МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРНІГІВСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ

Навчальний посібник

Ніжин
2018

УДК 004.056.5;061.68;681.518 (075.8)
І-74

Рекомендовано до друку вченою радою Чернігівського національного технологічного університету (протокол № 7 від 02.07.2018 р.)

Рецензенти:
С.В. Казмірчук; д-р техн. наук, доцент;
С.В. Зайцев, д-р техн. наук, доцент.

І-74 **Інформаційна безпека держави**: навч. посіб. для студ. спец. 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека»/ В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. – 166 с. : іл.

ISBN 978-617-7609-22-2

У навчальному посібнику викладено основні поняття інформаційної безпеки держави. Проведено класифікацію загроз для інформаційної безпеки держави, суспільства та особи. Визначено особливості та основні форми інформаційного протиборства. Викладено загальні поняття безпеки інформаційних ресурсів. Розглянуті способи побудови інформаційно-комунікаційних систем і мереж на основі сучасних способів передачі й обробки інформації та способи захисту інформації в інформаційних системах і мережах. Проведено аналіз політики та системи забезпечення інформаційної безпеки України. Наведено документи нормативно-правового забезпечення інформаційної безпеки України. Усі матеріали, які надруковані в цьому навчальному посібнику, надані виключно для використання в освітніх цілях.

Навчальний посібник призначено для студентів технічних спеціальностей вищих навчальних закладів із напряму підготовки 6.170103 «Управління інформаційною безпекою» та спеціальності 125 «Кібербезпека». Також може бути корисним для аспірантів, науковців, практичних працівників тощо.

УДК 004.056.5;061.68;681.518 (075.8)

ISBN 978-617-7609-22-2

Навчально-методичне видання

В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ

Навчальний посібник

В авторській редакції

Відповідальний за випуск – *Лук'яненко В.В.*

Підписано до друку 15.01.2019 р.
Формат 60х 84/16. Папір офсетний. Друк числовий.
Гарнітура Times New Roman. Обл.-вид. арк. 14,13.
Ум. друк. арк. 9,65. Тираж 300 прим.
Зам. № 560.

Віддруковано з оригінал-макету замовника

Видавець - ФОП Лук'яненко В.В. ТПК «Орхідея»

*Свідоцтво про внесення суб'єкта видавничої справи
до державного реєстру видавців, виготівників
і розповсюджувачів видавничої продукції
серія ДК № 3020 від 02.11.2007 р.*

*16600, Чернігівська обл., м. Ніжин, вул. Небесної сотні, 13 а.
Тел.: 068 815 06 60
E-mail: holdingvv@ gmail.com*

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ 5
ВСТУП 6
РОЗДІЛ 1. ЗАГАЛЬНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ 8
1.1. Поняття інформаційної безпеки держави, суспільства та особи 8
1.1.1. Інформаційна безпека (поняття і визначення) 8
1.1.2. Підходи до визначення поняття «інформаційна безпека» 10
1.1.3. Інтереси особи, суспільства та держави в інформаційній сфері 12
1.1.4. Об'єкти, суб'єкти та види інформаційної безпеки 12
1.1.5. Співвідношення понять інформаційної та кібербезпеки 13
Питання для самоконтролю 18
1.2. Небезпеки для інформаційної безпеки держави, суспільства та особи 19
1.2.1. Поняття загроз інформаційній безпеці 19
1.2.2. Види загроз інформаційній безпеці 20
1.2.3. Фактори загроз інформаційній безпеці 22
1.2.4. Джерела загроз інформаційній безпеці 22
1.2.5. Етапи розвитку засобів інформаційних комунікацій 25
Питання для самоконтролю 26
1.3. Принципи, форми та методи забезпечення інформаційної безпеки держави 27
1.3.1. Основні принципи забезпечення інформаційної безпеки держави 27
1.3.2. Основні форми забезпечення інформаційної безпеки держави 28
1.3.3. Методи забезпечення інформаційної безпеки 29
Питання для самоконтролю 33
1.4. Поняття та зміст інформаційного протиборства 34
1.4.1. Основні форми інформаційного протиборства 34
1.4.2. Основні форми інформаційної війни 37
1.4.3. Інформаційна зброя в інформаційній війні 41
Питання для самоконтролю 47
1.5. Основи теорії інформаційної боротьби 48
1.5.1. Зміст теорії інформаційної боротьби 48
1.5.2. Закони та закономірності інформаційної боротьби 50
1.5.3. Принципи інформаційної боротьби 51
1.5.4. Заходи інформаційної боротьби 52
1.5.5. Способи інформаційної боротьби 54
1.5.6. Форми ведення інформаційної боротьби 56
1.5.7. Методологія оцінки ефективності інформаційної боротьби 58
Питання для самоконтролю 59
РОЗДІЛ 2. ОСНОВИ БЕЗПЕКИ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ 60
2.1. Основи безпеки інформаційних ресурсів 60
2.1.1. Поняття та загальні властивості інформації. Поняття загроз 60
2.1.2. Загрози безпеки інформації та інформаційних ресурсів 63
2.1.3. Джерела загроз безпеці інформації 65
2.1.4. Класифікація вразливостей безпеки 66
2.1.5. Моделі порушень інформаційних ресурсів 67
2.1.6. Побудова моделі порушника 71
Питання для самоконтролю 74
2.2. Забезпечення безпеки інформації та інформаційних ресурсів 75
2.2.1. Основні напрями забезпечення безпеки інформації 75

2.2.2. Правовий захист ... 75
2.2.3. Організаційний захист ... 79
2.2.4. Інженерно-технічний захист ... 83
Питання для самоконтролю ... 89
2.3. Захист інформаційних систем ... 90
2.3.1. Джерела конфіденційної інформації ... 90
2.3.2. Інформаційна система як об'єкт захисту інформації ... 92
2.3.3. Рівні захисту інформаційних систем ... 94
2.3.4. Аналіз вразливостей корпоративних інформаційних систем ... 97
2.3.5. Основні принципи захисту інформації ... 101
Питання для самоконтролю ... 102
2.4. Інформаційно-комунікаційні системи та комп'ютерні мережі ... 103
2.4.1. Визначення інформаційно-комунікаційних систем ... 103
2.4.2. Захист інформації в комп'ютерних мережах ... 104
2.4.3. Безпека інформаційних ресурсів у ІКСМ на базі ISO/IEC ... 110
2.4.4. Задачі організації безпеки інформації та інформаційних ресурсів ... 111
Питання для самоконтролю ... 113
2.5. Основи управління інформаційною безпекою ... 114
2.5.1. Політика інформаційної безпеки організації ... 114
2.5.2. Основні правила інформаційної безпеки організації ... 117
2.5.3. Заходи управління інформаційною безпекою ... 122
Питання для самоконтролю ... 123
РОЗДІЛ 3. ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ ... 124
3.1. Забезпечення інформаційної безпеки України ... 124
3.1.1. Інформаційна безпека і її місце в системі національної безпеки України ... 124
3.1.2. Основні реальні та потенційні загрози інформаційній безпеці України ... 126
3.1.3. Стан та перспективи розвитку інформаційної безпеки України ... 130
Питання для самоконтролю ... 137
3.2. Система та політика забезпечення інформаційної безпеки України ... 138
3.2.1. Основні функції системи забезпечення інформаційної безпеки України ... 138
3.2.2. Мета функціонування та завдання системи забезпечення інформаційної безпеки ... 140
3.2.3. Органи забезпечення інформаційної безпеки і захисту інформації ... 143
3.2.4. Особливості забезпечення інформаційної безпеки України в різних сферах суспільного життя ... 144
Питання для самоконтролю ... 146
3.3. Інформаційна безпека України у сфері прав і свобод людини ... 147
3.3.1. Забезпечення захисту прав і свобод людини в інформаційній сфері ... 147
3.3.2. Види інформаційних прав і свобод і їх зв'язок з іншими правами та свободами людини та громадянина ... 148
3.3.3. Структура конституційного права на інформацію ... 149
3.3.4. Нормативно-правове забезпечення інформаційної безпеки України ... 151
Питання для самоконтролю ... 163
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ ... 164

21. Мехед Д. Б. Захист інформації в комп'ютерних мережах. *Технічні науки та технології*: науковий журнал. 2015. № 2 (2). С. 140 – 146.

22. Мехед Д., Ткач Ю., Базилевич В., Гур'єв В., Усов Я. Аналіз вразливостей корпоративних інформаційних систем. *Захист інформації*. 2018. № 1. С. 61 – 66.

23. Про внесення змін до Закону України «Про Державну службу спеціального зв'язку та захисту інформації України»: Закон України від 9 квітня 2014 року № 1194-VII. *Голос України.* 2014. 16 травня (№ 93).

24. Про державну таємницю: поточна редакція – Редакція від 05.08.2018, підстава – 2509 –VIII. / Закон, затверджений ВР України 21 січня 1994 року, № 3885-XII. *Голос України* від 10.03.1994.

25. 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.

26. Про доступ до публічної інформації: Закон України від 13.01.2011 р. № 2939-VI. *Відомості Верховної Ради України*. 2011. № 32. Ст. 314.

27. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР. *Відомості Верховної Ради України.* 1994. № 31. Ст. 286.

28. Про інформацію: Закон України від 02.10.1992 № 2657-XII. *Відомості Верховної Ради України.* 1992. № 48. Ст. 650.

29. Про науково-технічну інформацію: Закон України від 25.06.1993 № 3322-XII. *Відомості Верховної Ради України.* 1993. № 33. Ст. 345.

30. Про національну безпеку України: Закон України 21 червня 2018 р. № 2469-VIII. *Голос України.* 2018. 7 липня (№ 122).

31. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»: Указ Президента України від 26.05.2015 р. № 287/2015. *Урядовий кур'єр.* 2015. 29 травня (№ 95).

32. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15.03.2016 року № 96/2016. *Урядовий кур'єр.* 2016. 18 березня (№ 52).

33. Про телекомунікації: Закон України від 18.11.2003 № 1280-IV. *Урядовий кур'єр*. 2003. 24 грудня (№ 243).

34. Рибальський О. В., Хахановський В. Г., Кудінов В. А. Основи інформаційної безпеки та технічного захисту інформації: посібник для курсантів ВНЗ МВС України. Київ: Вид-во Національної академії внутрішніх справ, 2012. 104 с.

35. Юдін О. К. Інформаційна безпека. Нормативно-правове-забезпечення: підручник. Київ: Видавництво Національного авіаційного університету «НАУ-друк», 2011. 640 с.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Арістова І. В. Державна інформаційна політика: організаційно-правові аспекти. Харків, 2010. 366 с.

2. Бабак В. П. Теоретичні основи захисту інформації: підручник. Київ: НАУ, 2008. 752 с.

3. Бабак В. П., Корченко О. Г. Інформаційна безпека та сучасні мережеві технології: Англо-українсько-російський словник термінів. Київ: НАУ, 2003. 670 с.

4. Богуш В., Юдін О. Інформаційна безпека держави / голов. ред. Ю. О. Шпак. Київ: «МК-Прес», 2005. 432 с.

5. Бурячок В. Л. Основи формування державної системи кібернетичної безпеки: монографія. Київ: НАУ, 2013. 432 с.

6. Бурячок В. Л., Гулак Г. М., Толубко В. Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: підручник. Київ: ТОВ «СІК ГРУП Україна», 2015. 449 с.

7. Гончарова Л. Л., Возненко А. Д., Стасюк О. І., Коваль Ю. О. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах. Київ, 2013. 435 с.

8. Глобалізація і безпека розвитку / Білорус О. Г. та ін.; НАН України; Київ. нац. екон. ун-т. Київ: КНЕУ, 2011. 733 с.

9. Гнатюк С. О. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи. *Безпека інформації*. 2013. Т. 19, № 2. С 118 – 129.

10. Дудикевич В. Б., Опірський І. Р., Гаранюк П. І., Зачепило В. С., Партика А. І. Забезпечення інформаційної безпеки держави: навч. посіб. Львів: Видавництво Львівської політехніки, 2017. 204 с.

11. Інформаційна безпека держави: підручник: в 2 т. Т. 1. / В.М. Петрик та ін.; за заг. ред. В.В. Остроухова. Київ: ДНУ «Книжкова палата України», 2016. 264 с.

12. Інформаційна безпека сучасного суспільства: навчальний посібник / за заг. ред. А. І. Міночкіна. Київ: ВІТІ НТУУ «КПІ», 2006. 188 с.

13. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / за заг. ред. д-ра техн. наук, професора В. Б. Толубка. Київ: ДУТ, 2015. 288 с.

14. Кавун С. В., Носов В. В., Манжай О. В. Інформаційна безпека: навчальний посібник. Харків: Вид-во ХНЕУ, 2007. 352 с.

15.Кормич Б. Інформаційна безпека: організаційно-правові основи: Навчальний посібник. Київ: Кондор, 2005. 382 с.

16. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції: навчальний посібник. Київ: КНТ, 2006. 280 с.

17. Ліпкан В. А. Управління системою національної безпеки України. Київ: КНТ, 2006. 68 с. (Серія: Національна і міжнародна безпека).

18. Лісовська Ю. П. Інформаційна безпека України: навч. посіб. Київ: Кондор, 2018. 172 с.

19. Маракова І., Рибак А., Ямпольский Ю. Захист інформації: підручник для вищих навчальних закладів. Одеса, 2001. 164 с.

20. Мехед Д. Б., Базилевич В. М., Ткач Ю. М., Петренко Т. А. Аналіз загроз інформаційної безпеки в мережах стандарту IEEE 802.11. *Захист інформації*. Київ, 2015. Т. 17, № 4. С. 274 – 278.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АРМ - автоматизоване робоче місце
АСОІ - автоматизована система обробки інформації
АСУ - автоматизована система управління
БД (БнД) - база даних (банк даних)
ДРР - дешифрувально-розвідувальна робота
ЕОМ - електронна обчислювальна машина
ЗІ - захист інформації
ЗМІ - засоби масової інформації
ЗПЗ - загальне програмне забезпечення
ІзОД - інформація з обмеженим доступом
ІБ - інформаційна безпека
ІКТ - інформаційно-комунікаційна технологія
ІКСМ - інформаційно-комунікаційні системи та мережі
ІПБ - інформаційно-психологічна безпека
ІТ - інформаційна технологія
ІР - інформаційний ресурс
ІТС - інформаційно-телекомунікаційна система
ІС - інформаційна система
КБ - кібернетична безпека
КР - кібернетична розвідка
КбП - кіберпростір
КСЗІ - комплексна система захисту інформації
ЛОМ - локальна обчислювальна мережа
МОІ - мережа обміну інформацією
МОС - Міжнародна організація стандартизації
МР - мережева розвідка
НСД - несанкціонований доступ
ОЗП - оперативний запам'ятовуючий пристрій
ОС - операційна система
ПАК - програмно-апаратний комплекс
ПЗ - програмне забезпечення
ПІБ - політика інформаційної безпеки
ПК - персональний комп'ютер
ПРД - правила розмежування доступу
РІ - розвідувальна інформація
РІТС - розвідка інформаційно-телекомунікаційних систем
Рст - робоча станція
СІ - соціальний інжиніринг
СЗІ - система захисту інформації
СЗІБ - система забезпечення інформаційної безпеки
СПЗ - спеціальне програмне забезпечення
СУБД - системи управління базами даних
ТЗІ - технічний захист інформації
ФВБ - функціональна вимога безпеки

ВСТУП

За час свого існування людство пережило багато інформаційних революцій, вони стали причиною перетворень суспільних відношень через значні зміни у сфері обробки інформації. Наслідком подібних перетворень, зазвичай ставало надбання людством нової якості в процесі своєї еволюції. З кожним роком інформаційні системи ускладнюються, інформаційна безпека й політика набувають усе більш глобальний характер, виходячи на перший план. У XXI ст. виникло багато проблем, пов'язаних з інформаційною безпекою. Процеси глобалізації дуже гостро дали про себе знати й, крім позитивних елементів, виникли серйозні негативні явища, до яких світова спільнота виявилася неготовою. Головною умовою роботи державного службовця повинні бути знання про інформаційну безпеку, її структурні складові та критерії. З кожним роком стає нагальною роль інформаційної безпеки, оскільки суспільство вступає в епоху інформаційних війн, при яких цінність інформації зростає в багато разів. При цьому інформація – це не тільки товар, а й інструмент маніпуляції суспільством, думкою громадян, створенню конфліктів. Отже, як людина потребує захисту від інформації, так і інформація потребує захисту від людини. Особливо зростає роль інформаційної безпеки у сфері високих технологій, бо саме цифрова інформація стає одночасно і сировиною, і продуктом, яку виробляють, обробляють, продають та, на жаль, частіше крадуть. Здебільшого нині визначають інформаційну безпеку через комп'ютерну безпеку. Дійсно, величезні обсяги інформації, що містяться на електронних носіях дедалі відіграють усе більшу роль у сучасному світі. Але ця інформація дуже вразлива, що зумовлене її великими обсягами, багатозначністю, можливістю «інформаційних диверсій», анонімністю доступу. Захист інформації, що розміщена в середовищі комп'ютера – це набагато складніше, ніж збереження таємниці звичайного поштового листування. Враховуючи це, можна зробити висновок, що проблеми інформаційної безпеки надзвичайно актуальні й потребують поглибленого вивчення.

У науковій літературі відсутній єдиний усталений погляд на зміст поняття «інформаційна безпека». Існує необхідність уточнення поняття інформаційної безпеки, яке сприятиме осмисленню перспективних змін інформаційної безпеки та дозволить повніше розкрити її зміст та надання йому більш широкого й системного характеру.

Сьогодні провідні спеціалісти з цього питання ведуть дискусію, зокрема навколо характеристик небезпек та їхньої структури, принципів побудови системи забезпечення національної безпеки. Система інформаційної безпеки повинна відображати стан захищеності інтересів держави або суспільства, а також окремої людини в інформаційній сфері від загроз не тільки зовнішніх, а також і внутрішніх. При цьому система інформаційної безпеки – елемент у системі більш високого рівня – міжнародного та національного.

Для того щоб національна безпека України могла відповідати рівню провідних економічних держав, необхідні як послідовні дії з боку держави, спрямовані на підвищення ефективності й розвиток системи взаємодії учасників ІКТ-галузі та забезпечення безпеки критично важливих об'єктів інформаційної та кіберінфраструктур, так і приділення підприємствами та організаціями нашої держави більшої уваги до питань власної інформаційної й кібербезпеки.

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.

Питання для самоконтролю

1. Дайте визначення поняття «право на інформацію».
2. Як співвідносяться поняття «право на інформацію», «інформаційні права» ?
3. Яка структура конституційного права на інформацію?
4. Назвіть основні права та свободи в інформаційній сфері, що закріплюються Конституцією України.
5. Що Ви вважаєте слід зробити для створення надійної системи забезпечення інформаційної безпеки і захисту інформаційної сфери суспільства?
6. Які правові основи інформаційної діяльності закладено у Закон України «Про інформацію»?
7. Дайте визначення інформації згідно зі ст. 1 Закону України «Про інформацію».
8. Які основні види інформації визначаються в Законі України «Про інформацію»?
9. Як поділяється інформація за режимом доступу до неї?
10. Як здійснюється контроль за режимом доступу до інформації?
11. Як поділяється за своїм правовим режимом інформація з обмеженим доступом?
12. Яка інформація відноситься до конфіденційної?
13. Яка інформація відноситься до таємної інформації?
14. Чим та як визначається інформація, що складає державну таємницю?
15. Чим визначається ступінь таємності інформації?
16. Які грифи таємності можуть надаватися інформації та який їх терміни дії?
17. Яка інформація входить до інформаційних ресурсів України?
18. Чим забезпечується інформаційний суверенітет України?
19. Які засади інформаційної безпеки держави закладено у Закон України «Про національну безпеку України»?
20. Які види планування закладено у Закон України «Про національну безпеку України»?
21. Які є документи довгострокового планування?
22. Які є документи середньострокового планування?
23. Що передбачає короткострокове планування?

