буклетів, інших пропагандистських матеріалів із висвітленням європейської інтеграції.

Належне місце в інформаційній політиці з питань європейської інтеграції займають комунікативні заходи:

− проведення зустрічей членів Уряду з політиками, представниками центральних, регіональних ЗМІ, громадськістю;

– організація семінарів, брифінгів для представників засобів масової інформації;

– забезпечення виступів керівників у регіонах з окремих питань інтеграції України до Європейського Союзу;

– проведення інтерв'ю, прес-конференцій з питань євроінтеграції;

– організація культурних масових заходів: проведення виставок, конференцій, акцій, форумів, показ високоякісної європейської продукції;

– створення інформаційних центрів із надання населенню інформаційних та консультативних послуг із питань євроінтеграції;

Важливі завдання реалізації інформаційної політики з питань євроінтеграції стоять перед ЗМІ, зокрема:

– підготовка низки телевізійних проектів, програм, передач, репортажів із країн-членів ЄС та держав-кандидатів на вступ до ЄС про досвід європейської інтеграції, про нові можливості, перспективи, наслідки;

– залучення українських мас-медіа як друкованих, так і електронних, телебачення, радіо, інформаційних агентств до висвітлення різних аспектів української політики та внутрішнього життя через призму інтеграції до ЄС;

– розповсюдження через ЗМІ презентаційних та довідкових матеріалів із питань європейської інтеграції України;

– забезпечення участі керівників міністерств, інших центральних органів виконавчої влади в теле- і радіо передачах із метою роз'яснення політики України з питань європейської інтеграції;

– створення веб-сторінок органів виконавчої влади, присвячених питанням європейської інтеграції, та забезпечення розміщення в Інтернеті повідомлень у рамках європейських процесів;

– проведення Інтернет-конференцій із залученням зацікавлених міністерств, інших центральних органів виконавчої влади.

Виконання цих заходів дасть змогу поліпшити знання суспільства про сутність європейської інтеграції, специфіку функціонування ЄС, подолати психологічний пострадянський бар'єр суспільної думки стосовно нової системи європейських координат й інтеграційних перспектив, забезпечити всебічну підтримку Уряду українським суспільством. За цього важливого значення набувають знання про ЄС та виховання молодих людей у дусі спільних європейських цінностей та ідеалів. Звичайно, виконання цих усіх заходів потребує значних фінансових витрат.

Високою буде ефективність від організації просування України в країнах Європейського Союзу та від розроблення структурної програми просування України на міжнародному рівні в процесі інтеграції до ЄС. Український імідж за кордоном має суттєвий вплив на реалізацію цілей української зовнішньої політики у напрямку інтеграції до ЄС. Дуже важливим є формування позитивного національного іміджу, зокрема в країнах-членах Європейського Союзу. Україна має переконати європейську громадськість, насамперед чиновників Європейської Комісії, що вона гідна посісти чільне місце в стабільній демократичній Європі. Україна зацікавлена в лібералізації зовнішньоекономічних зв'язків з іншими країнами-членами ЄС. Для того, щоб співпрацювати з ними та формувати зону вільної торгівлі, що сприятиме інтенсифікації господарських взаємовідносин, активному обміну капіталом,

товарами, послугами, робочою силою, необхідно вирішити багато проблем, одна з яких – забезпечити європейську громадськість повною та вичерпною інформацією про інтеграційну політику України. Від кращого розуміння європейським співтовариством української політики, соціальної сфери, культури тощо залежить місце та роль України. Від кращого розуміння європейським співтовариством української політики, соціальної сфери, культури тощо залежить місце та роль України на світовій арені. Успіх переговорів з Європейським Союзом, рівень прийняття європейською громадськістю намірів України щодо входження в ЄС залежить також від результативної діяльності у напрямку просування України серед країн-членів. Для цього теж повинні слугувати відповідні заходи та повинні бути визначені індикатори їх результативності.

В умовах, коли Україна відстоює свій євроінтеграційний курс, проти України розпочато неоголошену війну з боку Російської Федерації. Складовою частиною цієї війни є контрпропаганда, яка ведеться проти України – справжня інформаційна війна. За останніми даними зараз проходить інформаційна операція на Сході України. Ворог намагається створити розкол між силовими структурами України та волонтерами, між силовими структурами і населення, скеровуються зусилля на зрив мобілізації тощо.

У зв’язку з посиленням негативного зовнішнього впливу на інформаційний простір України, що загрожує розмиванню суспільних цінностей і національної ідентичності, недостатніми залишаються обсяги вироблення конкурентного національного інформаційного продукту. Наближається до критичного стан безпеки інформаційно-комп’ютерних систем в галузі державного управління, фінансової і банківської сфери, енергетики, транспорту, внутрішніх та міжнародних комунікацій.

Забезпечення сприятливих зовнішніх умов для розвитку та безпеки держави передбачає забезпечення інформаційної безпеки при інтеграції до структур глобального інформаційного суспільства.

Отже, у сучасних умовах важливою складовою національної безпеки є інформаційна безпека України, що є станом захищеності національних інтересів у інформаційній сфері.

Хід роботи

1. Ознайомитися з теоретичними матеріалами по темі.
2. Проаналізувати стан безпеки інформаційно-комп’ютерних систем в галузі державного управління, фінансової і банківської сфери, енергетики, транспорту, внутрішніх та міжнародних комунікацій.
3. За результатами роботи підготувати звіт
4. Зробити висновки.

Контрольні питання

1. Що розуміється під "інформаційною безпекою України"?
2. Яке її місце в системі національної безпеки України?
3. Основні напрями політики інформаційної безпеки України?
4. Найважливіші завдання в області інформаційної безпеки?
5. Які відомства регулюють правові стосунки в області захисту інформації?
6. У яких сферах проявляються основні реальні та потенційні загрози безпеці України?

7. Охарактеризуйте загрози інформаційній безпеці України у воєнній сфері.
8. Охарактеризуйте загрози інформаційній безпеці України в економічній сфері.
9. Охарактеризуйте загрози інформаційній безпеці України у в екологічній сфері.

Практичне заняття № 7

2 години

Тема заняття: Система та політика забезпечення інформаційної безпеки України. Інформаційна безпека України у сфері прав і свобод людини.

Мета заняття: ознайомитися із політикою забезпечення інформаційної безпеки України та вимогами до інформаційної безпеки України у сфері прав і свобод людини.

Теоретичні відомості

Відсутність системи забезпечення інформаційної безпеки унеможливлює надійне забезпечення не лише інформаційної, а й національної безпеки. Головне призначення цієї системи полягає у досягненні цілей національної безпеки в інформаційній сфері, а отже основною функцією даної системи є забезпечення збалансованого існування інтересів особи, суспільства і держави в інформаційній сфері. Система забезпечення інформаційної безпеки України (СЗІБ) створюється і розвивається відповідно до Конституції України та інших нормативно-правових актів, що регулюють суспільні відносини в інформаційній сфері. Основу даної системи складають органи, сили та засоби забезпечення інформаційної безпеки, які вживають систему адміністративно-правових, інформаційно-аналітичних, організаційно-управлінських, та інших заходів, спрямованих на забезпечення стійкого функціонування системи державного управління. Формування СЗІБ має відбуватись за усвідомлення необхідності функціонування механізму балансу інтересів усієї системи державного управління в інформаційній сфері. Зазначимо, що за роки незалежності в Україні лише закладено основи для формування системи забезпечення інформаційної безпеки. Так, певним чином можна говорити про напрацювання великого масиву нормативно-правових актів, де визначені основні повноваження державних органів в інформаційній сфері.

Нормативно-правові засади побудови, поточної діяльності та розвитку системи забезпечення інформаційної безпеки України на сьогодні складають: Конституція України, Закон України «Про основи національної безпеки України», інші законодавчі та нормативно-правові акти, що регулюють суспільні відносини в інформаційній сфері.

Нормативно-правове підґрунтя має досить розвинений характер, оскільки більшість норм відповідають міжнародним стандартам, принципам і нормам забезпечення прав і свобод людини та громадянина, зокрема права на свободу слова, отримання та поширення інформації. Водночас, не сформованість нормативно-правової бази щодо регулювання суспільних відносин в сфері національної безпеки, відповідним чином негативно впливає на можливість формування достатньої і ефективно діючої нормативно-правової бази з питань забезпечення національної безпеки в інформаційній сфері. У Законі України «Про основи національної безпеки України» визначено дев'ять основних напрямів державної політики національної безпеки в різних сферах життєдіяльності. До однією з них належить інформаційна,

що дає усі підстави стверджувати, що інформаційна безпека є вагомою складовою національної.

У найбільш загальному плані під системою забезпечення інформаційної безпеки будемо розуміти систему інформаційно-аналітичних, теоретико-методологічних, адміністративно-правових, організаційно-управлінських, спеціальних та інших заходів, спрямованих на забезпечення стійкого розвитку об'єктів інформаційної безпеки, а також інфраструктури її забезпечення. Безперечно, можна довго дискутувати з приводу того чи іншого терміну, можна пропонувати численні варіанти, водночас змістовними вони будуть лише тоді, коли будуть визначені основи формування і функціонування СЗІБ. Основами формування і функціонування системи забезпечення інформаційної безпеки є:

- комплексне визначення поняття інформаційної безпеки та її складових елементів, світоглядне та концептуальне закріплення у концепції, доктрині, програмах, планах та інших документах;
- формування і діяльність оптимальної структури системи інформаційної безпеки, аналіз функціонування її окремих елементів, організація функціонування даної системи в цілому;
- формування єдиного методологічного підходу, а також вироблення і прийняття єдиного цілісного і узгодженого законодавства з питань інформаційної безпеки;
- створення чіткого механізму, метою якого була б координація діяльності елементів системи забезпечення інформаційної безпеки на усіх рівнях державного управління;
- підготовка і забезпечення найкращими професійними кадрами всіх складових елементів підсистеми інформаційної безпеки.

За наявності даних основ можна говорити про їх системну взаємодію, яка забезпечить створення і функціонування чіткої і надійної СЗІБ.

Відповідно до основ формування можна виокремити **основні функції системи забезпечення інформаційної безпеки України.**

1. Створення та забезпечення діяльності державних та недержавних органів та організацій - елементів системи забезпечення інформаційної безпеки, що включає:

- розроблення адміністративно-правових засад для побудови та функціонування системи інформаційної безпеки (доктрини інформаційної безпеки, організаційної та функціональної структури системи);
- системне забезпечення діяльності елементів системи: інформаційне, аналітичне, адміністративно-правове, матеріально-технічне, кадрове, ресурсне забезпечення усієї системи державного управління.

2. Управління системою інформаційної безпеки - здійснення свідомого цілеспрямованого впливу суб'єкта управління на загрози та небезпеки, внутрішні та зовнішні чинники, що впливають на стан інформаційної безпеки:

- розроблення на підставі доктрини інформаційної безпеки конкретних планів та технологій забезпечення інформаційної безпеки відповідно до потреб кожного рівня державного управління;
- здійснення прогнозування, планування, організації, регулювання та контролю усією системою інформаційної безпеки та окремими її елементами;

- оцінка результативності дій, витрат на проведення заходів щодо забезпечення інформаційної безпеки.

3. Здійснення планової та оперативної діяльності щодо забезпечення інформаційної безпеки:

- визначення інтересів органів державного управління в інформаційній сфері та їх пріоритетності відповідно до державної інформаційної політики;
- діагностування загроз та небезпек, виявлення джерел їх виникнення, а також прогнозування можливих наслідків у разі настання із відпрацюванням відповідних превентивних заходів.

4. Міжнародне співробітництво в сфері інформаційної безпеки:

- 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 розв'язання проблем інформаційної безпеки з урахуванням національних інтересів України;
- участь у роботі керівних, виконавчих та забезпечуючих підрозділів цих структур (організацій), спільне проведення планових та оперативних заходів.