Міністр внутрішніх справ України призначається на посаду ВР за поданням Прем'єр-міністра України. Діяльність Національної поліції України, Національної гвардії України, Державної прикордонної служби України, Державної служби України з надзвичайних ситуацій і Державної міграційної служби України спрямовується і координується Кабінетом міністрів через Міністра внутрішніх справ України. Визначено, що в мирний час Нацгвардія входить до складу сил безпеки і виконує правоохоронні функції, а також розвиває спроможності, необхідні для виконання завдань у складі сил оборони. Після запровадження воєнного стану Національна гвардія приводиться в готовність до виконання завдань за призначенням в умовах дії правового режиму воєнного стану, входить до складу сил оборони. Стратегічне керівництво Нацгвардією здійснює президент України через Генеральний штаб Збройних сил України, про що зазначається в указі президента про введення воєнного стану, який затверджується Верховною Радою.

Планування у сферах національної безпеки й оборони поділяється на довгострокове (понад п'ять років), середньострокове (до п'яти років) та короткострокове (до трьох років):

– документами довгострокового планування є Стратегія національної безпеки України, Стратегія воєнної безпеки України, Стратегія громадської безпеки та цивільного захисту України, Стратегія розвитку оборонно- промислового комплексу України, Стратегія кібербезпеки України, Національна розвідувальна програма;

– документами середньострокового планування є інші стратегічні документи, програми щодо розвитку складових сектору безпеки і оборони, зокрема оснащення їх сучасним озброєнням і військовою технікою, створення необхідних запасів матеріально-технічних засобів та необхідних для цього потужностей оборонно-промислового комплексу, реалізація інших заходів з посилення обороноздатності держави;

– короткострокове планування передбачає щорічне розроблення планів утримання та розвитку (діяльності) складових сектору безпеки і оборони, основних показників державного оборонного замовлення (на трирічний період), у яких визначаються завдання щодо реалізації документів довгострокового і середньострокового планування.

Основні принципи, норми та положення прийнятих законів та підзаконних актів відповідають загальноприйнятим міжнародно-правовим стандартам, у тому числі міжнародним конвенціям із 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 перебувають у постійному розвитку.

Метою посібника є надання необхідних теоретичних основ для засвоєння курсу майбутніми фахівцями з управління інформаційною безпекою та кібербезпеки й закріплення необхідних у подальшій роботі знань з основ інформаційної безпеки.

Матеріал дисципліни тісно пов'язаний зі спеціальними дисциплінами, що викладаються у закладах вищої освіти технічного профілю.

У першому розділі посібника розглянуто: основні поняття, об'єкти, суб'єкти та види інформаційної безпеки; види і класифікації загроз, дестабілізуючих факторів; методів та засобів забезпечення інформаційної безпеки держави. Розглянуті питання співвідношення понять інформаційної та кібербезпеки. Викладено поняття та зміст інформаційного протиборства, а також основи теорії інформаційної боротьби.

Другий розділ присвячено вивченню основ безпеки інформаційних технологій та інформаційних ресурсів. Викладено основні поняття організації безпеки інформаційних ресурсів. Розглянуто способи побудови інформаційно-комунікаційних систем та мереж на основі сучасних способів передачі й обробки інформації, а також режими роботи комп'ютерних мереж.

У третьому розділі показані основні загрози суспільству та інформаційному ресурсу України, що мають місце в нашій сучасності. Розглянута система та політика забезпечення інформаційної безпеки України. Викладено нормативно-правову складову процесу організації та становлення в Україні всієї структури інформаційної безпеки. Розглянуто основні концепції, які визначають сучасний стан та подальший розвиток національної та, як її складової, інформаційної безпеки України. Наведено нормативно-правові методи інформаційної безпеки з урахуванням вітчизняних та міжнародних стандартів.

В основу викладу дисципліни покладено матеріали декількох відомих публікацій. Це, зокрема, навчальний посібник В. М. Богуша та О. К. Юдина з курсу «Інформаційна безпека держави», а також підручник «Інформаційна безпека держави» за загальною редакцією В. В. Остроухова.

Використовувалися також наукові статті та методичні розробки викладачів кафедри кібербезпеки та математичного моделювання Чернігівського національного технологічного університету.

Навчальний посібник «Інформаційна безпека держави» може бути корисним також для студентів інших спеціальностей, які вивчають методи захисту інформації, заснованих на науково обґрунтованому аналізі ситуації та доступі до систем збору, зберігання й обробки інформації.

Підручник має передусім спонукати читачів до самостійного пошуку практичних заходів із протидії сторонньому кібернетичному впливу за тих чи інших конкретних умов.

Поглибленому опрацюванню матеріалу підручника сприятиме добірка питань для самоконтролю, якою завершується кожна його тема.

Усі матеріали, які надруковані в цьому навчальному посібнику, надані виключно для використання в освітніх цілях.

РОЗДІЛ 1. ЗАГАЛЬНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

1.1. Поняття інформаційної безпеки держави, суспільства та особи

1.1.1. Інформаційна безпека (поняття і визначення)

Дослідження такого складного явища, як інформаційна безпека, може бути успішним лише за умови наявності розробленого понятійного апарату. Головною складовою цього апарату є система понять, завдяки яким розкриваються сутнісні моменти досліджуваного явища.

Розглянемо основні поняття, визначення і терміни.

Інформація:

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

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

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

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

Інформаційний простір (національний):

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

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

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

Інформаційні ресурси:

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

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

Закон вказує, що загрози національній безпеці України та відповідні пріоритети державної політики у сферах національної безпеки та оборони визначаються у Стратегії національної безпеки України, Стратегії воєнної безпеки України, Стратегії кібербезпеки України, інших документах з питань національної безпеки та оборони, які схвалюються Радою національної безпеки та оборони й затверджуються указами Президента України.

Значна увага приділяється цивільному, у тому числі громадському контролю. Законодавчий акт визначає сфери відповідальності Президента України, Ради національної безпеки та оборони, Верховної Ради, Кабінету міністрів. Відповідна стаття закону визначає, що громадські об'єднання можуть, зокрема отримувати від державних органів інформацію з питань діяльності складових сектору безпеки та оборони, крім інформації з обмеженим доступом; проводити громадську експертизу проектів законів, рішень, програм, представляти свої висновки і пропозиції для розгляду відповідним державним органам. Однією з основних новацій Закону є розмежування цивільно-планувальних та воєнно-операційних функцій сектору оборони. Ідеться про розділення (з 2021 р.) посади начальника Генерального штабу та Головнокомандувача Збройних сил України. Сьогодні це одна посада.

Окрема стаття (тридцята) присвячена стратегії розвитку оборонно-промислового комплексу України. Її реалізація планується «з використанням механізмів державно-приватного партнерства» та із «залученням міжнародної консультативної, фінансової, матеріально-технічної допомоги». Встановлено обсяг видатків на фінансування сектору безпеки і оборони у розмірі не менше 5 % запланованого обсягу внутрішнього валового продукту, з яких не менше 3 % – на фінансування сил оборони.

Керівництво у сферах національної безпеки та оборони здійснює Президент України, який є Верховним головнокомандувачем Збройних сил України та видає накази і директиви з питань оборони; Президент очолює Раду національної безпеки і оборони, звертається з посланнями до народу та із щорічними і позачерговими посланнями до Верховної Ради про внутрішнє і зовнішнє становище України. Крім того, Міністр оборони України призначається на посаду Верховною Радою за поданням Президента з числа цивільних осіб. Перший заступник та заступники міністра оборони призначаються на посади з числа цивільних осіб. У прикінцевих та перехідних положеннях закону визначено, що це положення набирає чинності з 1 січня 2019 року. Головнокомандувач ЗСУ призначається на посаду за поданням Міністра оборони та звільняється з посади Президентом України. Головнокомандувач Збройних сил України підпорядковується Президенту та Міністру оборони. Повноваження головнокомандувача ЗСУ затверджуються Президентом України. При цьому вказано, що лише з 1 січня 2021 року набирає чинності норма щодо головнокомандувача ЗСУ, Генерального штабу Збройних сил України, видів та окремих родів військ (сил).

Протягом особливого періоду Генеральний штаб ЗСУ виконує функції стратегічного керівництва Збройними силами, іншими складовими сил оборони і є робочим органом Ставки верховного головнокомандувача (у разі її створення). Генштаб ЗСУ очолює начальник Генерального штабу ЗСУ, який призначається на посаду і звільняється з посади президентом України за поданням Міністра оборони. Законом визначено склад Збройних сил України - види та окремі роди військ (сил).

Слід додати, що одночасно з створенням правових та організаційних основ ТЗІ були створені правові та організаційні основи криптографічного захисту інформації.

Крім того, були прийняті Закони України «Про телекомунікації», «Про Національну програму інформатизації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про науково-технічну інформацію», а в Кримінальний кодекс України було введено розділ XVI, в якому визначалася відповідальність за злочини в інформаційній сфері.

8 липня 2018 р. набрав чинності Закон України «Про національну безпеку України». У шістьох розділах нового Закону сформульовано принципи державної політики у сферах національної безпеки та оборони. Фундаментальними національними інтересами України визначені:

– державний суверенітет і територіальна цілісність, демократичний конституційний лад, недопущення втручання у внутрішні справи України;

– сталий розвиток національної економіки, громадянського суспільства і держави для забезпечення зростання рівня та якості життя населення;

– інтеграція України в європейський політичний, економічний, безпековий, правовий простір, набуття членства в Європейському Союзі та в Організації Північноатлантичного договору, розвиток рівноправних взаємовигідних відносин з іншими державами.

Сектор безпеки і оборони України складається з чотирьох взаємопов'язаних складових: сили безпеки; сили оборони; оборонно-промисловий комплекс; громадяни та громадські об'єднання, які добровільно беруть участь у забезпеченні національної безпеки.

До складу сектору безпеки і оборони входять:

– Міністерство оборони України
– Збройні Сили України
– Державна спеціальна служба транспорту
– Міністерство внутрішніх справ України
– Національна гвардія України
– Національна поліція України
– Державна прикордонна служба України
– Державна міграційна служба України
– Державна служба України з надзвичайних ситуацій
– Служба безпеки України
– Управління державної охорони України
– Державна служба спеціального зв'язку та захисту інформації України
– Апарат Ради національної безпеки і оборони України
– розвідувальні органи України
– центральний орган виконавчої влади, що забезпечує формування та реалізує державну військово-промислову політику.

Законом визначено роль і місце Збройних сил, Міністерства внутрішніх справ, Служби безпеки, Державної спеціальної служби транспорту, Державної служби спеціального зв'язку та захисту інформації, розвідувальних органів і Управління державної охорони України у сфері безпеки та оборони.

Інформаційні технології:

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

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

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

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

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

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

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

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

Інформаційний продукт (продукція):

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

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

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

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

Інформаційне поле:

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

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

Інформаційне суспільство:

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

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

Інформатизація:

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

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

Інформатика: наукова діяльність, що вивчає інформаційні структури та процеси збирання (набуття, придбання), відображення, реєстрації, накопичення, збереження і поширення (розповсюдження, реалізацію) інформації за допомогою комп'ютерної техніки.

Інформаціологія: новітня загальна фундаментальна наука про інформаційні природні процеси матеріалізації та дематеріалізації в мікро- й макроструктурах Всесвіту, що самоорганізуються.

Інформаційна війна: процес боротьби між суб'єктами із застосуванням інформаційної зброї.

Інформаційна зброя: засоби, які дозволяють здійснювати замислені дії з повідомленнями, що передаються, обробляються, створюються, знищуються і сприймаються.

Інформаційна інфраструктура включає в себе:

– ***організаційні структури***, що забезпечують функціонування і розвиток єдиного інформаційного простору (зокрема, збирання, обробку, збереження, поширення, пошук і передачу інформації). Забезпечувальну частину складають науково-методичне, інформаційне, лінгвістичне, технічне, кадрове забезпечення;

– ***інформаційно-телекомунікаційні структури*** – територіально розподілені державні й корпоративні комп'ютерні мережі, телекомунікаційні мережі й системи спеціального призначення та загального користування, мережі й канали передачі даних, засоби комутації і керування інформаційними потоками;

– ***телекомунікаційні технології;***

– ***системи засобів масової інформації***.

Інформаційна безпека – захищеність (стан захищеності) основних інтересів особи, суспільства і держави у сфері інформації, включаючи інформаційну й телекомунікаційну інфраструктуру і власне ***інформацію*** та її ***параметри***, такі як ***повнота, об'єктивність, доступність і конфіденційність.***

Інформаційна безпека є складовою ***національної безпеки.*** Але особливістю інформаційної безпеки є те, що вона, як невід'ємна частина, входить до інших складових національної безпеки: економічної, воєнної, політичної безпеки тощо.

1.1.2. Підходи до визначення поняття «інформаційна безпека»

Поняття інформаційної безпеки держави, суспільства та особи, залежно від його використання, розглядається в декількох ракурсах.

У найзагальнішому випадку інформаційна безпека – це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави.

– залучення до розв'язання проблем ТЗІ вітчизняних вчених та висококваліфікованих спеціалістів;

– розвиток міжнародного співробітництва у 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;

– 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 із 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;

– 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.

– 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 в 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 із 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 усіх 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;

Більш розгорнуте формулювання інформаційної безпеки – це стан захищеності потреб в інформації особи, суспільства й держави, за якого забезпечується їхнє існування та прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз.

Треба відзначити, що задоволення потреб в інформації приводить до оволодіння відомостями про навколишній світ та процеси, що протікають у ньому, тобто інформованості особи, суспільства та держави. Стан інформованості визначає ступінь адекватності сприйняття суб’єктами навколишньої дійсності і, як наслідок, обґрунтованість рішень та дій, що приймаються.

Дослідження сутності інформаційної безпеки має враховувати той факт, що сутність є внутрішнім змістом предмета, який виражається у стійкій єдності всіх різноманітних і суперечливих формах буття. Базовою характеристикою інформаційної безпеки слід вважати імовірність появи загрози підвищеного ризику реалізації загрози або небезпеки для індивіда, суспільства та держави. Критерієм ефективності забезпечення інформаційної безпеки є високий рівень безпеки при мінімумі відповідних витрат. Отже, можна говорити про структуру поняття інформаційної безпеки. Основним її елементом є життєво важливі інтереси соціальної системи, які співвідносяться із зовнішніми чинниками у вигляді інтересів наднаціональних або інших національно-державних структур у межах міжнародного співтовариства. Зсередини національно-державного утворення його життєво важливі інтереси перебувають у взаємодії з інтересами елементів, які складають це утворення. У ролі останніх виступають соціальні групи, еліта, організації, партії, релігійні та етнічні утворення, рухи тощо. Сукупність внутрішніх і зовнішніх інформаційних загроз створюють передумови для порушення безпечного функціонування системи державного управління.

Вагомість інформаційно-комунікаційних процесів у сучасному світі дає підстави розглядати забезпечення інформаційної безпеки як одне з глобальних і пріоритетних завдань органів державного управління, вирішенню якого мають бути підпорядковані політична, економічна, воєнна, культурна та інші види діяльності системи державного управління.

В інформаційному праві інформаційна безпека – це одна зі сторін розгляду інформаційних відносин у межах інформаційного законодавства з позицій захисту життєво важливих інтересів особи, суспільства, держави та акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами.

Таким чином, визначаючи поняття інформаційної безпеки, можна виокремити декілька підходів окреслення сутності цього феномену, а саме розуміння інформаційної безпеки як:

1. Стану захищеності інформаційного простору.

2. Процесу управління загрозами та небезпеками, що забезпечує інформаційний суверенітет держави.

3. Стану захищеності національних інтересів держави в інформаційному середовищі.

4. Захищеності встановлених законом правил, за якими відбуваються інформаційні процеси в державі.

5. До суспільних відносин, пов'язаних із захистом життєво важливих інтересів людини і громадянина, суспільства та держави від реальних та потенційних загроз в інформаційному просторі.

6. Важливої функції держави.

7. Невід'ємної частини політичної, економічної, оборонної та інших складових національної безпеки.

1.1.3. Інтереси особи, суспільства та держави в інформаційній сфері

Інформаційна сфера – це сфера діяльності суб'єктів, пов'язана із створенням, перетворенням і споживанням інформації. Інформаційна сфера умовно поділяється на три основні предметні частини:

- створення і поширення вихідної та похідної інформації;
- формування інформаційних ресурсів, підготовки інформаційних продуктів, надання інформаційних послуг;
- споживання інформації;

та дві забезпечувальні предметні частини:

- створення і застосування інформаційних систем, інформаційних технологій і засобів їхнього забезпечення;
- створення й застосування засобів і механізмів інформаційної безпеки.

Інтереси особи в інформаційній сфері полягають:

- у реалізації конституційних прав людини та громадянина на доступ до інформації, на використання інформації в інтересах здійснення не забороненої законом діяльності, фізичного, духовного та інтелектуального розвитку;
- у захисті інформації, що забезпечує особисту безпеку.

Інтереси суспільства в інформаційній сфері полягають:

- у забезпеченні інтересів особи в цій сфері;
- у зміцненні демократії;
- у створенні правової соціальної держави;
- у досягненні та підтриманні суспільного спокою;
- у духовному відновленні держави.

Інтереси держави в інформаційній сфері полягають у створенні умов:

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

1.1.4. Об'єкти, суб'єкти та види інформаційної безпеки

Об'єктами інформаційної безпеки можуть бути: інформаційні системи різного масштабу й різного призначення. До соціальних об'єктів інформаційної безпеки звичайно відносять особу, суспільство, державу.

До **суб'єктів інформаційної безпеки** належать:

- держава, що здійснює свої функції через відповідні органи;

- 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 в 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, 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 у 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 у сфері ТЗІ, представлення інтересів України у відповідних міжнародних організаціях;

– 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 із 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 інформаційно-телекомунікаційних 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 із питань ТЗІ, які не містять відомостей, що становлять державну таємницю;

– узгодженість нормативно-правових актів та нормативних документів із 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, у державних установах і організаціях;

– громадяни, суспільні або інші організації й об'єднання, що володіють повноваженнями із забезпечення інформаційної безпеки відповідно до законодавства.

Види інформаційної безпеки:

– особи;

– суспільства;

– держави.

Інформаційна безпека особи – це стан захищеності психіки та здоров'я людини від деструктивного інформаційного впливу, який призводить до неадекватного сприйняття нею дійсності та (або) погіршення її фізичного стану.

Інформаційна безпека суспільства – можливість безперешкодної реалізації суспільством та окремими його членами своїх конституційних прав, пов'язаних із можливістю вільного одержання, створення й поширення інформації, а також ступінь їхнього захисту від деструктивного інформаційного впливу.