Звичайно, що перелік функцій не є вичерпним, водночас за їх наявності можна говорити про формування певної підсистеми, мета функціонування якої корелюватиме із загальною метою функціонування системи національної безпеки.

Актуальним в контексті розглядуваних проблем вбачається аналіз змісту та призначення системи забезпечення інформаційної безпеки. Забезпечення інформаційної безпеки досягається у процесі свідомої цілеспрямованої діяльності органів державного управління, по запобіганню можливого порушення їх нормального функціонування в результаті дії загроз та небезпек. Метою забезпечення інформаційної безпеки є створення нормальних умов функціонування конкретного органу державного управління, а також проведення моніторингу стану інформаційної безпеки для розроблення оптимальної моделі функціонування системи забезпечення інформаційної безпеки. Вживаючи термін «система», робиться логічний наголос на утворенні нової якості, яку складають загрози та небезпеки, суб'єкти забезпечення інформаційної безпеки. Адже структурна зв'язаність елементів системи забезпечення інформаційної безпеки є істотною її якісною характеристикою і розрив зв'язків між цими елементами може призвести до зникнення самої системи, а отже актуалізується питання забезпечення структурної єдності даної системи. Так, наприклад, захищеність Кабінету Міністрів України і незахищеність місцевої адміністрації міста Києва у своїй сукупності не утворять стан захищеності усієї системи інформаційної безпеки органів державного управління. Таким чином, суб'єкти системи забезпечення інформаційної безпеки України мають тісно взаємодіяти між собою, водночас кожний з них спеціалізується на вирішенні конкретних завдань відповідно до своєї предметної компетенції, вживаючи при цьому відповідні, визначені законом, адміністративно-правові форми та методи.

У результаті такої взаємодії зазначені суб'єкти доповнюють один одного, внаслідок чого утворюють струнку організаційно-функціональну систему, об'єднану як системою владно-розпорядчих повноважень, так і функцією по забезпеченню інформаційної безпеки. Отже, об'єктами системи забезпечення інформаційної

безпеки України є:

- інтереси органів державного управління в інформаційній сфері;
- система органів державного управління, а також їх компетентні особи і відносини між ними (суспільні відносини в інформаційній сфері);
- власне система забезпечення інформаційної безпеки України.

Мета функціонування, завдання системи забезпечення інформаційної безпеки

Мета функціонування системи забезпечення інформаційної безпеки полягає в організації управління системою інформаційної безпеки через ефективне функціонування самої системи її забезпечення. У більш загальному плані мета полягає у створенні необхідних економічних і соціокультурних умов та правових і організаційних механізмів формування, розвитку і забезпечення ефективного використання національних інформаційних ресурсів в усіх сферах життя і діяльності громадянина, суспільства й держави. Ефективність системи державного управління національними інформаційними ресурсами та їхнім захистом значною мірою визначає загальний рівень національної безпеки, а будь-які недоліки в структурі й функціонуванні системи державного управління цими процесами призводять до непоправних збитків суспільству й державі.

Головним завданням системи забезпечення інформаційної безпеки України є створення умов для організації управління системою інформаційної безпеки. До основних завдань системи забезпечення інформаційної безпеки належать:

- створення умов для забезпечення інформаційного суверенітету України;
- участь у вдосконаленні державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну;
- створення умов для активного залучення засобів масової інформації до боротьби з корупцією, зловживанням службовим становищем, іншими явищами, які загрожують національній безпеці України;
- забезпечення неухильного дотримання конституційного права громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції;
- вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України;
- забезпечення інформаційної безпеки усіх складових елементів системи державного управління;
- забезпечення інформаційно-аналітичного потенціалу країни;
- реалізація державної політики інформаційної безпеки;
- ведення активної розвідувальної, контррозвідувальної і оперативно-розшукової діяльності з метою забезпечення інформаційної безпеки для відпрацювання стратегічних, тактичних і оперативних рішень у сфері державного управління інформаційною безпекою та вироблення механізмів їх реалізації;

- виявлення, попередження і припинення розвідувальної та іншої, спрямованої на нанесення шкоди інформаційній безпеці України, діяльності спеціальних служб, а також окремих осіб чи організацій;

- виявлення, попередження і припинення інформаційного тероризму та іншої діяльності, спрямованої на підрив функціонування системи державного управління;

- моніторинг (спостереження, оцінка і прогноз) стану інформаційної безпеки у зв'язку із впливом загроз та небезпек як зсередини, так і ззовні системи державного управління;

- протидія технічному проникненню до інформаційних системи органів державного управління з метою вчинення злочинів, проведення диверсійно-терористичної та розвідувальної діяльності;

- запобігання можливої протиправної та іншої негативної діяльності суб'єктів системи забезпечення національної безпеки зсередини системи їй на шкоду;

- забезпечення збереження державної таємниці;

- організація демократичного цивільного контролю за функціонуванням системи органів державного управління тощо.

Відповідно до окресленої мети і завдань, доцільно визначити функції системи забезпечення інформаційної безпеки України. Під функціями системи забезпечення інформаційної безпеки розуміємо здійснення суб'єктами системи забезпечення інформаційної безпеки України діяльності зі створення умов для оптимального управління системою інформаційної безпеки. Серед основних функцій системи забезпечення інформаційної безпеки в умовах надзвичайної ситуації слід виділити:

- виявлення і прогнозування загроз життєво важливим інтересам об'єктів інформаційної безпеки, здійснення комплексу оперативних і довгострокових заходів для попередження та нейтралізації загроз;

- створення та підтримання напоготові сил і засобів забезпечення інформаційної безпеки; управління силами і засобами забезпечення інформаційної безпеки в умовах надзвичайної ситуації;

- здійснення системи заходів з відновлення нормального функціонування об'єктів інформаційної безпеки у регіонах, які постраждали внаслідок виникнення надзвичайної ситуації;

- участь в заходах, покликаних забезпечувати інформаційну безпеку за межами України відповідно до міжнародних договорів та угод, укладених або визнаних українською державою.

Враховуючи зазначене, **до основних функцій СЗІБ також можна віднести**:

- розроблення й прийняття політичних рішень, законодавчих і нормативно-правових актів щодо забезпечення системи управління національними інформаційними ресурсами та удосконалення механізмів реалізації правових норм чинного законодавства;

- визначення і здійснення повноважень системою органів державного управління щодо оперативного управління (володіння, розпорядження, користування) державними інформаційними ресурсами;

- розроблення і реалізація організаційних заходів і нормативно-методичного забезпечення відомчих і регіональних структур в сфері формування та використання інформаційних ресурсів за умови координації діяльності згаданих структур;

- розроблення і реалізація фінансово-економічних засад регулювання процесів формування та використання інформаційних ресурсів;

- здійснення державної реєстрації інформаційних ресурсів, забезпечення повноти створення первинних і похідних інформаційних ресурсів на засадах використання інформації, що виникає (створюється) у процесі діяльності органів державного управління;

- введення технологічно та методологічно єдиних засад формування інформаційних ресурсів за результатами діяльності органів державного управління (крім інформаційних ресурсів, що мають відомості, віднесені до державної таємниці та до іншої інформації з обмеженим доступом);

- забезпечення ефективного використання інформаційних ресурсів у діяльності органів державного управління;

- оптимізація державної політики інформатизації щодо забезпечення науково-технічних, виробничо-технологічних і організаційно-економічних умов створення та застосування інформаційних технологій, інших елементів інформаційної інфраструктури для формування, розвитку і ефективного використання інформаційних ресурсів та сприяння доступу уповноважених суб'єктів управління до світових інформаційних ресурсів, глобальних інформаційних систем;

- забезпечення функціонування ефективно діючої комплексної системи захисту інформаційних ресурсів системи органів державного управління;

- забезпечення захисту системи державного управління від хибної, спотвореної та недостовірної інформації;

- забезпечення розробки та застосування правових, організаційних і економічних механізмів стосовно форм та засобів обігу інформаційних ресурсів України (ринку інформації, інформаційних технологій, засобів обробки інформації та інформаційних послуг);

- регулювання інформаційного співробітництва, спрямованого на забезпечення рівноправного та взаємовигідного використання національних інформаційних ресурсів у процесі міжнародного обміну, здійснення єдиної державної політики наукової підтримки системи державного управління формуванням, розвитком і використанням національних інформаційних ресурсів;

- кадрове забезпечення функціонування системи державного управління національними інформаційними ресурсами; адміністративно-правове забезпечення функціонування системи державного управління;

- інформаційно-аналітичне забезпечення прийняття управлінських рішень у сфері управління інформаційними ресурсами;

- контроль за встановленим порядком і правилами формування, розвитку і використання інформаційних ресурсів;

- нагляд за додержанням законодавства в сфері формування, розвитку, використання інформаційних ресурсів та здійснення правосуддя у сфері суспільних інформаційних відносин.

У межах мети завдань та функцій постає необхідність в окресленні методів і структури системи забезпечення інформаційної безпеки України.

Політика інформаційної безпеки і її реалізація в Законодавстві України

Державна політика інформаційної безпеки реалізується в рамках політики

національної безпеки і політики інформатизації всіх сфер діяльності держави і суспільства.

Основними напрямами цієї політики є:

- забезпечення умов для розвитку і захисту всіх форм власності на інформаційні ресурси;
- формування і захист державних інформаційних ресурсів;
- створення і розвиток регіональних інформаційних систем і мереж;
- забезпечення національної безпеки у сфері інформатизації, а також забезпечення реалізації прав громадян, організацій в умовах інформатизації;
- розвиток законодавства у сфері інформаційних процесів, інформатизації і захисту інформації.

Відповідно до цих напрямів в Концепції національної безпеки визначені завдання в області інформаційної безпеки.

Найважливішими завданнями є:

- встановлення необхідного балансу між потребою у вільному обміні інформацією і допустимими обмеженнями її розповсюдження;
- вдосконалення інформаційної структури, прискорення розвитку нових інформаційних технологій і їх широке розповсюдження, уніфікація засобів пошуку, збору, зберігання, обробки і аналізу інформації з урахуванням входження України в глобальну інформаційну інфраструктуру;
- розробка відповідної нормативної правової бази діяльності органів державної влади і інших органів, завдання забезпечення інформаційної безпеки;
- розвиток вітчизняної індустрії телекомунікаційних і інформаційних засобів, їх пріоритетне в порівнянні із зарубіжними аналогами розповсюдження на внутрішньому ринку;
- захист державного інформаційного ресурсу.

Всі напрями політики захисту інформації і інформаційних ресурсів реалізовані в Законодавстві України.

Законодавство в області захисту інформації включає:

- Закон України «Про інформацію»;
- Закон України «Про державну таємницю»;
- Закон України «Про авторське право та суміжні права»;
- Закон України «Про друковані засоби масової інформації (пресу) в Україні»;
- Цивільний кодекс України;
- Кримінальний кодекс України.

В цілому розвиток законодавчої бази в області інформаційної безпеки йде по чотирьох основних напрямах:

- захист відомостей, що складають державну таємницю;
- захист конфіденційної інформації;
- захист авторського права у сфері інформатизації;
- захист права на доступ до інформації.

Основу законодавства складає закон «Про інформацію», який виражає основні напрями політики інформаційній безпеки, суть якоїв своїй основі зводиться до захисту державних інформаційних ресурсів, регулює стосунки, що виникають при формуванні і використанні інформаційних ресурсів, створенні і використанні інформаційних технологій, захисті інформації, прав суб'єктів, що беруть участь в

інформаційних процесах, а також визначає основні поняття, що використовуються в законодавстві.

Органи забезпечення інформаційної безпеки і захисту інформації

Органи забезпечення інформаційної безпеки в сукупності із законодавством утворюють державну систему інформаційної безпеки і захисту інформації.

Державна система захисту інформації включає:

- органи законодавчої, виконавчої і судової влади;
- законодавство, що регулює відносини в області захисту інформації і інформаційних ресурсів;
- нормативну правову базу по захисту інформації;
- служби (органи) захисту інформації підприємств, організацій, установ.

Органи законодавчої влади (Верховна Рада) видають закони, що регулюють стосунки в області захисту інформації.

Законодавство включає закони. Їх перелік буде розглянутий в ході вивчення тем дисципліни.

Нормативна база формується на основі нормативних правових актів в області захисту інформації, видаваних органами різних гілок влади, міністерствами, відомствами.

Основу нормативної бази складають керівні документи Держтехкомісії і стандарти, що видаються Держстандартом.

Органи виконавчої влади (Уряд) виконують закони. Для цього Уряд приймає відповідні ухвали в області захисту інформації і видає розпорядження, що є підзаконними нормативними правовими актами.

Міністерства і відомства відповідно до свого призначення розробляють і приймають ухвали і рішення, що є нормативними правовими актами свого рівня. Крім того, вони розробляють і затверджують такі нормативні акти як: положення, інструкції, правила, методичні рекомендації.

До нормативних актів цього рівня відносяться також накази і листи керівників відомств і міністерств.

До відомств, що регулюють відносини в області захисту інформації, відносяться:

- Державна службу спеціального зв’язку та захисту інформації України;
- Державна служба України з питань технічного захисту інформації;
- Держстандарт;
- Служба безпеки України;

Окрім цього в забезпеченні інформаційної безпеки беруть участь Служба зовнішньої розвідки (СЗР), Державна прикордонна служба і МВС.

Основним органом управління державної системи захисту інформації є Держтехкомісія. Відповідно до своїх функцій вона здійснює:

- координацію діяльності органів і організацій в області захисту інформації, що обробляється технічними засобами;
- організаційно-методичне керівництво діяльністю по захисту інформації в КС;
- розробку і фінансування науково-технічних програм по захисту інформації;
- затвердження нормативно-технічної документації;

- функції державного органу по сертифікації продукції по вимогах безпеки інформації;
- ліцензування діяльності підприємств по наданню послуг в області захисту інформації.

Для організації і здійснення захисту інформації в України **Держтехкомісією** розроблені Керівні документи із захисту інформації.

Держстандарт розробляє стандарти в області захисту інформації.

Органи СБУ виконують функції захисту державної таємниці.

Органи МВС ведуть боротьбу з правопорушниками в інформаційній сфері і комп'ютерними злочинами. Для цього в структурі МВС створено спеціальне управління для запобігання і розкриття комп'ютерних злочинів і захисту авторських прав.

Органи Державного митного комітету зобов'язані попереджати незаконне ввезення і вивезення з України "піратської" продукції, забезпечуючи тим самим захист авторських і патентних прав.

Керівники підприємств, організацій, установ, відповідно до своїх посадових обов'язків, при діяльності пов'язаною з інформацією, що складає державну або іншу таємницю, створюють службу (підрозділ) по захисту інформації. Для організації відповідної діяльності вони видають нормативні правові акти: накази, розпорядження; а також затверджують: інструкції, положення, правила, методичні рекомендації, пов'язані із захистом інформації і діяльністю служб захисту інформації.

Для діяльності, пов'язаної з державною таємницею, підприємство повинне мати ліцензію на цей вид діяльності, в його структуру вводиться спеціальний відділ, всі засоби захисту мають бути сертифіковані.

Судова влада здійснює нагляд і притягання до відповідальності за порушення законодавства в інформаційній сфері. У своїй діяльності суди керуються відповідними статтями КК України, ЦК України. Інформаційна безпека є важливою складовою національної безпеки України.

Методи та заходи забезпечення інформаційної безпеки України

Діяльність з забезпечення інформаційної безпеки здійснюється за допомогою різних способів, засобів і прийомів, які у своїй органічній сукупності складають методи.

Метод передбачає певну послідовність дій на підставі конкретного плану. Методи можуть значно змінюватися і варіюватися в залежності від типу діяльності, в якій вони використовуються, а також сфери застосування. Важливими методами аналізу стану забезпечення інформаційної безпеки є методи опису та класифікації.

Для здійснення ефективного захисту системи державного управління слід, по-перше, описати, а лише потім класифікувати різні види загроз та небезпек, ризиків та викликів і відповідно сформулювати систему заходів по здійсненню управління ними. У якості розповсюджених методів аналізу стану забезпечення інформаційної безпеки використовуються методи дослідження причинних зв'язків. За допомогою цих методів виявляються причинні зв'язки між загрозами, ризиками, викликами та небезпеками; здійснюється пошук причин, які стали джерелом і спричинили актуалізацію тих чи інших чинників небезпеки, а також розробляються

заходи по їх нейтралізації. У числі даних методів причинних зв'язків можна назвати наступні: метод схожості, метод відмінності, метод сполучення схожості і відмінності, метод змін, що супроводжують, метод залишків. Вибір методів аналізу стану забезпечення інформаційної безпеки залежить від конкретного рівня і сфери організації захисту.

В залежності від загрози уможливлюється завдання щодо диференціації як різних рівнів загроз, так і різних рівнів захисту. Що стосується сфери інформаційної безпеки, то у ній, зазвичай, виділяють: фізичний, програмно-технічний, управлінський, технологічний, рівень користувача, мережний, процедурний. Розглянемо дещо детальніше кожний з цих рівнів. На фізичному рівні здійснюється організація і фізичний захист інформаційних ресурсів, інформаційних технологій, що використовуються, і управлінських технологій. На програмно-технічному рівні здійснюється ідентифікація і перевірка дійсності користувачів, управління доступом, протоколювання і аудит, криптографія, екранування, забезпечення високої доступності.

На рівні управління здійснюється управління, координація і контроль організаційних, технологічних і технічних заходів на всіх рівнях управління з боку єдиної системи забезпечення інформаційної безпеки органів державного управління. На технологічному рівні здійснюється реалізація політики інформаційної безпеки за рахунок застосування комплексу сучасних автоматизованих інформаційних технологій. На рівні користувача реалізація політики інформаційної безпеки спрямована на зменшення рефлексивного впливу на суб'єктів державного управління, унеможливлення інформаційного впливу з боку соціального середовища. На рівні мережі дана політика реалізується у форматі координації дій органів державного управління, які пов'язані між собою однією метою. На процедурному рівні вживаються заходи, що реалізуються людьми. Серед них можна виділити наступні групи процедурних заходів: управління персоналом, фізичний захист, підтримання працездатності, реагування на порушення режиму безпеки, планування реанімаційних робіт.

Можна виокремити декілька **типів методів забезпечення інформаційної безпеки:**

- одноріневі методи будуються на підставі одного принципу управління інформаційною безпекою;
- багаторівневі методи будуються на основі декількох принципів управління інформаційною безпекою, кожний з яких слугує вирішенню власного завдання. При цьому приватні технології не пов'язані між собою і спрямовані лише на конкретні чинники інформаційних загроз;
- комплексні методи - багаторівневі технології, які об'єднані до єдиної системи координуючими функціями на організаційному рівні з метою забезпечення інформаційної безпеки виходячи з аналізу сукупності чинників небезпеки, які мають семантичний зв'язок або генеруються з єдиного інформаційного центру інформаційного впливу;
- інтегровані високоінтелектуальні методи - багаторівневі, багатокомпонентні технології, які побудовані на підставі могутніх автоматизованих інтелектуальних засобів із організаційним управлінням.

Загальні методи забезпечення інформаційної безпеки активно

використовуються на будь-якій стадії управління загрозами. До таких стадій належать:

- прийняття рішення з визначення області та контексту інформаційної загрози і складу учасників процесу протидії; ухвалення загальної стратегії і схеми дій в політичній, економічній і соціальній сферах життєдіяльності;
- забезпечення адекватного сприйняття загрози та небезпеки у більш низьких організаційних ланках системи державного управління;
- виділення необхідних політичних, економічних, соціальних, адміністративних і організаційних ресурсів, достатніх для реалізації програми відбиття інформаційної загрози і збереження сталого розвитку інформаційних ресурсів системи державного управління;
- трансформації результатів оцінки ризиків у відповідну політику безпеки, включаючи національну.

Специфіка методів, що використовуються, значно залежить від суб'єкта діяльності, об'єкта впливу, а також цілей, що переслідуються. Так, методи діяльності індивіда у зв'язку із його обмеженою можливістю з забезпечення інформаційної безпеки здебільшого зводяться до джерела загрози, апелювання до суспільної думки, а також до держави, яка має вживати рішучих заходів із нейтралізації інформаційних загроз. Саме суспільство частково використовує у своїй діяльності методи соціального регулювання, надання допомоги окремим індивідам і суспільним організаціям, яким спричинена шкода внаслідок виявлення загрози. Причому, на жаль, слід констатувати, що в нашій країні не на достатньому рівні усвідомлюють небезпеку саме в інформаційній сфері, немає штатних одиниць в органах державного управління по забезпеченню інформаційної безпеки, не проводиться підготовка відповідних фахівців для органів державного управління. Вельми важливим є застосування аналітичних методів пізнання і дослідження стану суспільної свідомості у сфері інформаційної безпеки.

Нині важливою умовою забезпечення інформаційної безпеки є не стільки секретність, конфіденційність інформації, скільки її доступність, цілісність, захист від загроз. Отже, система має відповідно реагувати та гарантувати ефективну діяльність у цьому напрямі. Іншим завданням захисту є забезпечення незмінності інформації під час її зберігання або передачі, тобто забезпечення її цілісності. Таким чином конфіденційність інформації, яка забезпечується за допомогою криптографічних методів не є головною вимогою при проектуванні систем захисту інформації органів державного управління. Виконання процедур крипто кодування і декодування може уповільнити передачу даних та зменшити доступ до них, через те, що працівник органу державного управління буде позбавлений можливості своєчасного та швидкого доступу до цих даних та інформації, через функціонування механізму захисту. Саме тому, забезпечення конфіденційності інформації має відповідати можливості доступу до неї. Таким чином, управління в сфері інформаційної безпеки має здійснюватися на підставі принципу доступності та безпеки. Система забезпечення інформаційної безпеки в першу чергу має гарантувати доступність і цілісність інформації, а її конфіденційність у випадку необхідності.

Здебільшого забезпечення інформаційної безпеки зводиться до того, що в системних блоках блокується доступ до флоппі-дисків і тим самим

унеможливлюється несанкціонований запис інформації. Окрім цього, системний адміністратор встановлює спеціальні програми-фільтри, що відсіюють можливість доступу до внутрішньої мережі ззовні. Можна перераховувати й інші методи захисту інформації, водночас, нині ототожнення забезпечення інформаційної безпеки із забезпеченням безпеки комп'ютерних систем є просто концептуальною помилкою. Тому не є дивиною, що на сьогодні більша частина українських банків втратила внаслідок власної недбалості чимало коштів. І характерною рисою українського суспільства є те, що жоден з банків жодного разу не визнав факту вчиненого кіберзлочину проти себе. У даному аспекті можна зауважити на ще одну проблему: зневага до вимог інформаційної безпеки та брак необхідних знань. Здебільшого під час робочого дня працівники, виконуючи свої службові обов'язки, відкривають паралельні вікна в Інтернеті, та самі, не усвідомлюючи того, відкривають доступ не лише до інформації, що зараз обробляється, а в цілому до комп'ютерної мережі усієї системи органів державного управління, починаючи від Кабінету Міністрів України, закінчуючи місцевими органами виконавчої влади.