Необхідний рівень інформаційної безпеки забезпечується сукупністю політичних, економічних, організаційних заходів, спрямованих на попередження, виявлення й нейтралізацію тих обставин, факторів і дій, які можуть завдати збитків чи зашкодити реалізації інформаційних прав, потреб та інтересів країни та її громадян.

Слід зазначити, що інформаційна безпека особи та суспільства між собою тісно пов'язані. Інформаційна безпека суспільства та його окремих осіб залежить від рівня:

– інтелектуальності, спеціальної теоретичної й практичної підготовки;

– критичного мислення, морального та духовного вдосконалення;

– гармонійного розвитку особи в суспільстві;

– технічних засобів захисту.

Інформаційна безпека держави – це стан її захищеності, при якій спеціальні інформаційні операції, акти зовнішньої інформаційної агресії, інформаційний тероризм, незаконне зняття інформації за допомогою спеціальних технічних засобів, комп'ютерні злочини та інший деструктивний інформаційний вплив не завдає суттєвої шкоди національним інтересам.

1.1.5. Співвідношення понять інформаційної та кібербезпеки

Поступове й доволі умовне поєднання віртуального і реального просторів за допомогою ІТ-систем і мережних технологій різного функціонального призначення, які в процесах обробки, передавання та зберігання інформації використовують електромагнітний спектр і діють як єдине ціле, а також відповідного програмного забезпечення призвело, зрештою, до формування ***кіберпростору*** (рис. 1.1) – високорозвиненої моделі об'єктивної реальності, в якій відомості щодо осіб, предметів, фактів, подій, явищ і процесів:

– подаються в деякому математичному, символьному (як сигнали, знаки, звуки, рухомі або нерухомі зображення) або в будь-якому іншому вигляді;

– розміщуються в пам'яті будь-якого фізичного пристрою, спеціально призначеного для зберігання, обробки й передавання інформації;

– перебувають у постійному русі по сукупності ІТ- систем і мереж.

Уперше термін «кіберпростір» було використано в Конвенції про злочинність у сфері комп'ютерної інформації від 23 листопада 2001 року. Сфера його дії на той час перебувала під впливом загальних механізмів правового регулювання суспільних відносин, обмежуючись специфічними об'єктами й інтересами суб'єктів правовідносин, а також комп'ютерними мережами, за допомогою яких можна брати участь у відповідних правовідносинах.

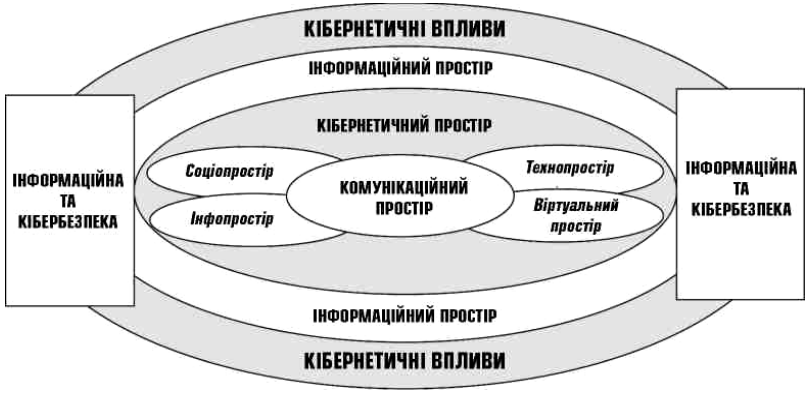

Рис. 1.1. Взаємозв'язок інформаційного та кіберпросторів

Нині кіберпростір має чимало визначень. Серед інших варто також відзначити й такі визначення поняття КбП:

– поліморфний віртуальний простір, що генерує інформаційна система як у формі складних світів, так і у простих реалізаціях (типу електронної пошти, глобальної навігації тощо);

– комунікаційне середовище, утворене системою зв'язків між об'єктами кіберінфраструктури – комп'ютерами, комп'ютерними мережами, програмним забезпеченням та інформаційними ресурсами, використовуване для забезпечення певних інформаційних потреб;

– штучне електронне середовище існування інформаційних об'єктів у цифровій формі, утворене в результаті функціонування кібернетичних комп'ютерних систем управління й обробки інформації, що забезпечує користувачам доступ до обчислювальних та інформаційних ресурсів систем, вироблення електронних інформаційних продуктів, а також обмін електронними повідомленнями, даючи змогу із застосуванням електронних інформаційних образів у режимі реального часу вступати у відносини (взаємодіяти) щодо спільного використання обчислювальних та інформаційних ресурсів системи (надання інформаційних послуг, ведення електронної комерції тощо);

– простір, сформований інформаційно-комунікаційними системами, в якому відбуваються процеси перетворення (створення, зберігання, обміну, обробки та знищення) інформації, поданої у вигляді електронних комп'ютерних даних;

– об'єкти інформаційної інфраструктури, що керуються інформаційними (автоматизованими) системами управління та інформації, що в них циркулює;

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 зумовлюються 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 узгодження інформаційних відносин у сфері ТЗІ 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 в 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;

– 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;

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 уся належна їй інформація, незалежно від змісту, форм, часу й 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.

Згодом з'явилася нагальна необхідність в удосконаленні та розвитку як нормативної, так і науково-технічної бази технічного захисту інформації, що і 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 й іншу передбачену законом таємницю, конфіденційної інформації, а також цілісності та доступності відкритої інформації, важливої для особи, суспільства і держави.

– середовище, утворене організованою сукупністю інформаційних процесів на основі взаємопоєднаних за єдиними принципами та правилами інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем.

Найбільш відмітними ознаками кіберпростору як субстанції, створенню якої сприяли передусім такі чинники: зміна характеру діяльності людини з ухвалення рішень; упровадження електронно-цифрових форм створення, обробки, зберігання та переміщення інформації, перехід від паперового діловодства до електронного тощо; абсолютна більшість фахівців вважає його неперевершені можливості зі створення незліченних зв'язків між окремими індивідами і соціальними групами та з надання різнопланових інформаційних послуг.

З урахуванням характерних особливостей кіберпростору як сфери вчинення заздалегідь спланованих деструктивних дій на кшталт проникнення в ІТС один одного, блокування або виведення з ладу найбільш уразливих елементів цих систем, дезорганізації оборонних автоматизованих систем управління протилежної сторони, систем управління її транспортом і енергетикою, економікою й фінансовою системою тощо (поряд із наземною, морською й повітряно-космічною сферами) і своєрідної сполучної ланки між такими поняттями, як Інтернет і кібернетика, усе це, у свою чергу, дає змогу:

– виокремити в цьому просторі систему певних відношень між суб'єктами та об'єктами інформаційної й кібернетичної інфраструктури;

– охарактеризувати злочини, втручання і загрози, пов'язані з особливостями існування та передавання інформації;

– розглядати кіберпростір із позицій власне віртуального і реального (електронного, комунікаційного, кібернетичного, інформаційного, особливого психологічного) тлумачення як додатковий вимір бойового простору, розрізняючи при цьому фізичний (інфраструктура, кабелі та роутери), семантичний (дані) і синтаксичний (протоколи передавання даних) рівні тощо.

Сучасний стан справ зумовлює небачені досі глибинні зміни у ставленні більшості держав світу до безпеки власного інформаційного та кіберпростору, а отже, і до посиленого захисту інформації, засобів її обробки та кіберсередовища, в якому ця інформація циркулює (рис. 1.2), тобто до вжиття заходів із забезпечення інформаційної та кібербезпеки.

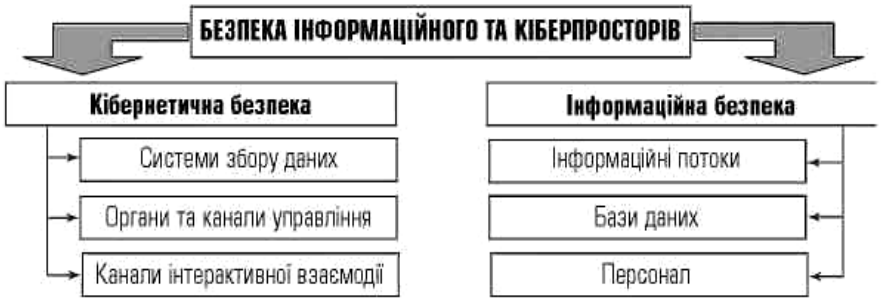

Рис. 1.2. Об'єкти впливу в інформаційному та кіберпросторі

При цьому ***інформаційну безпеку*** в найзагальнішому розумінні можна визначити як *такий стан захищеності інформаційного простору держави, за якого неможливо завдати збитку властивостям об'єкта безпеки, що стосуються інформації та інформаційної інфраструктури, і який гарантує безперешкодне використання й розвиток національної інфосфери в інтересах оборони* (рис. 1.3).

Рис. 1.3. Структура поняття «інформаційна безпека»

Спектр інтересів ІБ щодо інформації, інформаційних систем та інформаційних технологій як об'єктів безпеки можна поділити на такі основні категорії: ***доступність*** – можливість за прийнятний час отримати певну інформаційну послугу; ***цілісність –*** актуальність і несуперечливість інформації, її захищеність від руйнування та несанкціонованого змінювання; ***конфіденційність*** – захищеність від несанкціонованого ознайомлення.

Кібербезпеку (рис. 1.4) можна визначити як *стан захищеності кіберпростору держави загалом або окремих об'єктів її інфраструктури від ризику стороннього кібервпливу, за якого забезпечується їхній сталий розвиток, а також своєчасне виявлення, запобігання й нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним і/або національним інтересам*.

Рис. 1.4. Складові кібернетичної безпеки

Головні проблеми забезпечення кібернетичної безпеки постають із таких причин:

– відсутності чіткого усвідомлення ролі та значення кібербезпекової складової в системі забезпечення національної безпеки держави;

– дефініційної, термінологічної та нормативно-правової неврегульованості у сфері кібербезпеки;

– залежності держави від програмних і технічних продуктів іноземного виробництва;

– відсутності належної координації діяльності відповідних відомств, а отже, і неузгодженості дій зі створення окремих елементів системи кібербезпеки;

– дефіциту щодо методичного забезпечення та кадрового наповнення відповідних структурних підрозділів.

Інформація, що становить військову таємницю – це вид таємної інформації, який охоплює відомості у 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 щодо 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 значущою, 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 відносин, їхні 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 й 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.

Державну інформаційну політику розробляють і здійснюють органи державної влади загальної компетенції, а також відповідні органи спеціальної компетенції.

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 III 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 є у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються на їх бажання 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 й 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 й державі.

Комплексну сутність кібербезпеки за таких умов унаочнює схема, подана на рис. 1.5.

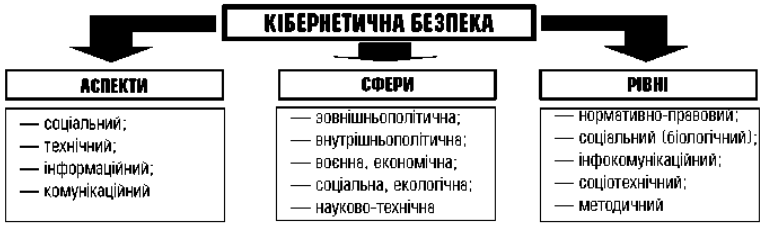

Рис. 1.5. Сутність кібернетичної безпеки

Протягом останніх років Україна, як і більшість країн світу, робить певні кроки в розбудові інформаційного суспільства, забезпечення інформаційної й кібербезпеки, а також у боротьбі з кіберзлочинністю. Нормативно-правову базу в цих сферах діяльності становлять такі документи:

– Конвенція Ради Європи про кіберзлочинність, ратифікована Законом України від 7.09.2005 року № 2824-IV;

– Закони України «Про інформацію», «Про національну безпеку України», «Про Державну службу спеціального зв'язку та захисту інформації України», «Про телекомунікації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про доступ до публічної інформації», «Про оборону України», «Про засади внутрішньої і зовнішньої політики», «Про об'єкти підвищеної небезпеки»;

– Укази Президента України, зокрема про Доктрину інформаційної безпеки, Стратегію національної безпеки України та Воєнну доктрину України;

– окремі положення Кримінального кодексу України, окремі постанови Кабінету Міністрів та рішення РНБОУ.

Практичними кроками щодо реалізації чинної нормативно-правової бази стало створення 2007 року в складі Державної служби спеціального зв'язку та захисту інформації (ДССЗЗІ) України Центру реагування на комп'ютерні інциденти. На виконання статті 35 Конвенції про кіберзлочинність у червні 2009 року при Службі безпеки України на базі спеціального підрозділу для боротьби з кіберзагрозами утворено Національний контактний пункт формату 24/7 щодо реагування та обміну терміновою інформацією про вчинені кіберзлочини. Крім цього, Указом Президента України «Про виклики та загрози національній безпеці України у 2011 році» від 10 грудня 2010 року № 1119/2010 ухвалено рішення щодо початку створення Єдиної загальнодержавної системи протидії кіберзлочинності. Іншим Указом Президента України «Про внесення змін до деяких законів України про структуру і порядок обліку кадрів Служби безпеки України» від 25 січня 2012 року № 34 у структурі СБ України створено Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки. З огляду на ступінь та динаміку поширення комп'ютерних інцидентів теренами України в липні 2010 року у структурі МВС України на базі Департаменту боротьби зі злочинами, пов'язаними з торгівлею людьми, утворено новий структурний підрозділ – Департамент боротьби з кіберзлочинністю і торгівлею людьми.

В законі України «Про національну безпеку України» затверджені такі поняття:

1. Стратегія національної безпеки України – документ, що визначає актуальні загрози національній безпеці України та відповідні цілі, завдання, механізми захисту національних інтересів України та є основою для планування й реалізації державної політики у сфері національної безпеки;

2. Стратегія воєнної безпеки України – документ, у якому викладається система поглядів на причини виникнення, сутність і характер сучасних воєнних конфліктів, принципи і шляхи запобігання їх виникненню, підготовку держави до можливого воєнного конфлікту, а також на застосування воєнної сили для захисту державного суверенітету, територіальної цілісності, інших життєво важливих національних інтересів;

3. Стратегія кібербезпеки України – документ довгострокового планування, що визначає загрози кібербезпеці України, пріоритети та напрями забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави;

4. Стратегія громадської безпеки та цивільного захисту України – документ довгострокового планування, що розробляється на основі Стратегії національної безпеки України за результатами огляду громадської безпеки та цивільного захисту і визначає напрями державної політики щодо гарантування захищеності життєво важливих для держави, суспільства та особи інтересів, прав і свобод людини і громадянина, цілі та очікувані результати їх досягнення з урахуванням актуальних загроз.

Питання для самоконтролю

1. Які основні підходи до визначення поняття «інформаційна безпека» Ви знаєте?
2. Назвіть основні ознаки інформаційної безпеки.
3. Назвіть основні визначення поняття «інформаційна безпека».
4. У чому полягають інтереси особи, суспільства та держави в інформаційній сфері?
5. Назвіть об’єкти, суб’єкти та види інформаційної безпеки.
6. Що таке інформація?
7. Що таке джерело інформації?
8. Які є носії інформації?
9. Що розуміють під інформаційними ресурсами?
10. Що таке загроза інформаційній безпеці?
11. Що таке кіберборотьба? Які основні особливості їй притаманні?
12. Дайте визначення поняття «кібернетична безпека».
13. Назвіть істотні ознаки, які його характеризують.
14. Причини головних проблем забезпечення кібернетичної безпеки.
15. Які стратегії затверджені в Законі України «Про національну безпеку України»?

– 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, де персональні дані про особу віднесені до конфіденційної інформації.

3.3.4. 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, а також у доктрині інформаційної безпеки 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 в суспільстві, державі та навколишньому природному середовищі.

придбання, накопичення інформації громадянами, юридичними особами або державою відповідно до чинного законодавства України. Зберігання інформації – значає 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 цей 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». Стаття 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;

1.2. Небезпеки для інформаційної безпеки держави, суспільства та особи

1.2.1. Поняття загроз інформаційній безпеці

Аналізу змісту поняття «інформаційна безпека» зазвичай дослідниками приділяється значна увага, у той час як такі поняття, як небезпека й загроза розглядаються дещо спрощено та здебільшого у звуженому плані, відірваному від контексту поняття «інформаційна безпека».

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

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

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

– загрози інформаційним правам і свободам особи (праву на виробництво, поширення, пошук, одержання, передавання і використання інформації; праву на інтелектуальну власність на інформацію і речову власність на документовану інформацію; праву на захист честі й гідності тощо).

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 у захисті інформаційних систем, наприклад, неконтрольований доступ до персональних комп'ютерів або неліцензійне програмне забезпечення (на жаль, навіть ліцензійне програмне забезпечення не позбавлене вразливостей).

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. Переважно 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 період 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 й ефективні засоби забезпечення інформаційної безпеки.

1.2.2. Види загроз інформаційній безпеці

Відповідно виділяють такі види загроз.

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 в 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 цього 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 у 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 із 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: можуть у разі їх реалізації

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 насамперед пошук і отримання необхідної інформації. Статтю 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.

3.3.3. 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 в 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,

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 II «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. Загалом 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.

3.3.2. Види інформаційних прав і свобод і їх зв'язок з іншими правами та свободами людини та громадянина

Крім загального визначення права людини на інформацію, у ст. 34 Конституції, є багато 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»);

призвести до колапсу і системної дестабілізації системи; можуть призвести до змін, несумісних 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. Ці загрози є також небезпечними, водночас вони стосуються структури окремих органів державної влади або їхніх компонентів; елементні – загрози, що впливають на окремі елементи структури системи. Такі 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 в 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, крім того, 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 загрозою суб'єктом управління системою безпеки.

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

Загрози можуть мати або об'єктивну природу, наприклад, зміна умов фізичного середовища (пожежі, повені і т. ін.) 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 унаслідок 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 дає змогу одержати дуже просту, зрозумілу й наочну схему для створення моделі загроз.

1.2.3. 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 ситуації 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 поширюють 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 унаслідок 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, які виробляють 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 ситуації, зростання числа комп'ютерних злочинів, особливо в кредитно-фінансовій сфері.

1.2.4. Джерела загроз інформаційній безпеці

З огляду на визначення загроз інформаційній безпеці, можна виділити декілька основних джерел загроз, які можуть стосуватися інтересів особи, суспільства й держави.

3.3. Інформаційна безпека України у сфері прав і свобод людини

3.3.1. Забезпечення захисту прав і свобод людини в інформаційній сфері

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 та преси. Воно значно змістовніше й має власну субстанцію, відіграє свою роль у задоволенні певних інтересів суб'єктів; тому обмеження цього 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», 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 України «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 оскаржувати 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 заподіяння шкоди правам та свободам громадян України.

5. Не підлягають розголошенню відомості, які становлять державну чи іншу передбачену законом таємницю.

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 й радіоелектронної боротьби, методів і засобів активної протидії інформаційно-пропагандистським і психологічним операціям імовірного супротивника.

Забезпечення інформаційної безпеки України в правоохоронній і судовій сферах.

Поряд із загальними методами та засобами захисту інформації застосовуються також специфічні методи і засоби забезпечення інформаційної безпеки в 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.