Отже, важливим методом забезпечення інформаційної безпеки є метод розвитку. Захист інформації не обмежується технічними методами. Для ефективного забезпечення інформаційної безпеки важливим є різноманітні моделі та методи оцінки загроз та небезпек. їх варіативність занадто лабільна та залежить як від рівня розвитку тієї чи іншої цивілізації, так і від контексту оцінки, що проводиться, наявності всебічних даних по факторам загроз, алгоритму вирахування коефіцієнту імовірності настання та розміру негативних наслідків. Наявність конкретних даних з цього питання дозволяє досить точно визначити ступінь впливу інформаційної зброї, рівень загроз та небезпек. Основним методом аналізу інформаційних ризиків є кількісний та якісний аналіз, факторний аналіз та інші. Мета якісної оцінки ризиків - ранжувати інформаційні загрози та небезпеки за різними критеріями, система яких дозволить сформувати ефективну систему впливу на них. Важливим методом забезпечення інформаційної безпеки є також метод критичних сценаріїв. У зазначених сценаріях аналізуються ситуації, коли уявний супротивник паралізує систему державного управління і відповідно знижує здатність підтримувати державне управління в межах оптимальних параметрів. Причому аналіз подій в світі дає усі підстави стверджувати, що інформаційні війни стають органічною частиною політики національної безпеки багатьох розвинених країн. Також можна зазначити на метод моделювання, за допомогою якого можна проводити навчання з інформаційної безпеки. Позитивний досвід цього є у США, де на базі однієї з відомих корпорацій постійно здійснюються оперативно-дослідницькі навчання, щоб моделювати різні форми інформаційних атак у ході інформаційної війни.

Серед методів забезпечення інформаційної безпеки важливе значення має метод дихотомії. Для протидії загрозам інформаційній безпеці вживаються необхідні заходи як в напрямку надання певного впливу на джерело загрози, так і в напрямку укріплення об'єкта безпеки. Відповідно виділяють дві предметні області протидії. Одна з них утворюється сукупністю джерел загроз, а інша - сукупністю заходів із забезпечення інформаційної безпеки органу державного управління. Вплив на джерело загрози інформаційної безпеки спрямований на зміну чинників та умов, здатних нанести шкоду об'єкту безпеки. Метою захисту є переконання супротивника у недоцільності здійснення загроз. Що стосується органів державного

управління, то джерело загроз може бути спрямовано на зміну міждержавних відносин, укріплення довіри між державами, створення умов, за яких здійснення небезпечних дій щодо об'єкта безпеки стає невигідним унаслідок виникнення небажаних наслідків або неможливим. Основним предметом за даного випадку є інформація, яка є у супротивника у вигляді відомостей, знань, оцінок. У свою чергу, інформація, що надходить від супротивника і становить собою загрозу, може бути піддана впливу для зміни її здатності завдавати шкоду, нейтралізації, трансформації або ліквідації її небезпечних властивостей. Вплив на інформаційну інфраструктуру важливий у тому випадку, коли загрозу може представляти середовище розповсюдження небезпечної інформації. Методи впливу на інформацію у формі повідомлень можна поділити також на електронні та неелектронні. Електронні методи впливу застосовуються у тих випадках, коли повідомлення закріплюються на електромагнітних носіях, котрі призначені для оброблення за допомогою засобів обчислювальної техніки. Вони полягають у знищенні, викривленні, копіюванні повідомлень, які зберігаються на цих пристроях. Такі дії можуть бути вчинені лише за допомогою технічного та програмного забезпечення. Неелектронні методи за своєю суттю мають той самий зміст, але реалізуються без використання засобів обчислювальної техніки для впливу на повідомлення, закріплення на інших, передусім паперових, носіях інформації.

Аналіз проблем забезпечення інформаційної безпеки дав змогу зробити висновок, що найбільш важливими напрямами діяльності у цій галузі є всебічна оцінка загроз та небезпек, національної уразливості, ідентифікація критичної інфраструктури. У процесі забезпечення інформаційної безпеки важливо розуміти характер, природу, сутність і зміст загроз та небезпек, вміти своєчасно ідентифікувати джерело загрози.

Система забезпечення інформаційної безпеки має бути міжвідомчою та ієрархічно організованою, її структура й організація має відповідати структурі державного управління з чіткою координацією дій окремих сегментів. Організація ефективної системи забезпечення інформаційної безпеки передбачає централізоване управління із конкретними відомчо-розпорядницькими функціями, які забезпечують моніторинг і контроль за усіма компонентами національного інформаційного простору. Система забезпечення інформаційної безпеки має у будь-яких ситуаціях скоординованої багатобічної і багатоаспектної інформаційної операції володіти здатністю зберігати важливі параметри свого функціонування, тобто підтримувати стан гомеостазису. Потребують подальшого вирішення питання щодо розробки комплексу інформаційних стандартів із урахуванням забезпечення інформаційної безпеки, розвиток системи сертифікації інформаційних продуктів, систем і послуг, створення системи ліцензування діяльності організацій по окремих напрямах формування єдиного інформаційного простору України.

Особливості забезпечення інформаційної безпеки України в різних сферах суспільного життя

Інформаційна безпека України є однієї зі складових національної безпеки України і впливає на захищеність національних інтересів України в різних сферах життєдіяльності суспільства та держави. Загрози інформаційній безпеці України та методи її забезпечення є загальними для цих сфер. У кожній з них є свої особливості

забезпечення інформаційної безпеки, пов'язані зі специфікою об'єктів забезпечення безпеки, ступенем їх уразливості від загроз інформаційній безпеці України. У кожній сфері життєдіяльності суспільства та держави поряд із загальними методами забезпечення інформаційної безпеки України можуть використовуватися часткові методи і форми, зумовлені специфікою чинників, що впливають на стан її інформаційної безпеки.

Забезпечення інформаційної безпеки України в сфері економіки

Забезпечення інформаційної безпеки України у сфері економіки відіграє ключову роль у забезпеченні національної безпеки України. Особлива увага приділяється захисту статистичної, фінансової, біржової, податкової та митної інформації, розробці, впровадженню та стандартизації захищених систем електронних платежів, грошей та торгівлі, та удосконаленню підготовки персоналу для роботи з економічною інформацією.

Забезпечення інформаційної безпеки України в сфері внутрішньої політики

Основними заходами із забезпечення інформаційної безпеки України в сфері внутрішньої політики є створення системи протидії монополізації вітчизняними і закордонними структурами складових інформаційної інфраструктури та активізація контрпропаганди, спрямованої на запобігання негативних наслідків поширення дезінформації про внутрішню політику України.

Забезпечення інформаційної безпеки України в сфері зовнішньої політики

Основними заходами із забезпечення інформаційної безпеки України в сфері зовнішньої політики є розробка основних напрямів державної політики щодо удосконалення інформаційного забезпечення зовнішньополітичного курсу України та створення її представництвам за кордоном умов для роботи з нейтралізації розповсюджуваної там дезінформації про зовнішню політику України.

Забезпечення інформаційної безпеки України у галузі науки та техніки

Найважливішими об'єктами забезпечення інформаційної безпеки України у галузі науки та техніки є: результати фундаментальних, пошукових і прикладних наукових досліджень, потенційно важливі для науково-технічного, технологічного та соціально-економічного розвитку країни. Реальний шлях протидії загрозам інформаційній безпеці України в галузі науки та техніки - це удосконалення законодавства України, яке регулює відносини в цій галузі.

Забезпечення інформаційної безпеки України у сфері духовного життя

Забезпечення інформаційної безпеки України у сфері духовного життя має на меті захист конституційних прав і свобод людини і громадянина, пов'язаних із розвитком, формуванням і поведінкою особистості, свободою масового інформування, використання культурної, духовно-моральної спадщини, історичних традицій і норм громадського життя, збереженням культурного надбання усіх народів України, реалізацією конституційних обмежень прав і свобод людини і громадянина в інтересах збереження та зміцнення моральних цінностей суспільства, традицій патріотизму та гуманізму, здоров'я громадян, культурного та наукового потенціалу України, забезпечення обороноздатності та безпеки України.

Забезпечення інформаційної безпеки України у загальнодержавних інформаційних і телекомунікаційних системах

Основними напрямами забезпечення інформаційної безпеки України в загальнодержавних інформаційних і телекомунікаційних системах є

запобігання перехопленню, витоку та несанкціонованого доступу до інформації, яка оброблюється чи зберігається в технічних засобах інформатизації, а також ліцензування, атестація і сертифікація об'єктів інформатизації та накладання територіальних, частотних, енергетичних, просторових і тимчасових обмежень у режимах використання технічних засобів.

Забезпечення інформаційної безпеки України у сфері оборони

Головними специфічними напрямами удосконалення системи забезпечення інформаційної безпеки України у сфері оборони є виявлення загроз та їхніх джерел, розвиток захищених систем зв'язку і управління військами та зброєю, підвищення надійності спеціального програмного забезпечення та вдосконалення прийомів і способів стратегічного та оперативного маскування, розвідки і радіоелектронної боротьби, методів і засобів активної протидії інформаційно-пропагандистським і психологічним операціям імовірного супротивника.

Забезпечення інформаційної безпеки України у правоохоронній і судовій сферах

Поряд із загальними методами та засобами захисту інформації застосовуються також специфічні методи і засоби забезпечення інформаційної безпеки у правоохоронній і судовій сферах - це створення захищеної багаторівневої системи інтегрованих банків даних оперативно-розшукового, довідкового, статистичного і криміналістичного характеру на базі спеціалізованих інформаційно-телекомунікаційних систем та підвищення рівня професійної та спеціальної підготовки користувачів інформаційних систем.

Міжнародне співробітництво України в галузі забезпечення інформаційної безпеки

Особливість міжнародного співробітництва України в галузі забезпечення інформаційної безпеки полягає в тому, що воно здійснюється в умовах загострення міжнародної конкуренції за володіння технологічними та інформаційними ресурсами. Основними напрямами міжнародного співробітництва України в галузі забезпечення інформаційної безпеки є заборона розробки, поширення та застосування «інформаційної зброї», забезпечення безпеки міжнародного інформаційного обміну та запобігання несанкціонованому доступу до інформації обмеженого доступу в міжнародних банківських телекомунікаційних мережах і системах інформаційного забезпечення світової торгівлі, до інформації міжнародних правоохоронних організацій, що ведуть боротьбу з транснаціональною організованою злочинністю, міжнародним тероризмом, поширенням наркотиків і психотропних речовин, незаконною торгівлею зброєю та матеріалами, які розщеплюються, а також торгівлею людьми.

Поняття права на інформацію

Забезпечення захисту прав і свобод людини в інформаційній сфері є однією з найважливіших цілей інформаційної безпеки, адже права і свободи людини у сфері інформації є ключовими інститутами громадянського суспільства, правової, демократичної держави, надбанням і цінністю європейської спільноти.

У літературі висловлюються погляди, в яких право громадян на інформацію - лише складова частина свободи слова та преси, або, навпаки, свобода інформації - умовне позначення цілої групи свобод і прав:

- свободи слова або свободи вираження думок; свободи преси та інших ЗМІ;
- права на одержання інформації, що має суспільне значення;

- свободи поширення інформації.

Вважається, що право на інформацію не охоплюється цілком свободою слова і преси. Воно значно багатіше, змістовніше і має власну субстанцію, грає свою роль у задоволенні певних інтересів суб'єктів; тому зрізаність даного найважливішого права необґрунтовано. Навряд чи виправданий і такий, надмірно широкий, підхід до змісту права на інформацію. Аргументом на користь таких висловлень є, безумовно, законодавча практика найвищого рівня - конституційна. Йдеться, наприклад, про ст. 34 Конституції України, де закріплені не лише свобода думки, слова, але і право на інформацію. Зовсім не випадково закріплені свобода думки і слова та право на інформацію в різних частинах, хоча й однієї статті. Тим самим підкреслюється як їхній взаємозв'язок і взаємопроникнення, так і відома автономність, самостійність, «суверенність». Взагалі, вперше поняття «право на інформацію» було визначено у ст. 9 Закону України «Про інформацію», а саме: «Всі громадяни України, юридичні особи і державні органи мають право на інформацію, що передбачає можливість вільного одержання, використання, поширення та зберігання відомостей, необхідних їм для реалізації ними своїх прав, свобод і законних інтересів, здійснення завдань і функцій». Причому, ст. 1 цього Закону визначає інформацію як «документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі». Але після набрання чинності Законом «Про телекомунікації», де в прикінцевих положеннях говориться про необхідність узгодження чинного законодавства з положеннями цього нового Закону, поняття інформації визначається вже як відомості, подані у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб.

Досить цікавим є також такі **основні положення**, що закріплюються відповідними нормами **Закону «Про інформацію»:**

1. Громадяни мають право доступу до інформації про них, а в період збору інформації мають право знати, які відомості про них і з якою метою збираються, а також оспорювати правильність, повноту, доцільність такої інформації.

2. Право на інформацію охороняється законом.

3. Держава гарантує усім учасникам інформаційних відносин рівні права та можливості доступу до інформації.

4. Інформація не може бути використана з метою, що завдає шкоди правам та свободам громадян України.

5. Не підлягають розголошенню відомості, які становлять державну чи іншу передбачену законом таємницю.

6. Реалізація права на інформацію громадянами, юридичними особами і державою не повинна порушувати громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи та законні інтереси інших громадян, права та інтереси юридичних осіб.

7. Кожному громадянину забезпечується вільний доступ до інформації, яка стосується його особисто, крім випадків, передбачених законами України.

З прийняттям Конституції України в 1996 році, право людини на інформацію - самостійне конституційне право, яке дозволяє людині вільно збирати, зберігати, використовувати і поширювати інформацію будь-яким способом, що гарантується ч. 2 ст. 34 Конституції України. Здійснення цього права може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського

порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя (ч. 3 ст. 34 Конституції України).

Комплекс прав та свобод в інформаційній сфері вважається непорушним та невідчужуваним. За основу положень розділу ІІ «Права, свободи та обов'язки людини і громадянина» Конституції України взято ряд міжнародних нормативно-правових актів. Зокрема, Загальна декларація прав людини, Міжнародний пакт про економічні, соціальні і культурні права, Міжнародний пакт про громадянські та політичні права. У цілому ст. 34 Конституції України відповідає ст. 19 Міжнародного пакту про громадянські і політичні права, який надає кожній людині право вільно шукати, одержувати і поширювати будь-яку інформацію та ідеї, незалежно від державних кордонів, та в будь-який спосіб за своїм вибором.

Види інформаційних прав і свобод і їх зв'язок з іншими правами та свободами людини та громадянина

Крім загального визначення права людини на інформацію в ст. 34 Конституції, є ряд інших інформаційних прав і свобод, що закріплюються конституційними нормами.

1. Свобода особистого і сімейного життя (ст. 32: «...не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини»);

2. Таємниця листування, телефонних переговорів, телеграфної й іншої кореспонденції (ст. 31: «...винятки можуть бути встановлені лише судом у випадках, передбачених законом, з метою запобігти злочинові чи з'ясувати істину під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо»);

3. Право громадянина не зазнавати втручання в його особисте та сімейне життя, шляхом збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, знайомитися в органах державної влади, органах місцевого самоврядування, установах та організаціях із відомостями про себе (ст. 32: це відноситься до відомостей, що «не є державною або іншою захищеною законом таємницею»);

4. Право громадянина направляти індивідуальні або колективні письмові звернення або особисто звертатися в органи державної влади, органи місцевого самоврядування та до посадових і службових осіб цих органів (ст. 40);

5. Право кожного громадянина на сприятливе навколишнє середовище, достовірну інформацію про її стан (ст. 50: «...така інформація ніким не може бути засекречена»);

6. Право кожного на свободу творчості і право доступу до культурних цінностей (ст. 54: результати інтелектуальної, творчої діяльності громадянина «ніхто не може використовувати або поширювати їх без його згоди, за винятками, встановленими законом»);

7. Право кожного громадянина на одержання кваліфікованої правової допомоги (ст. 59: «...у випадках, передбачених законом, ця допомога надається безоплатно»). Деякі конституційні положення, також мають відношення до інформаційних прав і

свобод. Так, за статтями 21, 24 усі люди є вільні і рівні у своєму праві на інформацію, яке є невідчужуваним та непорушним і не залежить від раси, кольору шкіри, релігійних та інших переконань, статі, етнічного та соціального походження тощо. Без отримання необхідної інформації, вільного її використання людина не змогла б розвивати свою особистість (ст. 23).

Право на інформацію пов'язане з правом на свободу світогляду і віросповідання, яке включає свободу сповідувати будь-яку релігію або не сповідувати ніякої, безперешкодно відправляти одноособово чи колективно релігійні культи і ритуальні обряди, вести релігійну діяльність (ст. 35). Реалізація права на освіту (ст. 53) неможлива без вільного інформаційного обміну між людьми. Процес навчання означає, перш за все, пошук і отримання необхідної інформації. Ст. 34 Конституції можна також розглядати як певний розвиток і конкретизацію положення ч. 3 ст. 15, що забороняє здійснення в Україні цензури, тобто обмежувальних заходів щодо здійснення свободи слова в засобах масової інформації. Вона гарантує духовну і творчу свободу, не обмежену ніякою обов'язковою ідеологією. Положення статті гарантують доступ до засобів масової інформації політичним партіям і рухам, громадським організаціям, профспілкам, кожній окремій людині. Ніхто не може бути примушений до зміни чи висловлювання своїх поглядів і переконань. Зрозуміло, що Конституція України закріплює основний зміст прав і свобод в інформаційній сфері, але їх конкретизація відображається в ряді інших нормативно-правових актах.

Структура конституційного права на інформацію

Структура конституційного права на інформацію, що закріплюється Конституцією України та Цивільним кодексом України, визначається такими складовими як:

- збирання інформації;
- зберігання інформації;
- використання інформації;
- поширення інформації.

Відповідно до Закону України «Про інформацію», структурою вищезазначеного права є:

- одержання;
- зберігання;
- використання;
- поширення.

Поняття «збирання» інформації, яке міститься у тексті Конституції, законодавчо не визначено, оскільки Закон України «Про інформацію» дає дефініції тільки таким поняттям як «одержання», «зберігання», «використання» та «поширення». Під одержанням інформації законодавець розуміє набуття, придбання, накопичення інформації громадянами, юридичними особами або державою відповідно до чинного законодавства України. Зберігання інформації — означає забезпечення належного стану інформації та її матеріальних носіїв. Використання інформації - задоволення інформаційних потреб громадян, юридичних осіб і держави. Поширення інформації - розповсюдження, оприлюднення, реалізацію інформації у встановленому законом порядку. Цікавим є той факт, що даний Закон у ст. 38 закріплює також «право власності на

інформацію», під яким розуміється «врегульовані законом суспільні відносини щодо володіння, користування і розпорядження інформацією». Отже, законодавець оперує такими поняттями, як «володіння», «користування», «розпорядження», які не визначені законодавчо. Тому, більшість науковців наголошують на необхідності уточнення понять «користування» і «розповсюдження» для з'ясування чіткої різниці між «використанням» і «користуванням» та між «поширенням» і «розповсюдженням» інформації, оскільки фактично використання інформації передбачає і збирання, і поширення інформації, і взагалі будь-які інші маніпуляції з нею. Особливої уваги для забезпечення інформаційної безпеки, заслуговує поняття «доступу до інформації». Ст. 28 Закону України «Про інформацію» містить поняття «режим доступу до інформації» як передбачений правовими нормами порядок одержання, використання, поширення і зберігання інформації.

Основними положеннями цього Закону згідно зі статтями 28, 29, 30, що закріплюють режим доступу до інформації, є:

1. За режимом доступу інформація поділяється на відкриту та інформацію з обмеженим доступом.

2. Держава здійснює контроль за режимом доступу до інформації.

3. Завдання контролю за режимом доступу до інформації полягає у забезпеченні додержання вимог законодавства про інформацію всіма державними органами, підприємствами, установами та організаціями, недопущенні необґрунтованого віднесення відомостей до категорії інформації з обмеженим доступом.

4. Державний контроль за додержанням встановленого режиму здійснюється спеціальними органами.

5. У порядку контролю Верховна Рада України може вимагати від урядових установ, міністерств, відомств звіти, які містять відомості про їх діяльність по забезпеченню інформацією зацікавлених осіб.

6. Будь-яке обмеження права одержання відкритої інформації забороняється Законом.

7. Інформація з обмеженим доступом поділяється на конфіденційну і таємну.

8. До конфіденційної інформації належать відомості, що знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб, які можуть поширюватися за їх бажанням відповідно до передбачених ними умов.

9. Таємною є інформація, що містить відомості, які становлять державну та іншу, передбачену Законом таємницю, розголошення якої завдає (чи може завдати) шкоди особі, державі, суспільству.

Відповідно до вимог ст. 37 Закону України «Про інформацію» не підлягають обов'язковому наданню для ознайомлення за інформаційними запитами офіційні документи, які містять інформацію:

- визнану у встановленому порядку державною таємницею;
- конфіденційну;
- про оперативну та слідчу роботу органів прокуратури, МВС, СБУ, роботу органів дізнання та суду у тих випадках, коли її розголос може зашкодити оперативним заходам, розслідуванню чи дізнанню, порушити право людини на справедливий та об'єктивний судовий розгляд її справи, створити загрозу життю або здоров'ю будь-якої особи;
- що стосується особистого життя громадян;

- щодо внутрівідомчої службової кореспонденції, якщо вона пов'язана з розробкою напряму діяльності установи, з процесом прийняття рішень і передує їх прийняттю;

- що не підлягає розголошенню згідно з іншими законодавчими актами;

- фінансових установ, підготовлену для контрольно-фінансових відомств. Зазначимо, що критерії віднесення інформації до таємної, порядок її обігу та захисту регулюються Законом України «Про державну таємницю».

Оскільки ч. 2 ст. 32 Конституції України забороняє збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, то досить цікавим є розгляд цієї проблеми детальніше. Ст. 23 Закону України «Про інформацію» містить такі основні норми:

1. Основними даними про особу (персональними даними) є національність, освіта, сімейний стан, релігійність, стан здоров'я, а також адреса, дата і місце народження.

2. Джерелами документованої інформації про особу є видані на її ім'я документи, підписані нею документи, а також відомості про особу, зібрані державними органами влади та органами місцевого і регіонального самоврядування в межах своїх повноважень.

3. Забороняється збирання відомостей про особу без її попередньої згоди, за винятком випадків, передбачених законом. Офіційне тлумачення статті 23 надано Конституційним Судом України у його Рішенні № 5-зп від 30.10.97, де персональні дані про особу віднесені до конфіденційної інформації.

Нормативно-правове забезпечення інформаційної безпеки України.

Базові засади інформаційної безпеки нашої держави закладено у статтях 17, 19, 31, 32, 34, 50, 57 та 64 Конституції України.

Закон України «Про інформацію» закріплює право громадян України на інформацію, закладає правові основи інформаційної діяльності. Закон стверджує інформаційний суверенітет України і визначає правові форми міжнародного співробітництва в галузі інформації, встановлює загальні правові основи одержання, використання, поширення та зберігання інформації, закріплює право особи на інформацію в усіх сферах суспільного і державного життя України, а також систему інформації, її джерела, визначає статус учасників інформаційних відносин, регулює доступ до інформації та забезпечує її охорону, захищає особу та суспільство від неправдивої інформації.

У ст. 1 закону ***інформація*** визначається як документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі.

Державну інформаційну політику розробляють і здійснюють органи державної влади загальної компетенції, а також відповідні органи спеціальної компетенції.

Всі громадяни України, юридичні особи і державні органи мають ***право на інформацію***, що передбачає можливість вільного одержання, використання, поширення та зберігання відомостей, необхідних їм для реалізації ними своїх прав, свобод і законних інтересів, здійснення завдань і функцій.

Кожному громадянину забезпечується вільний доступ до інформації, яка стосується його особисто, крім випадків, передбачених законами України.

Розділ II закону присвячено інформаційній діяльності, під якою розуміється

сукупність дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб і держави. Визначено основні напрями та *види* інформаційної діяльності – одержання, використання, поширення та зберігання інформації.

У розділі ІІІ закону наведені галузі, види, джерела інформації та режим доступу до неї. Основними галузями інформації визначені: політична, економічна, духовна, науково-технічна, соціальна, екологічна, міжнародна.