Питання для самоконтролю

1. Поняття системи забезпечення інформаційної безпеки.
2. Визначте мету формування системи забезпечення інформаційної безпеки.
3. Окресліть методи забезпечення інформаційної безпеки.
4. Які об'єкти системи забезпечення інформаційної безпеки України Ви знаєте?
5. Які можна виділити основні функції системи забезпечення інформаційної безпеки в умовах надзвичайної ситуації?
6. Сформулюйте найважливіші завдання у сфері інформаційної безпеки.
7. Які органи забезпечують інформаційну безпеку й захист інформації?
8. Які завдання у сфері інформаційної безпеки.
9. З чого складається державна система захисту інформації?

Джерела загроз інформаційній безпеці особи.

Інтереси особи, 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 захисті 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 навколо 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 із формування особистості, так 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.

Загалом структура споживчо-мотиваційної сфери особи утворюється базовими потребами, зумовленими його генотипом (в їжі, особистій безпеці, потреба в продовженні роду, довголітті, а також потребами у спілкуванні з іншими людьми), похідними потребами, що формуються діючою системою виховання. Способи і форми задоволення цих потреб великою мірою 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 передусім 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 розробляють інформаційні технології, 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 особи є використання на шкоду її інтересам персональних даних, що нагромаджуються різноманітними структурами, у тому числі органами державної влади, а також розширення можливості прихованого збирання інформації, що становить його особисту й сімейну таємницю, відомості про її приватне життя.

Це зумовлено насамперед труднощами реалізації механізмів охорони цих відомостей, подальшими досягненнями в 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 та 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 в руках невеликої групи власників.

Ці загрози можуть проявлятися у вигляді маніпуляції суспільною думкою щодо тих чи інших суспільно значущих 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.

Передусім 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 поширення 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 такі:

– 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;

Забезпечення інформаційної безпеки України у 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 у сфері внутрішньої політики.

Основними заходами із забезпечення інформаційної безпеки України у 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 у сфері зовнішньої політики.

Основними заходами із забезпечення інформаційної безпеки України у 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 поширеної там дезінформації про зовнішню політику України.

Забезпечення інформаційної безпеки України в галузі науки та техніки.

Найважливішими об'єктами забезпечення інформаційної безпеки України в 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 особи, свободою масового інформування, використання культурної, духовно-моральної спадщини, історичних традицій і норм громадського життя, збереженням культурного надбання всіх народів України, реалізацією конституційних обмежень прав і свобод людини та 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 обробляється 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.

Міністерства й 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 у сфері захисту інформації, відносяться:

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

Крім 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;
– організаційно-методичне керівництво діяльністю по захисту інформації в КС;
– розробку і фінансування науково-технічних програм по захисту інформації;
– затвердження нормативно-технічної документації.

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 й комп'ютерними злочинами. Для цього в структурі МВС створено спеціальне управління для запобігання і розкриття комп'ютерних злочинів.

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

Судова влада здійснює нагляд і притягнення до відповідальності за порушення законодавства в інформаційній сфері. У своїй діяльності суди керуються відповідними статтями КК України, ЦК України.

3.2.4. Особливості забезпечення інформаційної безпеки України в різних сферах суспільного життя

Інформаційна безпека України є однією 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 із них є свої особливості забезпечення інформаційної безпеки, пов'язані зі специфікою об'єктів забезпечення безпеки, ступенем їхньої 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.

– 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.

1.2.5. Етапи розвитку засобів інформаційних комунікацій

Враховуючи вплив на трансформацію ідей інформаційної безпеки, у розвитку засобів інформаційних комунікацій можна виділити декілька етапів:

– I етап – до 1816 року – характеризується використанням природно виникаючих засобів інформаційних комунікацій. У цей період основне завдання інформаційної безпеки полягало в захисті відомостей про події, факти, майно, місцезнаходження й інші дані, що мають для людини особисто або співтовариства, до якого вона належала, життєве значення.

– II етап – починаючи з 1816 року – пов'язаний із початком використання штучно створюваних технічних засобів електро- і радіозв'язку. Для забезпечення скритності й перешкодостійкості радіозв'язку необхідно було використовувати досвід першого періоду інформаційної безпеки на вищому технологічному рівні, а саме застосування перешкодостійкого кодування повідомлення (сигналу) з подальшим декодуванням прийнятого повідомлення (сигналу).

– III етап – починаючи з 1935 року – пов'язаний із появою засобів радіолокації й гідроакустики. Основним способом забезпечення інформаційної безпеки в цей період було поєднання організаційних і технічних заходів, спрямованих на підвищення захищеності засобів радіолокації від дії на їхні приймальні пристрої активними маскуючими і пасивними імітуючими радіоелектронними перешкодами.

– IV етап – починаючи з 1946 року – пов'язаний із винаходом і впровадженням у практичну діяльність електронно-обчислювальних машин (комп'ютерів). Завдання інформаційної безпеки вирішувалися переважно методами і способами обмеження фізичного доступу до устаткування засобів добування, переробки і передачі інформації.

– V етап – починаючи з 1965 року – зумовлений створенням і розвитком локальних інформаційно-комунікаційних мереж. Завдання інформаційної безпеки також вирішувалися, в основному, методами і способами фізичного захисту засобів добування, переробки і передачі інформації, об'єднаних у локальну мережу шляхом адміністрування і управління доступом до мережевих ресурсів.

– VI етап – починаючи з 1973 року – пов'язаний із використанням надмобільних комунікаційних пристроїв із широким спектром завдань. Загрози інформаційній безпеці стали набагато серйознішими. Для забезпечення інформаційної безпеки в комп'ютерних системах із безпровідними мережами передачі даних потрібно було розробити нові критерії безпеки. Утворилися співтовариства людей-хакерів, що ставлять собі за мету нанесення збитку інформаційній безпеці окремих користувачів, організацій і цілих країн. Інформаційний ресурс став найважливішим ресурсом держави, а забезпечення його безпеки – найважливішою й обов'язковою складовою національної безпеки. Формується інформаційне право – нова галузь міжнародної правової системи.

– VII етап – починаючи з 1985 року – пов'язаний зі створенням і розвитком глобальних інформаційно-комунікаційних мереж із використанням космічних засобів забезпечення. Можна припустити що черговий етап розвитку інформаційної безпеки, очевидно, буде пов'язаний із широким використанням надмобільних комунікаційних пристроїв із широким спектром завдань і глобальним охопленням у просторі та часі, забезпечуваним космічними інформаційно-комунікаційними системами. Для вирішення завдань інформаційної безпеки на цьому етапі необхідним є створення макросистеми інформаційної безпеки людства під егідою ведучих міжнародних форумів.

Питання для самоконтролю

1. Яким чином розрізняються групи загроз інформації?
2. Дайте визначення поняттям «загроза», «небезпека».
3. Визначте види загроз за ймовірністю реалізації.
4. Визначте види загроз за джерелами походження.
5. Визначте види загроз за значенням.
6. Визначте види загроз за структурою та об'єктом впливу.
7. Визначте види загроз за характером реалізації.
8. Які основні підходи до визначення дестабілізуючих факторів ви знаєте?
9. Визначте політичні фактори загроз.
10. Визначте економічні фактори загроз.
11. Визначте організаційно-технічні фактори загроз.
12. Назвіть джерела загроз інформаційній безпеці особи.
13. Назвіть джерела загроз інформаційній безпеці суспільству.
14. Назвіть джерела загроз інформаційній безпеці держави.
15. Які існують етапи розвитку засобів інформаційних комунікацій?

застосування інформаційних технологій, інших елементів інформаційної інфраструктури для формування, розвитку й 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 у сфері формування, розвитку, використання інформаційних ресурсів та здійснення правосуддя у сфері суспільних інформаційних відносин.

3.2.3. 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 у сфері захисту інформації й інформаційних ресурсів;

– нормативну правову базу захисту інформації;

– служби (органи) захисту інформації підприємств, організацій, установ.

Органи законодавчої влади (Верховна Рада) видають закони, що регулюють відносини у сфері захисту інформації.

Нормативна база формується на основі нормативних правових актів у сфері захисту інформації, виданих органами різних гілок влади, міністерствами, відомствами.

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.

– 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 й засобами забезпечення інформаційної безпеки в умовах надзвичайної ситуації;

– здійснення системи заходів із відновлення нормального функціонування об'єктів інформаційної безпеки в 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 й реалізація організаційних заходів і нормативно-методичного забезпечення відомчих і регіональних структур у сфері формування та використання інформаційних ресурсів за умови координації діяльності згаданих структур;

– розроблення й 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

1.3. Принципи, форми та методи забезпечення інформаційної безпеки держави

1.3.1. Основні принципи забезпечення інформаційної безпеки держави

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

Забезпечення інформаційної безпеки досягається в процесі свідомої цілеспрямованої діяльності органів державного управління із запобігання 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.

Держава здійснює свої заходи через відповідні органи, а громадяни, суспільні організації й об'єднання, що мають відповідні повноваження, – згідно із законодавством. В основу забезпечення інформаційної безпеки держави повинні бути покладені такі принципи:

- законність, дотримання балансу інтересів особи, 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 щодо заходів інших видів безпеки;

- адекватна інформованість об'єктів безпеки, у тому числі й 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 щодо будь-якого виду діяльності, то можна стверджувати, що цей принцип є загальним, і його дія поширюється на всі сфери безпеки особи, 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 поширення 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 тощо 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 всіх членів співтовариства рівною мірою, 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 в системі колективної безпеки.

1.3.2. Основні форми забезпечення інформаційної безпеки держави

Форми та способи забезпечення інформаційної безпеки утворюють власне інструмент, з допомогою якого сили інформаційної безпеки вирішують увесь комплекс завдань із захисту життєво важливих інтересів особи, 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 діяльності, у тому числі й політичній. 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 й силами та засобами системи інформаційної безпеки. Його основу становить збирання (добування) необхідних відомостей, здійснюване в процесі розвідувальної, оперативно-розшукової й оперативно-інформаційної діяльності.

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, їхніх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері й переслідування журналістів за політичні позиції;

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

– забезпечення інформаційної безпеки всіх складових елементів системи державного управління;

– забезпечення інформаційно-аналітичного потенціалу країни;

– реалізація державної політики інформаційної безпеки;

– ведення активної розвідувальної, контррозвідувальної й 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 та припинення інформаційного тероризму та іншої діяльності, спрямованої на підрив функціонування системи державного управління;

– моніторинг (спостереження, оцінка і прогноз) стану інформаційної безпеки у зв'язку з 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;

– участь у роботі керівних, виконавчих та забезпечуючих підрозділів цих структур (організацій), спільне проведення планових та оперативних заходів.

Безумовно, 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 у контексті розглядуваних проблем вбачається аналіз змісту та призначення системи забезпечення інформаційної безпеки. Забезпечення інформаційної безпеки досягається в процесі свідомої цілеспрямованої діяльності органів державного управління, щодо запобігання 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 становлять 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 цієї системи. Так, наприклад, захищеність Кабінету Міністрів України і незахищеність місцевої адміністрації міста Києва у своїй сукупності не утворять стан захищеності всієї системи інформаційної безпеки органів державного управління. Таким чином, суб'єкти системи забезпечення інформаційної безпеки України мають тісно взаємодіяти між собою, водночас кожний із 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 стрункy організаційно-функціональну систему, об'єднану як системою владно-розпорядчих повноважень, так і функцією по забезпеченню інформаційної безпеки. Таким чином, об'єктами системи забезпечення інформаційної безпеки України є:

– інтереси органів державного управління в інформаційній сфері;

– система органів державного управління, а також їхні компетентні особи й відносини між ними (суспільні відносини в інформаційній сфері);

– власне система забезпечення інформаційної безпеки України.

3.2.2. Мета функціонування та 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 й забезпечення ефективного використання національних інформаційних ресурсів у всіх сферах життя і діяльності громадянина, суспільства й держави. Ефективність системи державного управління

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 й 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 щодо 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 особи 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 переважно із застосуванням технічних засобів захисту, особистої, сімейної і професійної таємниці.

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

1.3.3. Методи забезпечення інформаційної безпеки

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 й забезпечувати захист як від зовнішніх, так і від внутрішніх загроз.

Діяльність із 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 й варіюватися залежно 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 необхідно, по-перше, описати, а лише потім класифікувати різні види загроз та небезпек, ризиків та викликів і відповідно сформулювати систему заходів зі здійснення управління ними. Поширеними методами аналізу стану забезпечення інформаційної безпеки є 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 з їх нейтралізації. У числі таких

методів причинних зв'язків можна назвати такі: 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. Залежно від загрози уможливлюється завдання щодо диференціації як різних рівнів загроз, так і різних рівнів захисту. Що стосується сфери інформаційної безпеки, то в ній, зазвичай, виділяють: фізичний, програмно-технічний, управлінський, технологічний, рівень користувача, мережевий, процедурний. Розглянемо дещо детальніше кожний із цих рівнів. На фізичному рівні здійснюється організація і фізичний захист інформаційних ресурсів, інформаційних технологій, що використовуються, і управлінських технологій. На програмно-технічному рівні здійснюється ідентифікації та перевірка дійсності користувачів, управління доступом, протоколювання й 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 реалізації 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 ця 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 такі 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: однорівневі 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 в єдину систему координуючими функціями на організаційному рівні з метою забезпечення інформаційної безпеки з огляду на аналіз 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 та схеми дій у політичній, економічній і соціальній сферах життєдіяльності; забезпечення адекватного сприйняття загрози та небезпеки в більш низьких організаційних

– формування й діяльність оптимальної структури системи інформаційної безпеки, аналіз функціонування її окремих елементів, організація функціонування цієї системи загалом;

– 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 всіх рівнях державного управління;

– підготовка й 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;

– системне забезпечення діяльності елементів системи: інформаційне, аналітичне, адміністративно-правове, матеріально-технічне, кадрове, ресурсне забезпечення всієї 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 з відпрацюванням відповідних превентивних заходів.

4. Міжнародне співробітництво у 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 вирішення проблем інформаційної безпеки з урахуванням національних інтересів України;

3.2. Система та політика забезпечення інформаційної безпеки України

3.2.1. Основні функції системи забезпечення інформаційної безпеки України

Відсутність системи забезпечення інформаційної безпеки унеможливлює надійне забезпечення не лише інформаційної, а й національної безпеки. Головне призначення цієї системи полягає в досягненні цілей національної безпеки в інформаційній сфері, а отже, основною функцією цієї системи є забезпечення збалансованого існування інтересів особи, суспільства і держави в інформаційній сфері. Система забезпечення інформаційної безпеки України (СЗІБ) створюється й розвивається відповідно до Конституції України та інших нормативно-правових актів, що регулюють суспільні відносини в інформаційній сфері. Основою цієї системи є 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 національну безпеку 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, несформованість нормативно-правової бази щодо регулювання суспільних відносин у сфері національної безпеки, відповідним чином негативно впливає на можливість формування достатньої й ефективно діючої нормативно-правової бази з питань забезпечення національної безпеки в інформаційній сфері.

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 щодо того чи іншого терміна, 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 в концепції, доктрині, програмах, планах та інших документах;

ланках системи державного управління; виділення необхідних політичних, економічних, соціальних, адміністративних і організаційних ресурсів, достатніх для реалізації програми відбиття інформаційної загрози та 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 з його обмеженою можливістю 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 почасти 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 із забезпечення інформаційної безпеки, не проводиться підготовка відповідних фахівців для органів державного управління. Дуже важливим є застосування аналітичних методів пізнання і дослідження стану суспільної свідомості у сфері інформаційної безпеки.

Наприклад, усвідомлення важливості забезпечення інформаційної безпеки на рівні індивіда, суспільства й організації заважає поширений міф про те, що захист інформації і криптографія те ж саме. Водночас таке розуміння є наслідком використання застарілих підходів до інформаційної безпеки, коли інформаційна безпеки лише ототожнюються із захистом інформації шляхом її шифрування. 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 криптокодування 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. Отже, управління у сфері інформаційної безпеки має здійснюватися на підставі принципу доступності та безпеки. Система забезпечення інформаційної безпеки насамперед має гарантувати доступність і цілісність інформації, а її конфіденційність – у випадку необхідності.

Також зазначимо, що вплив хакерів та їхня можливість суттєво вплинути на інформаційні системи дещо перебільшена. Здебільшого були зламані ті системи, які мали поганий захист. Так, наприклад, багато компаній в Україні, які мають солідний грошовий обіг і достатні фінансові джерела, не мають не те щоб цілісної системи безпеки взагалі, а й навіть окремо функціонуючої підсистеми забезпечення інформаційної безпеки. Переважно забезпечення інформаційної безпеки зводиться

до того, що в системних блоках блокується доступ до флоппі-дисків і тим самим унеможливлюється несанкціонований запис інформації. Крім 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 із банків жодного разу не визнав факту вчиненого кіберзлочину проти себе. У цьому 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 в цей час обробляється, а загалом до комп'ютерної мережі всієї системи органів державного управління, починаючи від Кабінету Міністрів України, закінчуючи місцевими органами виконавчої влади. Таким чином, один із найкращих засобів захисту інформації від нападу – не допускати його. Втім не треба плекати надію на створення абсолютної системи інформаційної безпеки, оскільки, як зазначалося вище, ми стоїмо на тій позиції, що загроза та небезпека є атрибутивними компонентами системи інформаційної безпеки, отже, їх існування та реалізація, а також негативні наслідки є природним компонентом системи інформаційної безпеки. Саме вони дають змогу побачити недоліки в системі управління інформаційною безпекою, і водночас слугують імпульсом до вдосконалення, тобто до розвитку.

Треба зауважити, що важливим методом забезпечення інформаційної безпеки є метод розвитку. Захист інформації не обмежується технічними методами, на що зазначає велике коло дослідників. 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 коефіцієнта ймовірності настання та розміру негативних наслідків. Наявність конкретних даних із 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 у світі дає всі 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

– 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 і 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. Безперечно, 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. Від кращого розуміння європейським співтовариством української політики, соціальної сфери, культури тощо залежить місце та роль України на світовій арені.

В умовах, коли Україна обстоює 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 населенням, 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.

Питання для самоконтролю

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 у сфері інформаційної безпеки?
5. В яких сферах проявляються реальні та потенційні загрози безпеці України?
6. Охарактеризуйте загрози інформаційній безпеці України у воєнній сфері.
7. Охарактеризуйте загрози інформаційній безпеці України в економічній сфері.
8. Охарактеризуйте загрози інформаційній безпеці України в екологічній сфері.
9. Які завдання реалізації інформаційної політики з питань євроінтеграції?

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 радіопередачах 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 межах європейських процесів;

постійно провадяться 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 у 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 в 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 такого 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 становити середовище поширення небезпечної інформації. Методи впливу на інформацію у формі повідомлень можна поділити також на електронні та неелектронні. Електронні методи впливу застосовуються в тих випадках, коли повідомлення закріплюються на електромагнітних носіях, що 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.

Питання для самоконтролю

1. Поняття забезпечення інформаційної безпеки держави.
2. Основні принципи забезпечення інформаційної безпеки держави.
3. Що таке превентивність?
4. Як можна тлумачити поняття адекватної інформованості?
5. Що таке інформаційний патронат?
6. Що таке інформаційна кооперація?
7. Дати визначення інформаційного протиборства.
8. Способи забезпечення інформаційної безпеки для конкретної особи.
9. Методи забезпечення інформаційної безпеки.
10. Рівні сфери інформаційної безпеки.
11. Які є методи впливу на інформацію?