Основними ***видами інформації*** є: статистична; адміністративна інформація (дані); масова інформація; інформація про діяльність державних органів влади та органів місцевого і регіонального самоврядування; правова інформація; інформація про особу; інформація довідково-енциклопедичного характеру; соціологічна інформація.

За ***режимом доступу*** інформація поділяється на ***відкриту інформацію*** та ***інформацію з обмеженим доступом***.

Держава здійснює контроль за режимом доступу до інформації.

Державний контроль за додержанням встановленого режиму здійснюється спеціальними органами, які визначають Верховна Рада України і Кабінет Міністрів України.

Доступ до відкритої інформації забезпечується шляхом: систематичної публікації її в офіційних друкованих виданнях (бюлетенях, збірниках); поширення її засобами масової комунікації; безпосереднього її надання заінтересованим громадянам, державним органам та юридичним особам.

Обмеження права на одержання відкритої інформації забороняється законом.

Інформація з обмеженим доступом за своїм ***правовим режимом*** поділяється на ***конфіденційну*** і ***таємну***.

Конфіденційна інформація – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов.

Громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, одержаною на власні кошти, або такою, яка є предметом їх професійного, ділового, виробничого, банківського, комерційного та іншого інтересу і не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї, включаючи належність її до категорії конфіденційної, та встановлюють для неї систему (способи) захисту.

Виняток становить інформація комерційного та банківського характеру, а також інформація, правовий режим якої встановлено Верховною Радою України за поданням Кабінету Міністрів України (з питань статистики, екології, банківських операцій, податків тощо), та інформація, приховування якої являє загрозу життю і здоров'ю людей.

До ***таємної інформації*** належить інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю (військова, комерційна, банківська, професійна, лікарська, адвокатська таємниця тощо), розголошення якої завдає шкоди особі, суспільству і державі.

Інформація, що становить військову таємницю – це вид таємної інформації, який охоплює відомості в сфері оборони, державної безпеки та охорони правопорядку, розголошення якої може завдати шкоди інтересам державної безпеки,

бойової готовності Збройних Сил України та інших військових формувань, їхніх окремих підрозділів, якщо ці відомості не належать до державної таємниці згідно з законодавством України.

Інформація, що становить комерційну таємницю – це відомості науково-технічного, технічного, виробничого, фінансово-економічного або іншого характеру (в тому числі секрети виробництва – так зване ноу-хау), що мають дійсну або потенційну комерційну цінність у силу її невідомості третім особам, до якої немає вільного доступу на законній підставі й у відношенні якої власником такої інформації введений режим комерційної таємниці.

Порядок обігу таємної інформації, що не становить державної таємниці, та її захист визначається відповідними державними органами за умов додержання вимог Закону України "Про інформацію".

Інформація з обмеженим доступом може бути поширена без згоди її власника, якщо вона є суспільно значимою, тобто якщо вона є предметом громадського інтересу і якщо право громадськості знати цю інформацію переважає право її власника на її захист.

Особливим видом таємної інформації є ***державна таємниця***. Вона охоплює відомості у сфері оборони, економіки, зовнішніх відносин, державної безпеки і органів правопорядку, розголошення яких може завдати шкоди життєво важливим інтересам України і які визначені у порядку, встановленому законом, державною таємницею та підлягає охороні з боку держави.

Віднесення інформації до категорії відомостей, що становлять державну таємницю, порядок її захисту та обігу, доступ до неї визначається Законом України «Про державну таємницю», яким закладено правову основу створення та функціонування системи охорони державної таємниці в Україні.

Ступінь таємності інформації визначається наданим ***грифом таємності*** «Таємно», «Цілком таємно» та «Особливої важливості».

У розділі IV закону визначені учасники інформаційних відноси, їх права та обов'язки. Основними учасниками цих відносин є: автори, споживачі, поширювачі, зберігачі (охоронці) інформації.

Кожний учасник інформаційних відносин для забезпечення його прав, свобод і законних інтересів має право на одержання інформації про: діяльність органів державної влади; діяльність народних депутатів; діяльність органів місцевого і регіонального самоврядування та місцевої адміністрації; те, що стосується його особисто.

Розділ V закону присвячений охороні інформації, відповідальності за порушення законодавства про інформацію. Держава гарантує всім учасникам інформаційних відносин рівні права і можливості доступу до інформації.

Інформація не може бути використана для закликів до повалення конституційного ладу, порушення територіальної цілісності України, пропаганди війни, насильства, жорстокості, розпалювання расової, національної, релігійної ворожнечі, посягання на права і свободи людини.

Не підлягають розголошенню відомості, що стосуються лікарської таємниці, грошових вкладів, прибутків від підприємницької діяльності, усиновлення (удочеріння), листування, телефонних розмов і телеграфних повідомлень, крім випадків, передбачених законом.

Порушення законодавства України про інформацію тягне за собою дисциплінарну, цивільно-правову, адміністративну або кримінальну відповідальність згідно з законодавством України.

Розділ VI закону присвячено міжнародній інформаційній діяльності, співробітництву з іншими державами, зарубіжними і міжнародними організаціями в галузі інформації.

Міжнародне співробітництво в галузі інформації з питань, що становлять взаємний інтерес, здійснюється на основі міжнародних договорів, укладених Україною та юридичними особами, які займаються інформаційною діяльністю.

Стаття 53 закону визначає ***інформаційний суверенітет***. Основою інформаційного суверенітету України є національні інформаційні ресурси.

До ***інформаційних ресурсів України*** входить вся належна їй інформація, незалежно від змісту, форм, часу і місця створення. Україна самостійно формує інформаційні ресурси на своїй території і вільно розпоряджається ними, за винятком випадків, передбачених законами і міжнародними договорами.

Інформаційний суверенітет України забезпечується:

- виключним правом власності України на інформаційні ресурси, що формуються за рахунок коштів державного бюджету;
- створенням національних систем інформації;
- встановленням режиму доступу інших держав до інформаційних ресурсів України;
- використанням інформаційних ресурсів на основі рівноправного співробітництва з іншими державами.

Узагальнена класифікація інформації у відповідності до Закону України «Про інформацію» надана на рис. 4.

Рис. 4. Класифікація інформації у відповідності до Закону України «Про інформацію»

В ст.10 Закону України «Про основи національної безпеки України» , визначені основні функції суб'єктів забезпечення національної безпеки України (інформаційна сфера окремо не виділена):

- вироблення і періодичне уточнення Стратегії національної безпеки України і Воєнної доктрини України, доктрин, концепцій, стратегій і програм, планування і здійснення конкретних заходів щодо протидії і нейтралізації загроз національним інтересам України;
- створення нормативно-правової бази, необхідної для ефективного функціонування системи національної безпеки;
- удосконалення її організаційної структури;
- комплексне кадрове, фінансове, матеріальне, технічне, інформаційне та інше забезпечення життєдіяльності складових (структурних елементів) системи;
- підготовка сил та засобів суб'єктів системи до їх застосування згідно з призначенням;
- постійний моніторинг впливу на національну безпеку процесів, що відбуваються в політичній, соціальній, економічній, екологічній, науково-технологічній, інформаційній, воєнній та інших сферах, релігійному середовищі,

міжетнічних стосунках; прогнозування змін, що відбуваються в них, та потенційних загроз національній безпеці;

- систематичне спостереження за станом і проявами міжнародного та інших видів тероризму;
- прогнозування, виявлення та оцінка можливих загроз, дестабілізуючих чинників і конфліктів, причин їх виникнення та наслідків прояву;
- розроблення науково-обгрунтованих пропозицій і рекомендацій щодо прийняття управлінських рішень з метою захисту національних інтересів України;
- запобігання та усунення впливу загроз і дестабілізуючих чинників на національні інтереси;
- локалізація, деескалація та врегулювання конфліктів і ліквідація їх наслідків або впливу дестабілізуючих чинників;
- оцінка результативності дій щодо забезпечення національної безпеки та визначення витрат на ці цілі;
- участь у двосторонньому і багатосторонньому співробітництві в галузі безпеки, якщо це відповідає національним інтересам України;
- спільне проведення планових та оперативних заходів у рамках міжнародних організацій та договорів у галузі безпеки.

Стаття 11 закону визначає загальні повноваження суб'єктів національної безпеки щодо контролю за здійсненням заходів забезпечення національної безпеки.

Необхідно відзначити, що цей закон був базовим для прийняття "Концепції національної безпеки України". Концепція визначала основні засади державної політики в сфері національної безпеки України та напрями її подальшого розвитку.

В її розділі III «Загрози національній безпеці України» у ряді загроз національній безпеці в інформаційній сфері виділено витік інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави.

А в розділі IV «Основні напрями державної політики національної безпеки України» для усунення цієї загрози запропоновано розробку і впровадження необхідних засобів та режимів отримання, зберігання, поширення і використання суспільно значущої інформації, створення розвиненої інфраструктури в інформаційній сфері.

У розділі V концепції було сформульовано напрями та заходи для формування збалансованої державної політики та ефективного проведення комплексу узгоджених заходів щодо захисту національних інтересів у політичній, економічній, соціальній, воєнній, екологічній, науково-технологічній, інформаційній та інших сферах створюється система забезпечення національної безпеки України.

Визначена система забезпечення національної безпеки - як 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 України.

Крім того були прийняті Закони України «Про телекомунікації», «Про Національну програму інформатизації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про науково-технічну інформацію», а у Кримінальний кодекс України було введено розділ XVI, в якому визначалася

відповідальність за злочини в інформаційній сфері.

Згодом з’явилася нагальна необхідність в удосконаленні та розвитку як нормативної, так і науково-технічної бази технічного захисту інформації, що й призвело до появи «Концепції технічного захисту інформації в Україні».

У загальних положеннях «Концепції технічного захисту інформації в Україні» визначено основи державної політики у сфері захисту інформації інженерно-технічними заходами. Зокрема визначено, що технічний захист інформації (далі - ТЗІ) є складовою частиною забезпечення національної безпеки України.

Встановлено головні завдання, що повинні вирішуватися концепцією. Концепція має забезпечити єдність принципів формування і проведення такої політики в усіх сферах життєдіяльності особи, суспільства та держави (соціальній, політичній, економічній, військовій, екологічній, науково-технологічній, інформаційній тощо) і служити підставою для створення програм розвитку сфери ТЗІ.

Також у загальних положеннях концепції визначено, що ТЗІ - це діяльність, спрямована на забезпечення інженерно-технічними заходами порядку доступу, цілісності та доступності (унеможливлення блокування) інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформації, а також цілісності та доступності відкритої інформації, важливої для особи, суспільства і держави.

Показано, що зростання загроз для інформації, спричинене лібералізацією суспільних та міждержавних відносин, кризовим станом економіки, застосуванням технічних засобів оброблення інформації та засобів зв'язку іноземного виробництва, поширенням засобів несанкціонованого доступу до інформації та впливу на неї, визначає необхідність розвитку ТЗІ.

Визначено, що напрями розвитку ТЗІ обумовлюються необхідністю своєчасного вжиття заходів, адекватних масштабам загроз для інформації, і ґрунтуються на засадах правової демократичної держави відповідно до прав суб'єктів інформаційних відносин на доступ до інформації та її захист.

При цьому приведення інформаційних відносин у сфері ТЗІ у відповідність з міжнародними стандартами сприятиме становленню України у світі як демократичної правової держави.

У розділі ІІ концепції «Загрози безпеці інформації та стан її технічного захисту» показано, що впровадження в усі сфери життєдіяльності особи, суспільства та держави інформаційних технологій зумовило поширення великих масивів інформації в обчислювальних та інформаційних мережах на значних територіях. За відсутності вітчизняних конкурентоспроможних інформаційних технологій надається перевага технічним засобам оброблення інформації та засобам зв'язку іноземного та спільного виробництва, які здебільшого не забезпечують захист інформації. Комунікаційне обладнання іноземного виробництва, яке використовується у мережах зв'язку, передбачає дистанційний доступ до його апаратних та програмних засобів, у тому числі з-за кордону, що створює умови для несанкціонованого впливу на їх функціонування і контролю за організацією зв'язку та змістом повідомлень, які пересилаються.

Прогрес у різних галузях науки і техніки призвів до створення компактних та високоефективних технічних засобів, за допомогою яких можна легко підключатися

до ліній телекомунікації та різноманітних технічних засобів оброблення інформації вітчизняного та іноземного виробництва з метою здобування, пересилання та аналізу розвідувальних даних. Для цього може використовуватись апаратура радіо, радіотехнічної, електронно-оптичної, радіо-теплової, акустичної, хімічної, магнітометричної, сейсмічної та радіаційної розвідок.

За таких умов створилися можливості ***витоку інформації, порушення її цілісності*** та ***блокування***. Витік інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформації, що є власністю держави, - це одна з основних можливих загроз національній безпеці України в інформаційній сфері. Загрози безпеці інформації в Україні зумовлені:

- не виваженістю державної політики в галузі інформаційних технологій, що може призвести до безконтрольного та неправомочного доступу до інформації та її використання;
- діяльністю інших держав, спрямованою на одержання переваги в зовнішньополітичній, економічній, військовій та інших сферах;
- недосконалістю організації в Україні міжнародних виставок апаратури різного призначення (особливо пересувних) та заходів екологічного моніторингу, що може використовуватися для здобування інформації розвідувального характеру;
- злочинною діяльністю, спрямованою на протизаконне одержання інформації з метою досягнення матеріальної вигоди або нанесення шкоди юридичним чи фізичним особам;
- використанням інформаційних технологій низького рівня, що призводить до впровадження недосконалих технічних засобів із захистом інформації, засобів контролю за ефективністю ТЗІ та засобів ТЗІ (далі - засоби забезпечення ТЗІ);
- недостатністю документації на засоби забезпечення ТЗІ іноземного виробництва, а також низькою кваліфікацією технічного персоналу у сфері ТЗІ.

Стан ТЗІ зумовлюється:

- недосконалістю правового регулювання в інформаційній сфері, зокрема у сфері захисту таємниць (крім державної), конфіденційної інформації та відкритої інформації, важливої для особи, суспільства та держави;
- недостатністю нормативно-правових актів і нормативних документів з питань проведення досліджень, розроблення та виробництва засобів забезпечення ТЗІ;
- незавершеністю створення системи сертифікації засобів забезпечення ТЗІ;
- недосконалістю системи атестації на відповідність вимогам ТЗІ об'єктів, робота яких пов'язана з інформацією, що підлягає технічному захисту;
- недостатньою узгодженістю чинних в Україні нормативно-правових актів та нормативних документів з питань ТЗІ з відповідними міжнародними договорами України.

У розділі ІІІ концепції «Система ТЗІ» визначено, що ***система ТЗІ*** - *це сукупність суб'єктів, об'єднаних цілями та завданнями захисту інформації інженерно-технічними заходами (далі - організаційні структури), нормативно-правова та матеріально-технічна база*.

Зазначено, що правову основу забезпечення ТЗІ в Україні становлять Конституція України, Закони України «Про інформацію», «Про захист інформації в автоматизованих системах», «Про державну таємницю», «Про науково-технічну

інформацію», інші нормативно-правові акти, а також міжнародні договори України, що стосуються сфери інформаційних відносин.

Принципами формування і проведення державної політики у сфері ТЗІ є:

- додержання балансу інтересів особи, суспільства та держави, їх взаємна відповідальність;
- єдність підходів до забезпечення ТЗІ, які визначаються загрозами безпеці інформації та режимом доступу до неї;
- комплексність, повнота та безперервність заходів ТЗІ;
- відкритість нормативно-правових актів та нормативних документів з питань ТЗІ, які не містять відомостей, що становлять державну таємницю;
- узгодженість нормативно-правових актів та нормативних документів з питань ТЗІ з відповідними міжнародними договорами України;
- обов'язковість захисту інженерно-технічними заходами інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформації, що є власністю держави, відкритої інформації, важливої для держави, незалежно від того, де зазначена інформація циркулює, а також відкритої інформації, важливої для особи та суспільства, якщо ця інформація циркулює в органах державної влади та органах місцевого самоврядування, Національній академії наук, Збройних Силах, інших військових формуваннях, органах внутрішніх справ, на державних підприємствах, в державних установах і організаціях (далі - державні органи, підприємства, установи і організації);
- виконання на власний розсуд суб'єктами інформаційних відносин вимог щодо технічного захисту конфіденційної інформації, що не належить державі, та відкритої інформації, важливої для особи та суспільства, якщо остання циркулює поза межами державних органів, підприємств, установ і організацій;
- покладення відповідальності за формування та реалізацію державної політики у сфері ТЗІ на спеціально уповноважений центральний орган виконавчої влади;
- ієрархічність побудови організаційних структур системи ТЗІ та керівництво їх діяльністю у межах повноважень, визначених нормативно-правовими актами;
- методичне керівництво спеціально уповноваженим центральним органом виконавчої влади у сфері ТЗІ діяльністю організаційних структур системи ТЗІ;
- скоординованість дій та розмежування сфер діяльності організаційних структур системи ТЗІ з іншими системами захисту інформації та системами забезпечення інформаційної та національної безпеки;
- фінансова забезпеченість системи ТЗІ за рахунок Державного бюджету України, бюджету Автономної Республіки Крим, місцевих бюджетів та інших джерел.

Основними функціями організаційних структур системи ТЗІ є:

- оцінка стану ТЗІ в державі, визначення пріоритетних напрямів його розвитку;
- розвиток правових засад удосконалення системи ТЗІ;
- виявлення та прогнозування загроз безпеці інформації;
- забезпечення інженерно-технічними заходами захисту інформації, що підлягає технічному захисту;
- створення умов для ТЗІ, що здійснюється суб'єктами інформаційних відносин

на власний розсуд;

- формування та забезпечення реалізації державної політики щодо створення та впровадження вітчизняних засобів забезпечення ТЗІ;
- створення національної системи стандартизації та нормування у сфері ТЗІ;
- організація фундаментальних і прикладних науково-дослідних робіт та розробок у сфері ТЗІ;
- забезпечення взаємодії організаційних структур системи ТЗІ з іншими системами захисту інформації та системами забезпечення інформаційної та національної безпеки;
- організація створення та виконання програм розвитку ТЗІ;
- забезпечення ліцензування підприємницької діяльності в сфері ТЗІ;
- організація контролю за якістю засобів забезпечення ТЗІ шляхом їх сертифікації;
- організація контролю за відповідністю вимогам ТЗІ об'єктів, діяльність яких пов'язана з інформацією, що підлягає технічному захисту, шляхом їх атестації;
- організація контролю за ефективністю ТЗІ на об'єктах, діяльність яких пов'язана з інформацією, що підлягає технічному захисту;
- забезпечення підготовки фахівців для роботи у сфері ТЗІ;
- сприяння залученню інвестицій і вітчизняного товаровиробника у сферу ТЗІ;
- організація міжнародного співробітництва в сфері ТЗІ, представлення інтересів України у відповідних міжнародних організаціях;
- забезпечення (кадрове, фінансове, нормативне, матеріально-технічне, інформаційне тощо) життєдіяльності складових організаційних структур системи ТЗІ.

Розділ IV концепції визначає основні напрями державної політики у сфері ТЗІ. Зокрема у ньому прийнято, що державна політика у сфері ТЗІ визначається пріоритетністю національних інтересів, має на меті унеможливлення реалізації загроз для інформації та здійснюється шляхом виконання положень цієї Концепції, а також програм розвитку ТЗІ та окремих проектів.

Основними ***напрямами державної політики у сфері ТЗІ*** є:

- нормативно-правове забезпечення:
- удосконалення чинних та створення нових нормативно-правових актів щодо захисту інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформації, що належить державі;
- розроблення нормативно-правових актів щодо захисту відкритої інформації, важливої для особи, суспільства та держави;
- удосконалення правових механізмів організаційного забезпечення ТЗІ;
- удосконалення нормативно-правових актів щодо умов і правил провадження діяльності у сфері ТЗІ;
- розроблення нормативно-правових актів щодо визначення статусу головної у сфері ТЗІ, головних (базових) за напрямами ТЗІ організацій;
- удосконалення нормативно-правових актів щодо здійснення контролю за імпортом з метою впровадження в Україні іноземних інформаційних технологій з захистом інформації та засобів забезпечення ТЗІ;
- розроблення нормативних документів з питань формування та розвитку моделі загроз для інформації;

- розроблення нормативних документів з питань сертифікації засобів забезпечення ТЗІ та атестації на відповідність вимогам ТЗІ об'єктів, робота яких пов'язана з інформацією, що підлягає технічному захисту;

- удосконалення чинних та розроблення нових нормативних документів з питань ТЗІ:

- у засобах обчислювальної техніки, в автоматизованих системах, оргтехніці, мережах зв'язку, комп'ютерних мережах та приміщеннях, де циркулює інформація, що підлягає технічному захисту;

- під час створення, експлуатації та утилізації зразків озброєнь, військової та спеціальної техніки;

- під час проектування, будівництва і реконструкції військово-промислових, екологічно небезпечних та інших особливо важливих об'єктів;

- організаційне забезпечення:

- забезпечення створення підрозділів ТЗІ в органах державної влади та органах місцевого самоврядування, академіях наук, Збройних Силах, інших військових формуваннях, органах внутрішніх справ, на підприємствах, в установах і організаціях всіх форм власності, діяльність яких пов'язана з інформацією, що підлягає технічному захисту;

- створення головної у сфері ТЗІ, головних (базових) за напрямами ТЗІ організацій, а також лабораторій системи сертифікації засобів забезпечення ТЗІ;

- підготовка кадрів для роботи у сфері ТЗІ;

- залучення до розв'язання проблем ТЗІ вітчизняних вчених та висококваліфікованих спеціалістів;

- розвиток міжнародного співробітництва в сфері ТЗІ;

- науково-технічна та виробнича діяльність:

- моніторинг і оцінка стану ТЗІ, підготовка аналітичних матеріалів і пропозицій щодо стратегії його розвитку;

- створення інформаційно-аналітичних моделей загроз для інформації та методології їх прогнозування;

- обґрунтування критеріїв та показників рівнів ТЗІ;

- створення методології синтезу систем багаторівневого захисту інформації, адекватних масштабам загроз безпеці інформації та режиму доступу до неї;

- створення методології, призначеної для визначення зниження ефективності продукції, зумовленої витоком інформації про неї, порушенням її цілісності чи блокуванням, та методології обґрунтування заходів ТЗІ;

- системне і поетапне розроблення сучасних засобів забезпечення ТЗІ;

- пріоритетне створення вітчизняних конкурентоспроможних інформаційних технологій та розвиток виробництва засобів забезпечення ТЗІ;

- створення умов для забезпечення головної у сфері ТЗІ, головних (базових) за напрямами ТЗІ організацій, а також лабораторій системи сертифікації засобів забезпечення ТЗІ науковим, контрольно-вимірювальним, випробувальним та виробничим обладнанням.

Першочерговими заходами щодо реалізації державної політики у сфері ТЗІ є:

- створення правових засад реалізації державної політики у сфері ТЗІ, визначення послідовності та порядку розроблення відповідних нормативно-правових актів;

- визначення перспективних напрямів розроблення нормативних документів з питань ТЗІ на основі аналізу стану відповідної вітчизняної та зарубіжної нормативної бази, розроблення зазначених нормативних документів;
- визначення номенклатури вітчизняних засобів обчислювальної техніки та базового програмного забезпечення, оргтехніки, обладнання мереж зв'язку, призначених для оброблення інформації з обмеженим доступом інших засобів забезпечення ТЗІ в органах державної влади та органах місцевого самоврядування, Національній академії наук, Збройних Силах, інших військових формуваннях, органах внутрішніх справ;
- налагодження згідно з визначеною номенклатурою виробництва засобів обчислювальної техніки та базового програмного забезпечення, оргтехніки, обладнання мереж зв'язку із захистом інформації, інших вітчизняних засобів забезпечення ТЗІ;
- завершення створення та розвиток системи сертифікації вітчизняних та закордонних засобів забезпечення ТЗІ;
- визначення реальних потреб системи ТЗІ у фахівцях, розвиток та вдосконалення системи підготовки, перепідготовки та підвищення кваліфікації фахівців з питань ТЗІ.