1.4. Поняття та зміст інформаційного протиборства

1.4.1. Основні форми інформаційного протиборства

Інформаційне протиборство – суперництво соціальних систем (країн, блоків країн) в інформаційній сфері щодо 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 в 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 їхніх 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 такі 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 їхніми власними цінностями й ідеологічними установками; збільшення ступеня свого впливу та присутності, встановлення контролю над стратегічними інформаційними ресурсами,

У 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, Доктрини 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 проєвропейської 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

– активізація скоординованої інформаційної роботи закордонних дипломатичних установ України;

– сприяння поширенню та розвитку системи іномовлення України;

– створення та забезпечення функціонування правового механізму взаємодії державних органів з інститутами громадянського суспільства з метою інформаційної підтримки комерційної, гуманітарної, просвітницької, культурної та іншої діяльності таких інститутів за межами України;

– постійний моніторинг пропаганди держави-агресора, розроблення та оперативна реалізація адекватних заходів протидії;

– недопущення використання міжнародного інформаційного простору в деструктивних цілях або для дій, що спрямовані на дискредитацію України на міжнародному рівні;

– реформування системи взаємовідносин з українською діаспорою шляхом забезпечення більш тісної співпраці та проведення ефективних заходів, зокрема в рамках комунікацій «від людини до людини»;

– участь у міжнародних культурних заходах з метою представлення національної культури та ідентичності;

– запровадження міжнародних культурних фестивалів в Україні з метою популяризації української культури та розвитку комунікацій «від людини до людини».

Для формування збалансованої державної політики та ефективного проведення комплексу узгоджених заходів щодо захисту національних інтересів в інформаційній сфері створення розвиненого й 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.

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 в 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.

інформаційно-телекомунікаційною структурою і національними ЗМІ; нарощування присутності власних ЗМІ в інформаційній сфері об’єкта проникнення і т. ін.

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 (зазвичай 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 становлять для його нормального (мирного) розвитку найбільшу небезпеку. Нині відсутні міжнародні та національні правові норми, які дозволяють у 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 перебувають фізичні інформаційні системи і засоби, але й 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 й 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 в інформаційній війні, суттєво розширюють коло можливих її учасників. Ними можуть бути окремі країни та їхні органи розвідки, злочинні, терористичні й 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 й 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 й масове поширення інформаційними каналами противника або глобальними мережами інформаційної взаємодії дезінформації або тенденційної інформації для впливу на оцінки, наміри й орієнтацію населення та осіб, що приймають рішення (психологічна війна);

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

Органи інформаційної війни – це органи керування інформаційною війною та люди (фахівці, офіцери, підрозділи) для її ведення.

– стимулювання розвитку національного виробництва текстового і аудіовізуального контенту, зокрема шляхом створення системи квотування та проведення цільових конкурсів на надання грантів;

– забезпечення функціонування Суспільного телебачення і радіомовлення України, у тому числі його належного фінансування;

– створення системи мовлення територіальних громад, яка сприятиме розширенню комунікативних можливостей та зниженню конфліктності всередині громад;

– підтримка вітчизняної книговидавничої справи, зокрема перекладів іноземних творів, забезпечення ними навчальних закладів і бібліотек;

– розвиток правових інструментів захисту прав людини і громадянина на вільний доступ до інформації, її поширення, оброблення, зберігання та захист;

– комплексна підтримка розвитку механізмів саморегуляції засобів масової інформації на засадах соціальної відповідальності;

– підвищення медіа-грамотності суспільства, сприяння підготовці професійних кадрів для медіа-сфери з високим рівнем компетентності;

– удосконалення законодавчого регулювання інформаційної сфери відповідно до актуальних загроз національній безпеці;

– задоволення потреб населення тимчасово окупованих територій в об'єктивній, оперативній і достовірній інформації;

– повне покриття території України цифровим та інтернет-мовленням замість аналогового і надання рівних можливостей доступу кожному громадянину до інформаційних ресурсів мережі Інтернет;

– формування системи державної підтримки виробництва вітчизняного аудіовізуального продукту;

– пропагування, у тому числі через аудіовізуальні засоби, зокрема соціальну рекламу, основних етапів і досвіду державотворення, цінностей свободи, демократії, патріотизму, національної єдності, захисту України від зовнішніх і внутрішніх загроз;

3) щодо відкритості та прозорості держави перед громадянами:

– розвиток механізмів електронного урядування;

– сприяння розвитку можливостей доступу та використання публічної інформації у формі відкритих даних;

– інформування громадян України про діяльність органів державної влади, налагодження ефективної співпраці зазначених органів із засобами масової інформації та журналістами;

– проведення реформи урядових комунікацій;

– розвиток сервісів, спрямованих на більш масштабне та ефективне залучення громадськості до прийняття рішень органами державної влади та органами місцевого самоврядування;

– сприяння формуванню культури суспільної дискусії;

4) щодо формування позитивного міжнародного іміджу України:

– грунтовне реформування системи представлення інформації про Україну на міжнародній арені;

– розвиток публічної дипломатії, у тому числі культурної та цифрової;

інших підприємств, установ, організацій, закладів культури та засобів масової інформації, а також використання місцевих радіостанцій, телевізійних центрів та друкарень для військових потреб і проведення роз'яснювальної роботи серед військ та населення; заборони роботи приймально-передавальних радіостанцій особистого та колективного користування і передачі інформації через комп'ютерні мережі в умовах запровадження правового режиму воєнного стану;

– оптимізація законодавчих механізмів реалізації зобов'язань України в межах Європейської конвенції про транскордонне телебачення щодо держав, які не є підписантами зазначеної Конвенції;

– створення і розвиток структур, що відповідають за інформаційно-психологічну безпеку, насамперед у Збройних Силах України, з урахуванням практики держав – членів НАТО;

– розвиток і захист технологічної інфраструктури забезпечення інформаційної безпеки України;

– забезпечення повного покриття території України цифровим мовленням, насамперед у прикордонних районах, а також тимчасово окупованих територій;

– розвиток цифрового мовлення, унеможливлення впливу на його інфраструктуру суб'єктів, що пов'язані з державою-агресором;

– побудова дієвої та ефективної системи стратегічних комунікацій;

– розвиток механізмів взаємодії держави та інститутів громадянського суспільства щодо протидії інформаційній агресії проти України;

– боротьба з дезінформацією та деструктивною пропагандою з боку Російської Федерації;

– посилення спроможностей сектору безпеки і оборони щодо протидії спеціальним інформаційним операціям, спрямованим на зміну конституційного ладу насильницьким шляхом, порушення суверенітету і територіальної цілісності, підрив обороноздатності України, деморалізацію особового складу Збройних Сил України та інших військових формувань, загострення суспільно-політичної ситуації;

– виявлення та притягнення до відповідальності згідно із законодавством суб'єктів українського інформаційного простору, що створені та використовуються державою-агресором для ведення інформаційної війни проти України, та унеможливлення їхньої підривної діяльності;

– унеможливлення вільного обігу інформаційної продукції (друкованої та електронної), насамперед походженням з території держави-агресора, що містить пропаганду війни, національної і релігійної ворожнечі, зміни конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України, провокує масові заворушення;

– проведення розвідувальними органами України акцій сприяння реалізації та захисту національних інтересів України в інформаційній сфері, протидії зовнішнім загрозам інформаційній безпеці держави за межами України;

– недопущення використання інформаційного простору держави в деструктивних цілях або для дій, що спрямовані на дискредитацію України на міжнародному рівні;

2) щодо забезпечення захисту і розвитку інформаційного простору України, а також конституційного права громадян на інформацію:

До органів інформаційної війни можуть належати:

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

– органи стратегічного рівня з відслідковування ознак початку інформаційної війни, які збирають і аналізують розвідувальну інформацію, визнають ознаки 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, 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.

1.4.2. 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 цього 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 із силами бойового управління противника. Метою даної боротьби є «обезголовлення» противника, позбавлення його надійної системи управління, захоплення ініціативи та примус противника реагувати на ситуацію, 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 таких функцій:

– підготовка й 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. У такій операції головні зусилля сил і засобів спрямовуються на забезпечення

– гарантування свободи інформаційної діяльності та права доступу до інформації в 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 та 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 з 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.

Пріоритетами державної політики в інформаційній сфері мають бути:

1) щодо забезпечення інформаційної безпеки:

– створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них;

– удосконалення повноважень державних регуляторних органів, які здійснюють діяльність щодо інформаційного простору держави, з метою досягнення адекватного рівня спроможності держави відповідати реальним та потенційним загрозам національним інтересам України в інформаційній сфері;

– законодавче врегулювання механізму виявлення, фіксації, блокування та видалення з інформаційного простору держави, зокрема з українського сегмента мережі Інтернет, інформації, яка загрожує життю, здоров'ю громадян України, пропагує війну, національну та релігійну ворожнечу, зміну конституційного ладу насильницьким шляхом або порушення територіальної цілісності України, загрожує державному суверенітету, пропагує комуністичний та/або націонал-соціалістичний (нацистський) тоталітарні режими та їхню символіку;

– визначення механізмів регулювання роботи підприємств телекомунікацій, поліграфічних підприємств, видавництв, телерадіоорганізацій, телерадіоцентрів та

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 і 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 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, у тому числі технічного захисту інформації в національних інформаційних ресурсах від кібернетичних атак.

3.1.3. Стан та перспективи розвитку інформаційної безпеки України

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;

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.

Інформаційні операції повинні проводитися в умовах комплексного, погодженого в 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.

За контекстом **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;

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

– протидії всім видам розвідки противника.

Крім 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 спектра, а також на забезпечення ефективного використання електромагнітного спектра своїми військами.

Інтерпретація терміна «радіоелектронна війна» набагато ширше аналогічного терміна «радіоелектронна боротьба», оскільки вона включає в себе, крім 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 загалом 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 всіх 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 й 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 та 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.).

– 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 вплив 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, у 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 неліцензованого 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 їхніх 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, книгорозповсюдження й бібліотечної справи від рівня розвинутих держав;

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 в 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, яких 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.

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;

1.4.3. 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 зазначити, 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 передусім 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 такими 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 вразливі 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 й 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;

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 немає 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 животіння (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 неконкурентоспроможність 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 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.

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. Розміщена на них інформація поширюється дуже швидко й 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.

3.1.2. 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 неконкурентоспроможність 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.

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.

– 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 таких 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 у результаті роботи прикладних програм, або масивів даних, що уже містяться 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 такі 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) здебільшого мовою програмування Асемблер і при виконанні не створюють ніяких аудіовізуальних відображень у комп'ютерній системі.

Особливістю комп'ютерних вірусів є їхня неспрямованість 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 в програми, передаватися лініями зв'язку, мережами обміну інформацією, виводити з ладу системи керування і т. ін.

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

– руйнування або зміна кодів програм в оперативній пам'яті;

– нейтралізація роботи тестових програм і систем захисту інформаційних ресурсів.

До засобів несанкціонованого доступу відноситься будь-яке 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 й реалізації несанкціонованого доступу до інформаційних ресурсів мереж обміну інформацією.

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

й управління, прийняті в межах їх компетенції в цій сфері; міжнародні договори й угоди визнані Україною.

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

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

Громадяни, суспільні й інші організації та об'єднання є суб'єктами безпеки, володіють правами й обов'язками з 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 із забезпечення безпеки;

– інтеграція з міжнародними системами безпеки.

Систему національної безпеки утворюють:

– органи законодавчої, виконавчої і судової влади;

– державні, суспільні й інші організації та об'єднання;

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

– законодавство, що регламентує відносини у сфері безпеки;

– сили забезпечення безпеки.

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

Сили забезпечення безпеки включають: правоохоронні та розвідувальні органи, державні органи спеціального призначення з правоохоронними функціями, сили цивільного захисту та інші органи, на які Конституцією та законами України покладено функції із забезпечення національної безпеки України.

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

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

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

РОЗДІЛ 3. ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ

3.1. Забезпечення інформаційної безпеки України

3.1.1. Інформаційна безпека і її місце в системі національної безпеки України

Необхідною умовою нормального існування й 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.

Законом України «Про національну безпеку України» визначаються та розмежовуються повноваження державних органів у сферах національної безпеки й оборони, створюється основа для інтеграції політики та процедур органів державної влади, інших державних органів, функції яких стосуються національної безпеки й оборони, сил безпеки і сил оборони, визначається система командування, контролю та координації операцій сил безпеки і сил оборони, запроваджується всеосяжний підхід до планування у сферах національної безпеки й оборони, забезпечуючи в такий спосіб демократичний цивільний контроль над органами та формуваннями сектору безпеки й оборони.

Згідно з цим Законом під **національною безпекою України** слід розуміти захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз.

Національні інтереси України – життєво важливі інтереси людини, суспільства й держави, реалізація яких забезпечує державний суверенітет України, її прогресивний демократичний розвиток, а також безпечні умови життєдіяльності й добробут її громадян.

Воєнна безпека – захищеність державного суверенітету, територіальної цілісності і демократичного конституційного ладу та інших життєво важливих національних інтересів від воєнних загроз.

Громадська безпека і порядок – захищеність життєво важливих для суспільства та особи інтересів, прав і свобод людини та громадянина, забезпечення яких є пріоритетним завданням діяльності сил безпеки, інших державних органів, органів місцевого самоврядування, їх посадових осіб та громадськості, які здійснюють узгоджені заходи щодо реалізації й захисту національних інтересів.

Державна безпека – захищеність державного суверенітету, територіальної цілісності і демократичного конституційного ладу та інших життєво важливих національних інтересів від реальних і потенційних загроз невоєнного характеру.

Загрози національній безпеці України – явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України.

Законодавчою основою забезпечення національної безпеки є Конституція України, закони України, укази Президента України, ухвали й розпорядження Кабінету Міністрів України, інші нормативно-правові акти державних органів влади

Програмні закладки

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.

До **Троянських програм** відносяться програмні закладки, які мають законний доступ до системи, проте виконують також і приховані (неоголошені) функції. Так, програма «Троянський кінь» у доповнення до основних (проектних і документованих) надає додаткові, але не описані в документації функціональні можливості, спрямовані на те, щоб обійти контроль доступу і призвести до несанкціонованого знищення, блокування, модифікації або копіювання інформації, порушення роботи ЕОМ, системи ЕОМ або їхньої мережі.

Ці можливості можуть самоліквідуватись, що робить неможливим їхнє виявлення, або ж можуть реалізовуватися постійно, але існувати потай. Найбільш небезпечним є опосередкований вплив, за якого «Троянський кінь» діє в межах повноважень одного користувача, але в інтересах іншого користувача, встановити особу якого інколи неможливо.

Різновидами «Троянського коня» є «Троянська матрьошка» та «Троянський черв'як».

«Троянська матрьошка» має ту особливість, що у фрагмент програми вставляються не команди, які самі виконують несанкціоновані операції, а команди, що формують ці команди й після виконання своєї функції, тобто коли вже автоматично на програмному рівні створений «Троянський кінь», самоліквідуються.

«Троянський черв'як» має ту особливість, що в нього закладений алгоритм саморозмноження, програмне автоматичне відтворення «Троянського коня». Програми-черв'яки автоматично копіюють себе в пам'яті одного або декількох комп'ютерів (за наявності комп'ютерної мережі) незалежно від інших програм. При цьому використовується тактика комп'ютерних вірусів (вірусів-черв'яків), які поширюються в комп'ютерній мережі й не заражають «батьківські» програми, файли або сектори на дисках.

«Черв'яки» проникають у пам'ять комп'ютера з комп'ютерної мережі й після визначення адрес інших комп'ютерів розсилають за цими адресами свої копії. Вони іноді створюють робочі файли на дисках операційної системи, проте можуть і взагалі не звертатися до ресурсів обчислювальної системи (за винятком оперативної пам'яті).

Впровадження **Троянських програм** в автоматизовані системи керування противника здійснюється такими способами:

– використанням віддалених атак;
– впровадженням програмних закладок в операційні системи та програмне забезпечення, що поставляються на експорт;
– агентурним шляхом.

Логічна бомба – це така програмна закладка, що здійснює зловмисні дії при виконанні ряду певних логічних умов. Вноситься таємно в програмне забезпечення ЕОМ і виконується внаслідок збігу певних обставин або у визначений момент (часова бомба) з метою спотворення, знищення, модифікування або викрадення даних.

Логічний люк – механізм усередині операційної системи (програмного забезпечення), який дозволяє програмі зловмисника отримати привілейовану функцію або режим роботи (які йому не були дозволені). Логічними люками можуть бути різноманітні помилки, що свідомо вводяться зловмисником у програмне забезпечення об'єкта.

Програмна пастка («пастка» – хитрий маневр, прийом для заманювання противника в невигідне, небезпечне становище) являє собою програмну закладку, яка використовує помилки або неточність у програмному забезпеченні.

Програмний черв'як – це програмна закладка, яка маскується під системні засоби пошуку вільних обчислювальних ресурсів у мережі.

Як засоби інформаційної зброї, програмні закладки мають достатньо специфічну форму реалізації процедури нападу, виконання функцій і дослідження систем захисту (наприклад, паролів доступу) елементів обчислювального середовища.

Інформаційна апаратна зброя включає апаратні засоби, призначені для виконання функцій інформаційної зброї. Прикладом інформаційної апаратної зброї можуть бути апаратні закладки, які впроваджуються в ПК, що готуються на експорт, та їхнє периферійне обладнання. Апаратні закладки маскуються під звичайні пристрої мікроелектроніки й застосовуються для збирання, обробки та передавання конфіденційної інформації.

Інформаційна зброя, що відноситься до різних класів, може застосовуватися спільно, а також деякі види інформаційної зброї можуть мати риси декількох класів.

Засоби ураження людей та їхньої психіки.

Засоби ураження (впливу) на людей та їхню психіку розрізняють залежно від мети їхнього застосування в психологічній війні. До таких цілей зазвичай відносять:

– створення інформації, яку одержує політичне керівництво, командування та особовий склад збройних сил противника, та нав'язування їм фальшивої або беззмістовної інформації;
– психологічна обробка військ та населення;
– ідеологічні диверсії та дезінформування;
– організація масових демонстрацій під фальшивими лозунгами;
– пропаганда та розповсюдження фальшивих чуток;
– змінювання та керування індивідуальною та колективною поведінкою.

Поряд із використанням традиційних засобів (друковані та електронні засоби масової інформації) йде активна розробка та апробація спеціальних засобів впливу на людину як через ЗМІ, так і через комп'ютерні мережі: засоби інформаційно-психологічного впливу, психогенного впливу, психоаналітичного впливу, нейролінгвістичного впливу, психотронного впливу та психотропного впливу.

Ці заходи управління застосовуються для більшості організацій і в більшості середовищ. Слід зазначити, що, хоча всі заходи управління у стандартах та нормативних документах є важливими, доречність (застосовність) якого-небудь засобу управління повинна визначатися у світлі певних ризиків, з якими стикається безпосередньо зазначена організація. Отже, незважаючи на те, що вищезгаданий підхід розглядається, як відправна точка інформаційної безпеки, він не є догмою та не заміняє вибір заходів управління, заснованих на оцінці ризику.

Критичними факторами для успішної реалізації інформаційної безпеки в межах організації є:

– політика безпеки, цілі й дії, які відповідають меті бізнесу;
– підтримка й зобов'язання з боку керівництва;
– правильне розуміння вимог безпеки, оцінки ризику й управління ризиком;
– ефективний маркетинг безпеки для всіх адміністраторів і службовців;
– розподіл повноважень керівництва політикою інформаційної безпеки та стандартами між усіма службовцями й підрядниками;
– забезпечення відповідного тренування й навчання;
– всебічна й збалансована система виміру, що використовується для оцінки ефективності управління інформаційною безпекою й пропозиції в межах зворотного зв'язку, спрямовані на поліпшення бізнесу;
– оцінка загроз інформації, руйнівного впливу на інформацію й уразливості інформації й засобів обробки, а також ймовірності їхнього виникнення.

Питання для самоконтролю

1. Що розуміється під «політикою інформаційної безпеки»?
2. Що являє собою система забезпечення інформаційної безпеки організації?
3. Які є основні принципи політики безпеки організації?
4. Що передбачає аналіз ризиків інформаційної сфери?
5. Наведіть основні правила інформаційної безпеки організації.
6. Які є варіанти побудови системи забезпечення інформаційної безпеки?
7. Наведіть комплекс заходів із забезпечення безпеки інформації.
8. Які повинні бути вироблені підходи забезпечення безпеки інформації на правовому рівні?
9. Які повинні бути вироблені підходи забезпечення безпеки інформації на організаційному рівні?
10. Які повинні бути вироблені підходи забезпечення безпеки інформації на технічному рівні?
11. Які є правила розмежування доступу користувачів?
12. Що містити в собі документальне оформлення політики безпеки?

– організаційний, у якому наводиться перелік підрозділів, робочих груп, посадових осіб, які відповідають за роботи у сфері захисту інформації, їхніх функції, викладаються підходи, що застосовуються до персоналу (опис посад з точки зору безпеки інформації, організація навчання та перепідготовки персоналу, порядок реагування на порушення режиму безпеки та ін.);

– класифікаційний, де визначаються матеріальні та інформаційні ресурси, які є в наявності в організації, та необхідний рівень їхнього захисту;

– розділ, у якому визначається підхід щодо керування об'єктами та обладнанням організації;

– розділ, у якому висвітлюються питання фізичного захисту;

– розділ, у якому висвітлюються питання захисту інформації від витоку технічними каналами;

– розділ, де викладено порядок розробки та супроводження системи, модернізації апаратного та програмного забезпечення;

– розділ, який регламентує порядок проведення відновлювальних робіт і забезпечення неперервного функціонування організації загалом та окремих складових та об'єктів організації;

– юридичний розділ, у якому приводиться підтвердження відповідності політики безпеки законодавству України.

2.5.3. Заходи управління інформаційною безпекою

Після ідентифікації вимог безпеки варто вибирати й застосовувати заходи управління таким чином, щоб забезпечувати впевненість у зменшенні ризиків. Засоби управління можуть бути обрані зі стандартів або з іншої безлічі документів та заходів управління визначених для даного класу систем, або можуть бути розроблені, щоб задовольнити потреби компанії відповідно до обраної політики безпеки.

Заходи управління варто вибирати, ґрунтуючись на відношенні вартості реалізації послуг та впровадження систем безпеки й зниження ризиків і можливих втрат, якщо відбудеться порушення. Не грошові фактори, наприклад, втрата репутації, соціальні тощо, варто також брати до уваги з метою підтримки конкурентоспроможності компанії.

Деякі із заходів управління в стандартах та нормативних документах, можуть розглядатися, як керівні принципи для управління інформаційною безпекою й застосовуються більшістю організацій.

Заходи управління (розглянуті із законодавчого погляду) включають:

– захист даних і секретність особистої інформації;

– охорону інформаційних ресурсів організації;

– права на інтелектуальну власність.

Заходи управління (розглянуті як загальна стала практика для інформаційної безпеки) містять:

– документи, що стосуються політики інформаційної безпеки;

– розподіл обов'язків, пов'язаних з інформаційною безпекою;

– структуру підрозділів й навчання, що пов'язані з інформаційною безпекою;

– управління безперервністю бізнесу.

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** – нині ще немає систем попередження, які дозволили б їй відрізнити стратегічну атаку з використанням інформаційної зброї від інших форм діяльності в інформаційному просторі, включаючи шпигунство й випадкові помилки;

– **труднощі при створенні й підтримці коаліцій** – коаліції тільки збільшують уразливість їхніх учасників від інформаційної поразки;

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

Питання для самоконтролю

1. Дайте визначення поняття «інформаційне протиборство».
2. Назвіть рівні проведення інформаційного протиборства.
3. Назвіть основні ступені інформаційного протиборства.
4. Що відноситься до органів інформаційної війни?
5. Назвіть основні форми інформаційної війни.
6. Що являє собою оперативна безпека?
7. Яким чином відрізняється інформаційна зброя від звичайних засобів ураження?
8. Назвіть сферу застосування інформаційної зброї.
9. Назвіть основні об'єкти застосування інформаційної зброї.
10. Що таке комп'ютерні віруси?
11. Які існують види програмних закладок?
12. Які існують особливості застосування інформаційної зброї?

1.5. Основи теорії інформаційної боротьби

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

Мета й завдання інформаційної боротьби визначають її зміст, а також і структуру теорії інформаційної боротьби. При цьому на зміст інформаційної боротьби великий вплив справляє багато 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 й 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.

Наприклад, загальні ПРД можуть бути такими (за припущення, що в організації визначено такі ієрархічні ролі: адміністратор безпеки організації, адміністратор, користувач):

– кожне робоче місце повинно мати свого адміністратора, який несе відповідальність за його працездатність та за дотримання всіх вимог і процедур, пов'язаних з обробкою інформації та її захистом. Таку роль може виконувати уповноважений користувач. Цей користувач повинен бути забезпечений відповідними інструкціями й навчений всім вимогам і процедурам;

– попередження неавторизованого доступу до даних, програмного забезпечення, інших ресурсів організації, керування механізмами захисту здійснюється адміністратором безпеки організації (об'єкта організації);

– для попередження поширення комп'ютерних вірусів відповідальність за дотримання правил використання програмного забезпечення несуть: адміністратор безпеки організації, на об'єкті організації – адміністратор безпеки об'єкта організації. Повинно використовуватися тільки програмне забезпечення, яке дозволено політикою безпеки (ліцензійне, яке має відповідні сертифікати, експертні висновки тощо);

– за всі зміни програмного забезпечення, створення резервних і архівних копій несе відповідальність адміністратор безпеки організації (об'єкта організації). Такі роботи виконуються за його дозволом;

– кожний користувач має свій унікальний ідентифікатор і пароль. Право видачі цих атрибутів надається адміністратору. Атрибути для адміністраторів надає адміністратор безпеки організації. Видача атрибутів дозволяється тільки після документальної реєстрації особи як користувача. Користувачам забороняється спільне використання персональних атрибутів;

– користувачі проходять процедуру аутентифікації для отримання доступу до ресурсів організації;

– атрибути користувачів періодично змінюються, а невикористовувані та скомпрометовані – видаляються;

– процедури використання активного мережного обладнання, а також окремих видів програмного забезпечення, яке може суттєво впливати на безпеку (аналізатори трафіку, аналізатори безпеки мереж, засоби адміністрування і т. ін.), авторизовані і здійснюються під контролем адміністратора безпеки інформаційної системи;

– усі користувачі повинні знати «Інструкцію користувача» (пройти відповідний курс навчання, скласти іспит);

– адміністратор безпеки організації й адміністратори мереж повсякденно здійснюють перевірку працездатності засобів захисту інформації, ведуть облік критичних з погляду безпеки подій і готують звіти щодо цього.

Загальні ПРД мають бути конкретизовані на рівні вибору необхідних функціональних послуг захисту (профілю захищеності) та впровадження організаційних заходів захисту інформації.

Документальне оформлення політики безпеки має містити в собі такі розділи:

– загальний, у якому визначається ставлення керівництва організації до проблеми інформаційної безпеки організації;

(надзвичайних ситуацій) з метою забезпечення неперервного функціонування організації в захищеному режимі. Під час планування цих робіт рекомендується враховувати такі питання:

– виявлення критичних з погляду безпеки процесів у роботі організації;

– визначення можливого негативного впливу надзвичайних ситуацій на роботу організації;

– визначення й узгодження обов'язків персоналу і користувачів, а також порядку їхніх дій у надзвичайних ситуаціях;

– підготовка персоналу і користувачів до роботи в надзвичайних ситуаціях.

План проведення відновлювальних робіт і забезпечення неперервного функціонування організації повинен описувати дії щодо улагодження інциденту, дії щодо резервування, дії щодо відновлення. Він включає в себе:

– опис типових надзвичайних ситуацій, які потенційно найбільш можливі в організації внаслідок наявності вразливих місць, або які реально мали місце під час роботи;

– опис процедур реагування на надзвичайні ситуації, які слід вжити одразу після виникнення інциденту, що може призвести до порушення політики безпеки;

– опис процедур тимчасового переводу організації або окремих її компонентів на аварійний режим роботи;

– опис процедур поновлення нормальної виробничої діяльності організації або окремих її компонентів;

– порядок тестування плану, тобто проведення тренувань персоналу в умовах імітації надзвичайних ситуацій.

План проведення відновлювальних робіт і забезпечення неперервного функціонування організації підлягає перегляду в разі виникнення істотних змін у організації. Такими змінами можуть бути:

– встановлення нового обладнання або модернізація наявного, включення до складу організації нових компонентів;

– встановлення нових систем життєзабезпечення на об'єктах організації (сигналізації, вентиляції, пожежогасіння, кондиціонування тощо);

– проведення будівельно-ремонтних робіт;

– організаційні зміни у структурі організації, виробничих процесах, процедурах обслуговування організації;

– зміни у технології зберігання, обробки та передавання інформації;

– зміни у програмному забезпеченні;

– будь-які зміни у складі і функціях СЗІБ.

Правила розмежування доступу користувачів та процесів до ресурсів інформаційної сфери організації.

Найважливішу частину політики безпеки, яка регламентує доступ користувачів і процесів до ресурсів інформаційної сфери організації, складають *правила розмежування доступу (ПРД).*

ПРД – це певний абстрактний механізм, який виступає посередником при будь-яких взаємодіях об'єктів організації і є найбільш суттєвим елементом політики безпеки.

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 цій 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. Цей 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 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 й 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 й теорію сил і засобів ураження інформації. Загальні положення визначають предмет, завдання і зміст теорії ураження інформації, форми та 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 й 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 та принципи інформаційної боротьби.

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

Розрізняють загальні й 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 й розвитку тих чи інших явищ інформаційної боротьби. Закони інформаційної боротьби являють собою більш менш точне відображення у свідомості людей тих об'єктивних зв'язків і відносин, які існують і діють в інформаційному просторі. Якщо вони пізнані, відображені, описані, то стають основою для практичної діяльності з підготовки і ведення інформаційної боротьби.

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

– загальні закони діалектики;

– загальні та 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.

У 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 така закономірність: кількість і якість засобів інформаційної боротьби, а також особового складу зумовлюють 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 меншою мірою залежить від рівня професійної та морально-психологічної підготовки особового складу. Чим вона вища, тим більше можливостей для активних та

– забезпечення фізичного захисту об'єктів організації та носіїв інформації;

– проведення обстеження середовищ функціонування організації;

– порядку виконання робіт із захисту інформації, взаємодії з цих питань з іншими суб'єктами системи захисту інформації в державі;

– виконання робіт з модернізації організації (окремих компонентів);

– регламентації доступу сторонніх користувачів до інформаційної сфери організації;

– регламентації доступу власних користувачів і персоналу до інформаційної сфери організації;

– здійснення профілактичних заходів (наприклад, попередження ненавмисних дій, що призводять до порушення політики безпеки, попередження появи вірусів;

– реалізації окремих положень політики безпеки, найбільш критичних з точки зору забезпечення захисту аспектів (наприклад, реалізація віддаленого доступу до організації (об'єктів організації), використання мереж передачі даних загального користування, зокрема Internet, використання несертифікованого програмного забезпечення і т. ін.).

На технічному рівні забезпечення безпеки інформації повинні бути вироблені підходи щодо застосування технічних і програмно-технічних засобів, які реалізують задані вимоги із захисту інформації. Під час розгляду різних варіантів реалізації рекомендовано враховувати такі аспекти:

– інженерно-технічне обладнання виділених приміщень, в яких розміщуються компоненти організації, експлуатація і супроводження засобів блокування технічних каналів витоку інформації;

– реєстрація санкціонованих користувачів організації, авторизація користувачів у системі;

– керування доступом до інформації і механізмів, що реалізують послуги безпеки, включаючи вимоги до розподілу ролей користувачів і адміністраторів;

– виявлення і реєстрація небезпечних подій з метою здійснення повсякденного контролю або проведення службових розслідувань;

– перевірка й забезпечення цілісності критичних даних на всіх стадіях їхньої обробки в організації;

– забезпечення конфіденційності інформації, у тому числі використання криптографічних засобів;

– резервне копіювання критичних даних, супроводження архівів даних і програмного забезпечення;

– відновлення роботи об'єктів організації після збоїв, відмов, особливо для об'єктів із підвищеними вимогами до доступності інформації;

– захист програмного забезпечення, що використовується в організації (на об'єктах організації), від внесення несанкціонованих доповнень і змін;

– забезпечення функціонування засобів контролю, у тому числі засобів виявлення технічних каналів витоку інформації.

Організація проведення відновлювальних робіт і забезпечення неперервного функціонування об'єктів організації та організації загалом.

Повинні бути вироблені підходи щодо планування й порядку виконання відновлювальних робіт після збоїв, аварій, інших непередбачених ситуацій

перевищує гранично допустимий, то вносяться відповідні зміни до складу заходів і засобів захисту, після чого всі процедури виконуються повторно до одержання прийнятного результату.

Визначення вимог до заходів, методів та засобів безпеки організації.

Вихідними даними є:

– завдання і функції організації;

– результати аналізу середовищ функціонування організації;

– модель загроз, модель порушників;

– результати аналізу ризиків.

На підставі цих даних визначаються компоненти організації, для яких необхідно або доцільно розробити свої власні політики безпеки, відмінні від загальної політики безпеки у організації.

Для кожного компонента та (або) організації загалом формується перелік необхідних функціональних послуг захисту від несанкціонованого доступу та вимог до рівнів реалізації кожної з них, визначається рівень гарантій реалізації. Визначені вимоги складають профіль захищеності інформації в організації (складових організації).

Для кожного компонента та (або) організації взагалі визначаються загальні підходи та вимоги з захисту інформації від витоку технічними каналами.

На наступному кроці визначаються механізми безпеки, що реалізують функціональні послуги безпеки, здійснюється вибір технічних засобів захисту інформації від витоку технічними каналами.

Вибір основних рішень із забезпечення безпеки інформації.

Комплекс заходів із забезпечення безпеки інформації розглядається на трьох рівнях:

– правовому;

– організаційному;

– технічному.

На правовому рівні забезпечення безпеки інформації повинні бути вироблені підходи щодо:

– системи нормативно-правового забезпечення робіт з захисту інформації у організації;

– підтримки керівництвом організації заходів із забезпечення безпеки інформації в організації, виконання правових та (або) договірних вимог із захисту інформації, визначення відповідальності посадових осіб, організаційної структури, комплектування й розподілу обов'язків співробітників СЗІБ;

– процедур доведення до персоналу та користувачів організації основних положень політики безпеки інформації, їхнього навчання і підвищення кваліфікації з питань безпеки інформації;

– системи контролю за своєчасністю, ефективністю й повнотою реалізації в організації рішень із захисту інформації, дотриманням персоналом і користувачами положень політики безпеки.

На організаційному рівні забезпечення безпеки інформації повинні бути вироблені підходи щодо:

– застосування режимних заходів на об'єктах організації;

рішучих дій приймається для захисту 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.

У галузі інформаційної боротьби можна визначити такі закономірності:

– обумовленість масштабів та спрямованості характером створення воєнно-політичної та економічної ситуації, а також цілями воєнної політики держави, суспільних та економічних структур, які беруть 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.

1.5.3. Принципи інформаційної боротьби

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

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 переважно 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 й до руйнівного впливу на інформаційне середовище противника;

– принцип високої активності й 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 й засобами інформаційної боротьби;

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

– принцип врахування духовного фактора в інтересах виконання поставлених завдань;

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

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

1.5.4. 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 особи, суспільства й держави.

Інформаційна боротьба включає комплекс заходів інформаційного забезпечення, інформаційного захисту й інформаційної протидії, що здійснюються за єдиним задумом і планом з метою захоплення й 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 й обмін нею між органами керування з метою організації і ведення бойових дій. Результативність інформаційного забезпечення залежить від багатьох факторів і умов, які, зрештою, здійснюють вплив на два основних елементи: інформування органу керування і сприйняття одержаної ним інформації.

Інформування – акт передавання органу керування певної поточної інформації. Залежно від змісту інформації, інформування можна класифікувати таким чином:

– правильне інформування;

– правильне дезінформування;

– трансінформування;

– трансдезінформування.

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

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

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

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

кожному конкретному випадку експертним методом або емпіричним шляхом, на підставі досвіду експлуатації подібних систем, шляхом реєстрації певних подій і визначення частоти їхнього повторення тощо. Оцінка може мати числове або смислове значення (наприклад, ймовірність реалізації загрози - незначна, низька, висока, неприпустимо висока).

У будь-якому випадку, існуючий ризик не повинен перевищувати гранично допустимий для кожної загрози. Перевищення свідчить про необхідність впровадження додаткових заходів захисту. Мають бути розроблені рекомендації щодо зниження ймовірності виникнення або реалізації загроз та величини ризиків.

– Оцінювання величини можливих збитків, пов'язаних із реалізацією загроз. Виконується кількісна або якісна оцінка збитків, що можуть бути нанесені організації внаслідок реалізації загроз. Доцільно, щоб ця оцінка складалась з величин очікуваних збитків від втрати інформацією кожної з властивостей (конфіденційності, цілісності або доступності) або від втрати керованості організації внаслідок реалізації загрози. Для одержання оцінки можуть бути використані ті ж методи, що і у процесі аналізу ризиків. Величина можливих збитків визначається розміром фінансових втрат або, у разі неможливості визначення цього, за якісною шкалою (наприклад, величина збитків – відсутня, низька, середня, висока, неприпустимо висока).

2.5.2. Основні правила інформаційної безпеки організації

Вибір варіанта побудови системи забезпечення інформаційної безпеки залежно від конфіденційності інформації, яка зберігається, обробляється та передається в організації, рівня її критичності, величини можливих збитків від реалізації загроз, матеріальних, фінансових та інших ресурсів, які є в розпорядженні організації, а також інших чинників, обґрунтовується пропозиція щодо доцільності застосування варіантів побудови системи забезпечення інформаційної безпеки (СЗІБ).

Можливі такі варіанти:

– досягнення необхідного рівня інформаційної безпеки за мінімальних витрат і допустимого рівня обмежень на технології зберігання, обробки та передавання інформації в організації;

– досягнення необхідного рівня захищеності інформації за допустимих витрат і заданого рівня обмежень на технології зберігання, обробки та передавання інформації в організації;

– досягнення максимального рівня захищеності інформації за необхідних витрат і мінімального рівня обмежень на технології зберігання, обробки та передавання інформації в організації.

Якщо інформація становить державну таємницю, то необхідно застосовувати переважно третій варіант.

Оцінювання витрат на СЗІБ.