Значущість забезпечення ТЗІ, його наукоємність вимагає концентрації зусиль науково-технічного та виробничого потенціалу міністерств, інших центральних органів виконавчої влади, академій наук.

Слід додати, що одночасно з створенням правових та організаційних основ ТЗІ були створені правові та організаційні основи криптографічного захисту інформації.

У травні 1998 р. прийнято Указ Президента України “Про Положення про порядок здійснення криптографічного захисту інформації в Україні” (відповідно, саме положення було підготовлено дещо раніше).

У липні 2002 року був прийнятий Закон України «Про Національну систему конфіденційного зв'язку», у січні 2003 р. надано розпорядження Президента України «Про заходи щодо забезпечення розвитку і функціонування Національної системи конфіденційного зв'язку», з дорученням Президента Кабінету Міністрів щодо практичної організації такої системи.

Основні принципи, норми та положення прийнятих законів та підзаконних актів відповідають загальноприйнятим міжнародно-правовим стандартам, в тому числі міжнародним конвенціям з прав людини.

Таким чином, було закладено основні традиції інформаційної безпеки України. Подальший розвиток цієї сфери державного будівництва вимагатиме удосконалення інфраструктури захисту інформації та законів і численних підзаконних актів та нормативних документів, якими регламентується діяльність цієї інфраструктури, а також діяльність органів державного управління, установ та організацій науки й виробництва, які використовують у своїй діяльності інформацію з обмеженим доступом.

На теперішній час в Україні розроблено основна правова та нормативна база, та створена інфраструктура, що має забезпечити надійний захист інформації у державі.

Разом з тим слід пам’ятати, що технічні способи несанкціонованого зняття інформації та засоби протидії цим протиправним діям знаходяться у постійному розвитку.

Зважаючи на цей безперервний розвиток та постійну інформаційну боротьбу, що складає один з важливих елементів сучасної світової політики, для забезпечення своєї незалежності Україні необхідно і далі удосконалювати та розвивати як правові засади (в тому числі й міжнародні), так і структурну й технічну складову інформаційної безпеки.

Хід роботи

1. Ознайомитися з теоретичними матеріалами по темі.
2. Проаналізувати, яку роль у забезпеченні інформаційної безпеки держави відіграє Державна служба спеціального зв'язку та захисту інформації України.
3. За результатами роботи підготувати звіт
4. Зробити висновки.

Контрольні питання

1. Поняття системи забезпечення інформаційної безпеки.
2. У чому полягає відмінність системи інформаційної безпеки від системи забезпечення інформаційної безпеки?
3. Визначте мету формування системи забезпечення інформаційної безпеки.
4. Окресліть методи забезпечення інформаційної безпеки.
5. Охарактеризуйте забезпечення інформаційної безпеки України в сфері економіки.
6. Охарактеризуйте забезпечення інформаційної безпеки України в сфері внутрішньої та зовнішньої політики.
7. Як тлумачиться забезпечення інформаційної безпеки України у галузі науки та техніки?
8. Як можна охарактеризувати забезпечення інформаційної безпеки України у загальнодержавних інформаційних і телекомунікаційних системах?
9. Дайте визначення поняття «право на інформацію».
10. Як співвідносяться поняття «право на інформацію», «інформаційні права» ?
11. Яка структура конституційного права на інформацію?
12. Назвіть основні права та свободи в інформаційній сфері, що закріплюються Конституцією України.
13. Що Ви вважаєте слід зробити для створення надійної системи забезпечення інформаційної безпеки і захисту інформаційної сфери суспільства?
14. Які базові засади інформаційної безпеки нашої держави закладено у статтях 17, 19, 31, 32, 34, 50, 57 та 64 Конституції України?
15. Які правові основи інформаційної діяльності закладено у Закон України «Про інформацію»?
16. Надайте визначення інформації згідно зі ст. 1 Закону України «Про інформацію».
17. Які основні види інформації визначаються у Законі України «Про інформацію»?
18. Як поділяється інформація за режимом доступу до неї?
19. Як здійснюється контроль за режимом доступу до інформації?
20. Як поділяється за своїм правовим режимом інформація з обмеженим доступом?
21. Яка інформація відноситься до конфіденційної?
22. Яка інформація не може бути конфіденційною?
23. Яка інформація відноситься до таємної інформації?
24. Чим та як визначається інформація, що складає державну таємницю?

25. Чим визначається ступень таємності інформації?
26. Які грифи таємності можуть надаватися інформації та який їх терміни дії?
27. Яка інформація входить до інформаційних ресурсів України?
28. Чим забезпечується інформаційний суверенітет України?

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Арістова І.В. Державна інформаційна політика: організаційно-правові аспекти / МВС України, Ун-т внут. справ - Х., 2010. -366с.

2. Бабак В.П., Теоретичні основи захисту інформації : Підручник. – К.: НАУ, 2008. – 752 с.

3. Бабак В.П., Корченко О.Г. Інформаційна безпека та сучасні мережеві технології: Англо-українсько-російський словник термінів / – К.:НАУ, 2003. – 670 с.

4. Богуш В. Інформаційна безпека держави/ Володимир Богуш, Олександр Юдін,;// Гол. ред. Ю. О. Шпак. - К.: "МК-Прес", 2005. - 432 с.

5. Бурячок, В. Л. Основи формування державної системи кібернетичної безпеки: Монографія. – К.:НАУ, 2013. – 432 с.

6. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. – К.: ДУТ, 2015.— 288 с.

7. Гончарова Л.Л., Возненко А.Д., Стасюк О.І., Коваль Ю.О. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах. – К., 2013. – 435 с., іл.160.

8. Горбенко І.Д. Гриненко Т.О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації. – Х.: ХНУРЕ, 2004. – 368 с.

9. Глобалізація і безпека розвитку / [Білорус О. Г., Гончаренко М. О., Зленко В. А. та ін.]; НАН України, Київ. нац. екон. ун-т. - К.: КНЕУ, 2011. - 733 с.

10. Гнатюк С.О. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи. // Безпека іііформаїііі. – 2013. Том 19, № 2 (2013) – С 118-129.

11. Гуцалюк М. Інформаційна безпека України: нові загрози / Гуцалюк М. // Бизнес и безопасность. - 2003. - № 5. - С. 2-3.

12. Дронь М.М., Малайчук В.П., Петренко О.М. Основи теорії захисту інформації: Навч. посібник. – Д.: Вид-во Дніпропетр. ун-ту, 2001. – 312 с.

13. Інформаційна безпека держави: підручник / [В.М. Петрик. М.М. Присяжнюк., Д.С. Мельник та ін.]; в 2 т. Т. 1. / за заг. ред. В.В. Остроухова - К.: ДНУ «Книжкова палата України». 2016. 264 с.

14. Інформаційна безпека сучасного суспільства: Навчальний посібник / За заг. ред. А. І. Міночкіна. - К.: ВІТІ НТУУ "КПІ", 2006. - 188 с.

15. Кавун С. В. Інформаційна безпека. Навчальний посібник / С. В. Кавун, В.В. Носов, О.В. Манжай. — Харків: Вид. ХНЕУ, 2007. — 352 с. (Укр. мов.)

16.Кормич Б. Інформаційна безпека: організаційно-правові основи: Навчальний посібник / Борис Кормич,. -К.: Кондор, 2005. -382 с.

17. В.А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський. Інформаційна безпека України в умовах євроінтеграції: Навчальний посібник. — К.: КНТ, 2006. — 280 с.

18. Ліпкан В.А. Управління системою національної безпеки України. — К.: КНТ, 2006. — 68 с (Серія: Національна і міжнародна безпека).

19. Маракова І. Захист інформації: Підручник для вищих навчальних закладів/ Ірина Маракова, Анатолій Рибак, Юрій Ямпольский;// Мін-во освіти і науки України, Одеський держ. політехнічний ун-т, Ін-т радіоелектроніки і телекомунікацій. - Одеса, 2001. -164 с.

20.Мехед Д. Б. Аналіз загроз інформаційної безпеки в мережах стандарту IEEE 802.11 / Д. Б. Мехед, В. М. Базилевич, Ю. М. Ткач, Т. А. Петренко // Захист інформації . – К.: НАУ, 2015. – Т. 17, № 4. – С. 274 - 278.

21.Мехед Д. Б. Захист інформації в комп'ютерних мережах / Д. Б. Мехед // Технічні науки та технології: науковий журнал / Черніг. нац. технол. ун-т. – Чернігів, 2015. – N 2 (2). – С. 140 - 146.

22. Д. Мехед, Ю. Ткач, В. Базилевич, В. Гур'єв, Я. Усов, "Аналіз вразливостей корпоративних інформаційних систем", Захист інформації, ТОМ 20, №1, С. 61- 66, 2018.

23. Почепцов Г.Г. Інформаційна політика / Г.Г.Почепцов. С.А.Чукут. – К.: Знання. 2008. – 663 с.

24. Правове забезпечення інформаційної діяльності в Україні / Володимир Горобцов, Андрій Колодюк, Борис Кормич та ін.; Ред. І. С. Чиж;// Ін-т держави і права ім. В.М.Корецького, Нац. Академія Наук України, Держ. комітет телебачення і радіомовлення України. -К.: Юридична думка, 2006. – 384 с.

25. Про внесення змін до Закону України «Про інформацію»: Закон України від 13.01.2011 р. № 2938-VI // Офіційний вісник України. – 2011. – № 10.

26. Про державну службу спеціального зв'язка та захисту інформації: за станом на 07.08.2011 р. / Закон, затверджений ВР України 23 лютого 2006 року, № 3475-1V. - Офіц. вид. - К.: Урядовий кур'єр від 11.04.2006, № 68.

27. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25.02.2017 р. № 47/2017 // Офіційний вісник Президента України. – 2017. – № 5. – С. 15.

28. Про доступ до публічної інформації: Закон України від 13.01.2011 р. № 2939-VI // Відомості Верховної Ради України. – 2011. – № 32. – Ст. 314.

29. Про захист інформації в інформаційно-телекомунікаційних системах: за станом на 30.04.2009 р. / Закон, затверджений ВР України 05.07.1994, №80/94-ВР. - Офіц. вид. - К.: Відомості Верховної Ради України від 02.08.1994.

30. Про інформацію: за станом на 09.05.2011 р. / Закон, затверджений ВР України 02.10.1992, № 2657-ХП. - Офіц. вид. К.: Відомості Верховної Ради України від 01.12.1992.

31. Про основи національної безпеки України: за станом на 20.07.2010 р. / Закон, затверджений ВР України 19 червня 2003 р., №964-IV.- К: Урядовий кур'єр від 30.07.2003, № 139.

32. Про Стратегію національної безпеки України: за станом на 12.02.2007 р. / Указ Президента України від 12.02.2007 р., № 105/2007. Офіц. вид. - К.: Урядовий кур'єр від 07.03.2007, № 43.

33. Про телекомунікації: за станом на 15.10.2011 р. / Закон, затверджений ВР України, 18.11.2003, № 1280-IV. - Офіц. вид. - К: Урядовий кур'єр від 24.12.2003, № 243.

34. Рибальський О.В., Хахановський В.Г., Кудінов В.А. Основи інформаційної безпеки та технічного захисту інформації. Посібник для курсантів ВНЗ МВС України. – К.: Вид. Національної академії внутріш. справ, 2012. – 104 с.