Здійснюється первинне (попереднє) оцінювання допустимих витрат на блокування загроз, виходячи з вибраного варіанта побудови СЗІБ і виділених на це коштів. На етапі проектування СЗІБ, після формування пропозицій щодо складу заходів і засобів захисту, здійснюється оцінювання залишкового ризику для кожної пропозиції (наприклад, за критерієм «ефективність/вартість»), вибирається найбільш оптимальна серед них, і первинна оцінка уточнюється. Якщо залишковий ризик

Концепція інформаційної безпеки в організації представляє систему поглядів, основних принципів, розкриває основні напрями забезпечення безпеки інформації. Розроблення концепції здійснюється після розгляду повної структури організації й виконується на підставі аналізу таких чинників:

– правових і (або) договірних засад;

– вимог до забезпечення безпеки інформації згідно з завданнями і функціями організації;

– загроз, впливу яких зазнають ресурси організації, що підлягають захисту;

– за результатами аналізу мають бути сформульовані загальні положення безпеки, які стосуються або впливають на технологію зберігання, обробки та передавання інформації в організації:

- мета та пріоритети, яких необхідно дотримуватись у організації під час забезпечення інформаційної безпеки;

- загальні напрями діяльності, необхідні для досягнення цієї мети;

- аспекти діяльності в галузі безпеки інформації, які повинні вирішуватися на рівні організації загалом;

- відповідальність посадових осіб та інших суб'єктів взаємовідносин, у організації, їхні права й обов'язки щодо реалізації завдань інформаційної безпеки.

Аналіз ризиків передбачає вивчення моделі загроз для інформаційної сфери організації та моделі порушників, можливих наслідків від реалізації потенційних загроз (рівня можливої заподіяної ними шкоди) і формування на його підставі моделі захисту інформації в організації. Під час проведення аналізу ризиків необхідним є виконання таких робіт:

– Визначення компонентів і ресурсів організації, які необхідно враховувати під час аналізу. Повинні бути визначені критичні, з точки зору безпеки, компоненти і ресурси організації, які можуть бути об'єктами атаки або самі є потенційним джерелом порушення безпеки інформації (об'єкти захисту). Для цього використовуються відомості, одержані в результаті обстеження середовищ функціонування організації.

– Ідентифікація загроз з об'єктами захисту. Встановлюється відповідність моделі загроз і об'єктів захисту, тобто складається матриця загрози/компоненти (ресурси) організації. Кожному елементу матриці повинен бути зіставлений опис можливого впливу загрози на відповідний компонент або ресурс організації. У процесі упорядкування матриці може уточнюватися список загроз і об'єктів захисту, внаслідок чого буде коригуватись модель загроз.

– Оцінка ризиків. Повинні бути отримані оцінки гранично припустимого й наявного (реального) ризику здійснення кожної загрози впродовж певного проміжку часу, тобто ймовірності її здійснення впродовж цього інтервалу. Для оцінки ймовірності реалізації загрози рекомендується вводити декілька дискретних ступенів (градацій). Оцінювання слід робити за припущення, що кожна подія має найгірший з погляду власника інформації, що потребує захисту, закон розподілу, а також за умови відсутності заходів захисту інформації.

На практиці для більшості загроз неможливо одержати достатньо об'єктивні дані про ймовірність їхньої реалізації і доводиться обмежуватися якісними оцінками. У цьому випадку значення ймовірності реалізації загрози визначається в

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

Ступінь відповідності уявлень органу керування про ці характеристики їхнім вихідним величинам створює передумови для виникнення різноманітних ситуацій інформаційної боротьби. Ці передумови реалізуються залежно від того, наскільки інформація, що поступає, співвідноситься з образами істинних і неправдивих елементів ситуації, які зберігаються в інформаційному кадастрі.

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

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

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

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

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 ситуацію.

Інформаційна протидія – сукупність заходів інформаційної боротьби, спрямованих на протидію інформаційному забезпеченню протиборчої сторони. Інформаційна протидія включає блокування добування, обробки й обміну інформацією та впровадження дезінформації на всіх етапах інформаційного забезпечення. Завдання інформаційної протидії вирішуються шляхом маскування, контррозвідки, радіоелектронного придушення й 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 поширюється й 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 й розвідки в умовах ведення противником радіоелектронної боротьби, застосування розвідувально-ударних комплексів, самонавідної зброї та усунення взаємного впливу радіоелектронних засобів.

1.5.5. Способи інформаційної боротьби

Способи інформаційної боротьби визначають порядок і прийоми застосування сил і засобів інформаційної боротьби для захоплення й 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 й комбіновані, а також за аналогією зі збройною боротьбою виділити дві основні групи способів: наступальні й 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 й у ході бойових дій шляхом виконання комплексу заходів інформаційної протидії повністю або частково припиняється добування (збирання) інформації про ситуацію й обмін інформацією в системах управління військами і зброєю противника. Для реалізації цього способу застосовується вогневе, радіоелектронне й інформаційне ураження (придушення) елементів систем управління військами (силами) і зброєю противника.

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

Політика безпеки має бути розроблена таким чином, щоб вона не потребувала частої модифікації (потреба частої зміни вказує на надмірну конкретизацію, наприклад, не завжди доцільно вказувати конкретну назву чи версію програмного продукту).

Політика безпеки повинна передбачати використання всіх можливих заходів захисту інформації, зокрема: правові та морально-етичні норми, організаційні (адміністративні), фізичні, технічні (апаратні та програмні) заходи – і визначати правила та порядок застосування в організації кожного з цих видів.

Політика безпеки повинна базуватися на таких *основних принципах*:

– системності;

– комплексності;

– неперервності захисту;

– достатності механізмів і заходів захисту та їхньої адекватності загрозам;

– гнучкості керування системою захисту, простоти і зручності її використання;

– відкритості алгоритмів і механізмів захисту.

Політика безпеки повинна доказово *давати гарантії* того, що:

– в організації (в кожній окремій складовій частині, у кожному функціональному завданні і т. ін.) забезпечується адекватність рівня захисту інформації рівню її критичності;

– реалізація заходів захисту інформації є рентабельною;

– у будь-якому середовищі функціонування організації забезпечується можливість оцінювати та перевіряти захищеність інформації;

– забезпечується персоніфікація положень політики безпеки (стосовно суб'єктів організації), звітність (реєстрація, аудит) для всіх критичних, з погляду безпеки, ресурсів, до яких здійснюється доступ у процесі функціонування інформаційної системи;

– персонал і користувачі забезпечені достатньо повним комплектом документації стосовно порядку забезпечення захисту інформації;

– усі критичні з погляду безпеки інформації, технології (функції) організації мають відповідні плани забезпечення неперервної роботи та її поновлення в разі виникнення непередбачених ситуацій;

– враховані вимоги всіх документів, які регламентують порядок захисту інформації в організації, та забезпечується їхнє суворе дотримання.

Політика безпеки розробляється на підготовчому етапі створення СЗІБ організації.

Методологія розробки політики безпеки організації включає в себе такі роботи:

– розробка концепції безпеки інформації у організації;

– аналіз ризиків;

– визначення вимог до заходів, методів та засобів захисту;

– вибір основних рішень із забезпечення безпеки інформації;

– організація виконання відновлювальних робіт і забезпечення неперервного функціонування організації;

– документальне оформлення політики безпеки.

2.5. Основи управління інформаційною безпекою

2.5.1. Політика інформаційної безпеки організації

Необхідність у політиці безпеки на сьогодні є очевидним фактом для будь-якого, навіть достатньо невеликого підприємства. Політика безпеки загалом – це сукупність програмних, апаратних, організаційних, адміністративних, юридичних, фізичних заходів, методів, засобів, правил і інструкцій, які чітко регламентують усі аспекти діяльності підприємства, включаючи інформаційну систему, та забезпечують їхню безпеку.

Крім свого прямого призначення, політика безпеки має ще один корисний ефект: у результаті аналізу інформаційних потоків, інвентаризації інформаційних ресурсів та ранжирування інформації, яка оброблюється, передається або зберігається, за мірою її цінності керівництво підприємства одержує цілісну картину одного з найбільш складних об'єктів – інформаційної системи, що позитивно впливає на якість керування бізнесом взагалі і, як наслідок, покращує його прибутковість і ефективність.

Політику з інформаційної безпеки організації можна визначити як сукупність вимог та правил з інформаційної безпеки організації для об'єкта інформаційної безпеки, вироблених з метою протидії заданій множині загроз інформаційній безпеці організації з урахуванням цінності інформаційної сфери, що підлягає захисту та вартості системи забезпечення інформаційної безпеки.

Об'єкт інформаційної безпеки організації – це об'єкт (об'єкти) організації, вплив порушника інформаційної безпеки на який (які) може призвести до реалізації загрози інформаційній безпеці організації. Управління об'єктом відповідно до заданої політики інформаційної безпеки організації щодо специфічних дій, що відносяться до інформаційної безпеки організації, здійснюється єдиним керівним органом (адміністратором) системи забезпечення інформаційної безпеки організації.

Система забезпечення інформаційної безпеки організації (СЗІБ) являє собою сукупність правових норм, організаційних та технічних заходів, служб інформаційної безпеки та механізмів захисту, органів управління та виконавців, спрямованих на протидію заданій множині загроз інформаційній безпеці організації з метою звести до мінімуму можливі збитки користувачу або оператору зв'язку організації. Адміністратором (керівним органом) системи забезпечення інформаційної безпеки організації може бути фізична або юридична особа, яка є відповідальною за реалізацію політики забезпечення інформаційної безпеки організації.

Під час розробки політики безпеки повинні бути враховані технологія зберігання, обробки та передавання інформації, моделі порушників і загроз, особливості апаратно-програмних засобів, фізичного середовища та інші чинники. У організації може бути реалізовано декілька різних політик безпеки, які істотно відрізняються.

Як складові частини загальної політики безпеки в організації мають існувати політики забезпечення конфіденційності, цілісності, доступності оброблюваної інформації. Політика безпеки повинна стосуватись: інформації (рівня критичності ресурсів організації), взаємодії об'єктів (правил, відповідальності за захист інформації, гарантій захисту), сфери застосування.

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

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

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

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

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

Спосіб провокування противника призначений для спонукання противника до здійснення будь-яких дій, корисних протилежній стороні.

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

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

1.5.6. Форми ведення інформаційної боротьби

До основних форм ведення інформаційної боротьби зазвичай відносять такі:

– 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 й 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. 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, 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. У такій операції головні зусилля сил і засобів спрямовуються на забезпечення інформаційної безпеки органів управління об’єднань і з’єднань, на захист інформації в системах керування. Частина сил і засобів спрямовуються на дезорганізацію управління військами і зброєю противника.

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

За масштабами інформаційні операції можна класифікувати як стратегічні, оперативно-стратегічні, оперативні й оперативно-тактичні та характеризувати такими основними показниками: просторовим розмахом, тривалістю, а також кількісним і якісним складом сил і засобів. Водночас необхідно відзначити, що ця специфічна галузь протиборства не передбачає використання таких чітко

Обмін інформацією й програмним забезпеченням між організаціями та окремими користувачами виконується згідно зі встановленими процедурами управління відповідно до чинного законодавства, стандартів або внутрішніх нормативних документів. Обміни варто виконувати на основі угод, або встановлювати внутрішні процедури й стандарти із захисту інформації й носіїв інформації при їх передачі. Ці 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 з управління 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 з формування й передачі пакетів;

– стандарти з ідентифікації кур’єра;

– відповідальність й обов’язки у разі 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 та 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.

Питання для самоконтролю

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

З цього погляду 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 з організації, а також проведення реєстрації всіх видалень для підтримки процедур аудиту;

– носії інформації повинні зберігатися в надійному, безпечному середовищі, відповідно до встановлених вимог.

Усі 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 в документах, обчислювальних системах, мережах, мобільних засобах зв'язку, пошті, мовній пошті, мовному зв'язку взагалі, системах із 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.

визначених для бойових дій понять, як фронт і тил (інформаційний вплив може здійснюватися на всю глибину території противника).

У деяких умовах не виключена можливість проведення в межах 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. Залежно від масштабу й 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 зазвичай називають **інформаційними акціями**, оскільки вони виходять за межі власне інформаційної боротьби у сфері інформаційного протиборства геополітичних суб'єктів.

Інформаційні дії (акції) можна класифікувати за видами (наступальні й оборонні), масштабом (стратегічні, оперативно-стратегічні, оперативні, оперативно-тактичні й тактичні) й об'єктами впливу (інформаційні системи, морально-психологічний стан особового складу та їхня комбінація). До наступальних інформаційних дій належать 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 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). У межах інформаційної блокади можуть також проводитися інформаційні удари різного виду та масштабу. Одним з основних способів досягнення мети інформаційної блокади у воєнний час є радіоелектронне **блокування** [electronic blocking] – узгоджений вплив засобами радіоелектронного придушення і функціонального ураження на технічні елементи систем розвідки й 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 й комбіновані) і ступенем зосередження сил і засобів (вибіркові, зосереджено масовані й 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 із системами керування противника, з метою зриву управління на окремих напрямках на певний час.

Комп'ютерний (програмний) удар – це узгоджений за часом, глибиною й 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.

1.5.7. 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 збройної боротьби в методології оцінки ефективності можна виділити два основних рівні. Перший (вищий) рівень включає оцінку ефективності у війнах і

Основна ідея стандарту – допомогти комерційним та державним господарським організаціям вирішити достатньо складне завдання: забезпечення надійного захисту інформаційних ресурсів та організація ефективного доступу до даних і процесу їх обробки згідно з визначеними послугами та вимогами.

Основна структура стандарту

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

2.4.4. Задачі організації безпеки інформації та інформаційних ресурсів

Забезпечення безпеки інформаційних мереж – запобігання ушкодженню інформаційних активів і переривання дій, пов'язаних із 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.

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.

2.4.3. 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 зі специфічними областями технічної діяльності. Технічні комітети ISO й IEC співпрацюють у сферах взаємного інтересу. Інші урядові й неурядові міжнародні організації, пов'язані з ISO й IEC, також беруть участь у цій роботі. Нині сформовано відповідні стандарти 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 цьому 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 тощо в контексті інформаційної безпеки.

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

збройних конфліктах загалом, 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 відповідно 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 певні взаємопов'язані етапи оцінки ефективності інформаційної боротьби:

– формування інформаційного кадастру органів керування протиборчих сторін;

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

– порівняльну оцінку величини показника інформованості органів керування своїми силами і засобами та 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:

$$F = K_1 / K_2 .$$

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

Питання для самоконтролю

1. Дати визначення інформаційної боротьби.
2. Яка мета інформаційної боротьби?
3. Які фактори впливають на зміст інформаційної боротьби?
4. Які існують заходи інформаційної боротьби?
5. Охарактеризувати принципи інформаційної боротьби**.**
6. Дати визначення метода оцінки ефективності інформаційної боротьби.
7. Які існують форми ведення інформаційної боротьби?
8. Які існують способи інформаційної боротьби?
9. Що таке радіоелектронно-вогневий удар?
10. Формула для обчислення числового значення критерію ефективності інформаційної боротьби.

РОЗДІЛ 2. ОСНОВИ БЕЗПЕКИ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

2.1. Основи безпеки інформаційних ресурсів

2.1.1. Поняття та загальні властивості інформації. Поняття загроз

На сьогодні є багато різних варіантів визначення суті терміна «інформація». Одне з визначень: інформація – це зафіксоване на носії уявлення про предмети, процеси, події, явища та ін.

Під фіксацією розуміють закріплення чого-небудь у певному положенні або вигляді. Найпростішим прикладом є письмове закріплення відомостей, думок. Інформація для свого функціонування завжди вимагає наявності носія.

При цьому носієм інформації може виступати поле або речовина. У деяких випадках як носій інформації може розглядатися людина. У процесі інформаційних відносин носії можуть бути або носіями-джерелами, або носіями-одержувачами залежно від напряму переміщення інформації. У Законі України «Про інформацію» під джерелами інформації розуміються передбачені, або встановлені Законом носії інформації: документи або інші носії інформації, які є матеріальними об'єктами, що зберігають інформацію. Стосовно одержувачів, то вони сприймають інформацію через той чи інший сенсор (датчик, вимірювальний перетворювач). Процес сприйняття є досить складним, включаючи процеси прийому та перетворення інформації, що забезпечує віддзеркалення об'єктивної реальності й орієнтування в навколишньому світі. Сприйняття може включати:

- виявлення об'єкта в полі сприйняття;
- розрізнення окремих ознак усередині об'єкта;
- виділення в ньому інформативного змісту, адекватного меті дії;
- формування образу сприйняття.

У наведеному вище визначенні терміна «інформація» під уявленням розуміється образ та/або суть предмета, процесу, події, природного явища тощо, сприйняті датчиками приладів або безпосередньо органами чуття, а також створені відтворювальною і/або творчою уявою людини чи елементами штучного інтелекту різних пристроїв. При цьому уява – це психічна діяльність, що полягає у створенні уявлень і уявних ситуацій, яка загалом не сприймалася людиною в реальній дійсності (творча уява) або відтворюють колишні враження і спогади, що спираються на життєвий досвід (відтворювальна уява). З огляду на вищевикладене вчені аналітично розрізняють відтворювальну й творчу уяву, але насправді ці обидва компоненти тісно взаємодіють між собою в процесі створення уявлень. Інформація має деякі істотні з погляду її захисту властивості. Ці властивості для користувача або власника інформації можна розглядати як деякі бажані стани інформації (носіїв інформації). Такими властивостями є:

– конфіденційність – властивість інформації бути захищеною від несанкціонованого ознайомлення;

– цілісність – властивість інформації бути захищеною від несанкціонованого спотворення, руйнування або знищення;

– доступність – властивість інформації бути захищеною від несанкціонованого блокування.

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 в 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 у мережі.

4. Контроль і відновлення цілісності всіх даних, що перебувають у 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 таким чином.

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

2. Канальний рівень – збільшення надійності захисту (за 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 погляду 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 цьому 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. Усі 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.

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 транспортної адреси в мережі, мультиплексування й 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 як стандарт. Він використовується як високонадійний протокол взаємодії між комп'ютерами в мережі з комутацією пакетів.

Протоколи верхніх рівнів. До протоколів верхніх рівнів відносяться протоколи **сеансового, представницького та 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 у 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 із 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 із 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 здебільшого не помічається легальними учасниками інформаційного обміну.

2. Умисне знищення або спотворення (фальсифікація) повідомлень у 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.

Події, які потенційно можуть порушити одну з названих властивостей інформації, відповідно, називають загрозами порушення конфіденційності, цілісності та доступності інформації.

Загрози порушення конфіденційності спрямовані на розголошення інформації з обмеженим доступом.

Загрози порушення працездатності (доступності) спрямовані на створення ситуацій, коли в результаті навмисних дій знижується працездатність обчислювальної системи, або її ресурси стають недоступними.

Загрози порушення цілісності полягають у спотворенні або зміні неавторизованим користувачем інформації, що зберігається або передається. Цілісність інформації може бути порушена як зловмисником, так і в результаті об'єктивних впливів зі сторони середовища експлуатації системи.

Вважають, що забезпечення безпеки інформації повинно носити комплексний характер. Усе більше фахівців пропонують свої рішення в галузі забезпечення безпеки інформаційних ресурсів як комплексні. Проте організація забезпечення безпеки інформації повинна носити не просто комплексний характер, але ще й ґрунтуватися на всебічному аналізі можливих негативних наслідків, за якого важливо не проігнорувати суттєві аспекти.

Порушення інформаційної безпеки можливе лише у випадках переміщення інформації. Наприклад, під час несанкціонованого ознайомлення (читання) документа з паперового носія відбувається переміщення (копіювання) інформації в мозок людини, яка стає носієм-одержувачем цієї інформації.

У процесі переміщення інформації може відбуватися зміна її носія. Наприклад, носіями інформації під час її переміщення можуть виступати:

– матеріальні середовища (повітря, вода, метал та ін.);

– сенсори або датчики;

– перетворювачі та інші об'єкти живої й неживої природи, що виконують функцію проміжних носіїв інформації.

Загрози *конфіденційності* спрямовані на заборонене режимом доступу переміщення інформації від носія-джерела до носія-одержувача. Інформація зберігає конфіденційність, якщо додержується насамперед режимна адекватність носіїв інформації.

Поняття «режимна адекватність» складається з термінів «режим» і «адекватність». Режим – це сукупність норм для досягнення якої-небудь мети. Наприклад, для захисту інформації. Тут обов'язково враховується режим доступу до інформації як передбачений правовими нормами порядок отримання, використання, поширення і зберігання інформації. Адекватність (від лат. adaequatus – прирівняний, рівний) – це відповідність, правильність, точність.

Смислове значення складових поняття «режимна адекватність носіїв інформації» є таким: це відповідність режимів доступу носіїв інформації (джерела та одержувача) під час їх взаємодії.

Загрози *цілісності* інформації спрямовані на заборонену режимом доступу (порядком отримання, використання, поширення та зберігання інформації) її зміну або спотворення, що призводить до порушення її якості або повного знищення. Цілісність інформації може бути порушена сумісно, а також унаслідок об'єктивного впливу з боку середовища, що оточує носій інформації.

Інформація зберігає цілісність, якщо дотримується встановлена режимна адекватність щодо правил її модифікації (видалення).

Будь-якого суб'єкта, що впливає на носій-джерело інформації з метою модифікації інформації, можна розглядати як носія інформації, що несе в собі уявлення про необхідну модифікацію (видалення) інформації носія-джерела інформації. У процесі модифікації також відбувається переміщення інформації, що модифікується.

Вплив об'єктів, процесів зовнішнього середовища та інших чинників, які часто відносять до «випадкових» – це невідповідність носія-джерела інформації встановленому режиму доступу, що часто призводить до порушення комунікабельності. Такий вплив є порушенням режимної адекватності, і як наслідок – комунікабельності носіїв інформації.

Термін «комунікабельність» (від пізньолатинського – communicabilis – той, що з'єднується) означає сумісність (здатність до спільної роботи) різнотипних систем передачі інформації (наприклад, в електрозв'язку – аналогових і дискретних, у телебаченні – з різним числом рядків розкладання телевізійного кадру тощо). Тому комунікабельні носії інформації – це носії інформації, здатні до взаємодії.

Приклад некомунікабельності носіїв: через такий сенсор, як органи зору (очі) людина не здатна сприйняти голосову (акустичну) інформацію. Приклад комунікабельності носіїв: через сенсор – органи зору (очі) людина здатна сприйняти інформацію, зафіксовану на паперовому носії зрозумілою для неї мовою.

Загрози доступності (відмова в обслуговуванні) спрямовані на навмисне або ненавмисне порушення комунікабельності носіїв інформації в процесі їх взаємодії. Порушення комунікабельності перериває дозволені режимом доступу процеси переміщення інформації. Інформація зберігає доступність, якщо зберігається комунікабельність носіїв інформації під час їх взаємодії.

Для правильного визначення об'єкта захисту необхідно знати основні поняття, пов'язані із секретною інформацією.

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

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

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

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

Доступ до відомостей, що становлять державну таємницю, – надання уповноваженою посадовою особою дозволу громадянину на ознайомлення з

Протокол канального рівня повинен забезпечити таке:

– 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 та служить для ідентифікації повідомлення, правильного прийому кадрів, відновлення і повторної передачі в разі помилок і т. ін. 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.

Отже, 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 й забезпечувати такі властивості: глобальну однозначність, маршрутну незалежність і незалежність від рівня послуг.

На мережевому рівні дані представляються у вигляді пакета, який містить інформаційне поле й 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:

– зі 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.

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

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 (табл. 2.1).

Таблиця. 2.1. 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.

конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, або ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, цією посадовою особою відповідно до її службових повноважень.

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

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

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

Ступінь секретності – категорія, що характеризує важливість такої інформації, можливі збитки внаслідок її розголошування, ступінь обмеження доступу до неї та рівень її охорони державою. Критерій визначення ступеня секретності інформації встановлює відповідний державний орган.

У разі потреби на державних підприємствах, в установах і організаціях з урахуванням особливостей їхньої діяльності розробляються й за узгодженням із міністерством, іншим центральним органом виконавчої влади, до сфери управління якого вони належать, вводяться в дію переліки конкретних видів документів у відповідній сфері діяльності.

Таким чином, для державної інформації з обмеженим доступом уже визначені відомості, які в обов'язковому порядку є об'єктом захисту.

2.1.2. Загрози безпеки інформації та інформаційних ресурсів

Насамперед заходи забезпечення інформаційної безпеки в організації спрямовуються тільки на те, щоб не допустити збитків від втрати інформації з обмеженим доступом. Відповідно до цього вже передбачається наявність цінної інформації, в разі втрати якої організація може понести збитки. А якщо є цінна інформація, то, безперечно ж, є можливість здійснення будь-яких дій, які можуть нанести шкоду цій інформації. Усі шкідливі дії можуть бути здійснені тільки при наявності будь-яких слабких місць. А якщо є дії, то є найвища загроза їх здійснення, а також наявні джерела, з яких ці загрози можуть виходити.

Виникає такий ланцюг: джерело загрози – фактор (вразливість) – загроза (дія) – наслідки (атака).

Джерело загрози – це потенційні антропогенні, техногенні або стихійні носії загрози безпеці.

Загроза (дія) – це можлива небезпека (потенційна або така, що існує реально) вчинення будь-якого діяння (дії або бездіяльності), спрямованого проти об'єкта захисту (інформаційних ресурсів), яке наносить збиток власнику або користувачу, що проявляється як небезпека спотворення або втрати інформації.

Фактор (вразливість) – це властиві об'єкту інформатизації причини, які призводять до порушення безпеки інформації на конкретному об'єкті та зумовлені вадами процесу функціонування об'єкта інформатизації, властивостями архітектури інформаційно-телекомунікаційної системи, протоколами обміну та інтерфейсами, що застосовуються, програмним забезпеченням і апаратними засобами.

Наслідки (атака) – це можливі наслідки реалізації загрози (можливі дії) під час взаємодії джерела загрози через наявні фактори (вразливості).

Атака – це завжди пара «джерело-фактор», що реалізує загрозу та призводить до збитків.

Прояви збитків можуть бути різноманітні:

– моральні й матеріальні збитки ділової репутації організації;

– моральні, фізичні або матеріальні збитки, пов'язані з розголошенням персональних даних окремих осіб;

– матеріальні (фінансові) збитки від розголошення конфіденційної інформації;

– матеріальні (фінансові) збитки від необхідності відновлення порушених інформаційних ресурсів;

– матеріальні збитки (втрати) від неможливості виконання взятих на себе зобов'язань перед третьою стороною;

– моральні та матеріальні збитки від дезорганізації діяльності організації;

– матеріальні та моральні збитки від порушення міжнародних відносин.

Треба відзначити, що збитки можуть бути спричинені як будь-яким суб'єктом (у цьому випадку відбувається правопорушення), так і бути наслідком незалежного від суб'єкта прояву (наприклад, стихійних випадків, або інших впливів, таких як прояви техногенних властивостей цивілізації).

У першому випадку наявна вина суб'єкта, яка визначає спричинену шкоду як склад злочину, що здійснюється зі злими намірами (навмисно) або з необережності, і спричинені збитки необхідно класифікувати як склад злочину, відповідно до кримінального права.

У другому випадку збитки носять імовірнісний характер і повинні бути зіставлені як мінімум із тим ризиком, який обговорюється цивільним, адміністративним або арбітражним правом, як предмет розгляду. Визначення того, хто саме є причиною збитків, є другим за важливістю (після спроби цього не допустити) питанням для потерпілого.

У теорії права під **збитками** розуміють невигідні для власника майнові наслідки, що виникли внаслідок правопорушення. Збитки виражаються у зменшенні майна, або в недоодержанні прибутку, який був би одержаний у разі відсутності правопорушення (втрачена вигода). Якщо розглядати як суб'єкт, що спричинив збитки, будь-яку особу), то категорія «збитки» є справедливою тільки в тому випадку, коли можна довести, що вони спричинені, тобто діяння особи необхідно кваліфікувати в термінах правових актів як склад злочину. Тому при класифікації загроз безпеці інформації в цьому випадку доцільно враховувати вимоги чинного кримінального права, які визначають склад злочину.

Для прикладу можна розглянути склади злочину, які визначаються кримінальними кодексами в багатьох державах.

Крадіжка – здійснення з корисливою метою протиправного безоплатного вилучення і (або) обіг чужого майна на користь винного або інших осіб, що спричинили збитки власникові майна.

Копіювання комп'ютерної інформації – це повторювання та стійке збереження інформації на машинному або іншому носієві.

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 із 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 такими критеріями:

1) за масштабом – локальні та глобальні;

2) за способом організації – централізовані і децентралізовані;

3) за топологією (конфігурації) – зіркоподібні, кільцеві, шинні, змішані.

Різновиди комп'ютерних мереж по виділених значенням перерахованих критеріїв характеризуються таким чином:

– локальні обчислювальні мережі – мережі, вузли яких розташовуються на невеликих відстанях один від одного;

– 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 й дерев'яні будинки), у 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.

Це питання розглянемо на прикладі найбільш поширеної і визнаної еталонної моделі взаємодії відкритих систем ISO / OSI (ВОС).

В основу еталонної моделі покладена ідея декомпозиції процесу функціонування відкритих систем на рівнях, причому розбиття на рівні проводиться таким чином, щоб згрупувати в межах 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 межах 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. У межах моделі ISO/OSI кожен конкретний рівень може взаємодіяти тільки із сусідніми. Сукупність правил (процедур) взаємодії об'єктів однойменних рівнів називається протоколом.

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 цієї 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 мережевих 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 цей 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, зокрема, розв'язання задачі про забезпечення безпеки інформації й захищеності даних.

2.4.2. 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 й мережеве обладнання. Для передачі інформації можуть бути використані різні фізичні явища, переважно різні види електричних сигналів чи електромагнітного випромінювання. Середовищами передавання в комп'ютерних мережах можуть бути телефонні кабелі, та спеціальні мережеві кабелі: коаксіальні кабелі, виті пари, волоконно-оптичні кабелі, радіохвилі, світлові сигнали. Мережа дає змогу окремим

Знищення – це зовнішній вплив на майно, у результаті якого воно припиняє своє існування або стає повністю непридатним для використання за цільовим призначенням. Знищене майно не може бути відновлене шляхом ремонту або реставрації та повністю виводиться з господарського обігу.

Знищення комп'ютерної інформації – стирання її у пам'яті комп'ютера.

Пошкодження – зміна властивостей майна, унаслідок якого суттєво погіршується його стан, втрачається значна частина його корисних властивостей і воно стає повністю або частково непридатним для цільового використання.

Модифікація комп'ютерної інформації – внесення будь-яких змін, крім пов'язаних з адаптацією програми для комп'ютера або баз даних.

Блокування комп'ютерної інформації – штучне ускладнення доступу користувачів до інформації, не пов'язане з її знищенням.

Несанкціоноване знищення, блокування, модифікація, копіювання інформації – будь-які дії з інформацією, що не дозволені законом, власником або компетентним користувачем.

Обман (заперечення автентичності, нав'язування хибної інформації) – навмисне спотворення або приховування істини з метою введення в оману особи, у веденні якої перебуває майно, і таким чином домогтися від неї добровільної передачі майна, а також повідомлення з цією метою свідомо неправдивих відомостей.

Якщо розглядати як суб'єкт, що спричинив збитки, будь-яке природне або техногенне явище, то під збитками можна розуміти невигідні для власника майнові наслідки, викликані цими явищами, які можуть бути компенсовані за рахунок третьої сторони (страхування ризиків настання події) або за рахунок власних засобів власника інформації.

2.1.3. Джерела загроз безпеці інформації

Носіями загроз безпеці інформації є **джерела загроз.** Джерелами загроз можуть бути як суб'єкти (особистість), так і об'єктивні прояви. Причому джерела загроз можуть бути як усередині організації – внутрішні джерела, так і ззовні її – зовнішні джерела. Поділ джерел на суб'єктивні та об'єктивні виправданий, зважаючи на попередні міркування щодо вини або ризику збитку інформації, а поділ на внутрішні та зовнішні джерела виправданий тому, що для тієї самої загрози методи відбиття для внутрішніх і зовнішніх загроз можуть бути різними.

Усі джерела загроз безпеці інформації можна поділити на три групи:

– зумовлені діями суб'єкта (антропогенні джерела загроз);

– зумовлені технічними засобами (техногенні джерела загроз);

– зумовлені стихійними джерелами.

Антропогенними джерелами загроз виступають суб'єкти, дії яких можуть бути кваліфіковані як навмисні або випадкові злочини. Тільки в цьому випадку можна говорити про заподіяння збитку. Ця група джерел загроз найбільш численна та становить найбільший інтерес з погляду організації захисту, оскільки дії суб'єкта завжди можна оцінити, спрогнозувати та прийняти адекватні заходи. Методи протидії у цьому випадку керовані й залежать від волі організаторів захисту інформації.

Антропогенним джерелом загроз можна вважати суб'єкта, що має доступ (санкціонований або несанкціонований) до роботи зі штатними засобами об'єкта, що потребує захисту. Суб'єкти (джерела), дії яких можуть призвести до порушення безпеки інформації, можуть бути як зовнішніми, так і внутрішніми. Зовнішні джерела можуть бути випадковими або навмисними та мати різний рівень кваліфікації.

Внутрішні суб'єкти (джерела) здебільшого являють собою висококваліфікованих спеціалістів у галузі розробки та експлуатації програмного забезпечення та технічних засобів, знайомих зі специфікою завдань, що вирішуються, структурою та основними функціями та принципами роботи програмно-апаратних засобів захисту інформації, які мають можливість використання штатного обладнання та технічних засобів мережі.

Необхідно враховувати також, що особливу групу внутрішніх антропогенних джерел складають особи з порушеною психікою та спеціально впроваджені та завербовані агенти, які можуть бути з числа основного, допоміжного та технічного персоналу, а також представників служби захисту інформації.

Друга група містить джерела загроз, що визначаються технократичною діяльністю людини та розвитком цивілізації. Проте наслідки, викликані такою діяльністю, вийшли з-під контролю людини та діють самі по собі. Людство дійсно стає все більше залежним від техніки, і джерела загроз, які залежать від властивостей техніки, менше прогнозовані й тому потребують особливої уваги. Цей клас джерел загроз безпеці інформації є особливо актуальним у сучасних умовах, оскільки очікується різке зростання кількості техногенних катастроф, викликаних фізичним та моральним старінням наявного обладнання, а також відсутністю коштів на його оновлення. Технічні засоби, що є джерелами потенційних загроз безпеці інформації, також можуть бути зовнішніми та внутрішніми.

Третя група джерел загроз об'єднує обставини, що становлять непереборну силу, тобто такі обставини, які носять об'єктивний і абсолютний характер, що поширюється на всіх. До непереборної сили в законодавстві та договірній практиці відносять стихійні лиха або інші обставини, які неможливо передбачити або їм запобігти або можливо передбачити, але не можливо запобігти їм при сучасному рівні знань і можливостей людини. Такі джерела загроз абсолютно не піддаються прогнозуванню, і тому заходи захисту від них повинні застосовуватися завжди.

Стихійні джерела потенційних загроз інформаційній безпеці переважно є зовнішніми щодо об'єкта захисту. Під ними розуміють насамперед природні катаклізми.

2.1.4. Класифікація вразливостей безпеки

Загрози, як можливі небезпечності здійснення будь-якої дії, спрямованої проти об'єкта захисту, проявляються не самі по собі, а через вразливості (фактори), що призводять до порушення безпеки інформації на конкретному об'єкті інформатизації.

Вразливості, властиві об'єкту інформатизації, невіддільні від нього та зумовлюються недоліками процесу функціонування, властивостями архітектури автоматизованих систем, протоколами обміну та інтерфейсами, програмним забезпеченням і апаратною платформою, умовами експлуатації та розташування.

2.4. Інформаційно-комунікаційні системи та комп'ютерні мережі

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 й відображення даних. Базовими властивостями інформаційних ресурсів є їхня 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.

2.4.1. Визначення інформаційно-комунікаційних систем

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 загалом потребує знання принципів роботи та характеристик її окремих елементів: комп'ютерів, комунікаційного устаткування, операційних систем, мережевих додатків і т. ін.

Багаторівневою моделлю інформаційно-комунікаційної системи називається повний інтегрований комплекс середовища та комунікаційних і 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.

Незважаючи 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 в глобальних мережах.

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. 2.3.

Рис. 2.3. Структура монітору звернень

Практичне створення монітору звернень, як видно з рис. 2.3, 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 й об'єкта доступу. На основі присвоєних кожному суб'єкту й об'єкту доступу конкретних рівнів і категорій у моделі визначаються їх рівні безпеки, а потім встановлюється їх взаємодія. При цьому в моделі приймається, що один рівень безпеки домінує над іншим тільки тоді, коли відповідний йому рівень конфіденційності більше чи дорівнює конфіденційності іншого, а множина категорій включає множину категорій другого.

Питання для самоконтролю

1. Які існують категорії джерел конфіденційної інформації?
2. Які складові має інформаційна система?
3. Розкрийте поняття «цілісність».
4. Розкрийте поняття «доступність».
5. Розкрийте поняття конфіденційності інформації.
6. Назвіть основні напрями забезпечення безпеки інформації.
7. Розкрийте зміст моделі системи захисту інформації.
8. Якими показниками може бути оцінено якість розподілу доступу?
9. Назвіть основні принципи та рівні захисту інформаційних систем.

Джерела загроз можуть використовувати вразливості для порушення безпеки інформації, одержання незаконної вигоди (нанесення збитків власникові, користувачеві інформації). Крім того, можливі не зловмисні дії джерел загроз з активізації тих чи інших вразливостей, що завдають шкоду.

Кожній загрозі можуть бути зіставлені різноманітні вразливості. Усунення або суттєве послаблення вразливостей впливає на можливість реалізації загроз безпеці інформації.

Вразливості безпеці інформації можуть бути: об'єктивними, суб'єктивними, випадковими.

Об'єктивні вразливості залежать від особливостей побудови та технічних характеристик обладнання, що застосовується на об'єкті захисту. Повне усунення цих вразливостей неможливе, але вони можуть суттєво послаблятися технічними та інженерно-технічними методами відбиття загроз безпеці інформації.

Суб'єктивні вразливості залежать від дій співробітників і, в основному, вилучаються організаційними та програмно-апаратними методами.

Випадкові вразливості залежать від особливостей середовища, яке оточує об'єкт захисту, та непередбачених обставин. Ці фактори зазвичай малопередбачувані і їх усунення можливе тільки при проведенні комплексу організаційних та інженерно-технічних заходів із протидії загрозам інформаційній безпеці.

2.1.5. Моделі порушень інформаційних ресурсів

Інформаційні ресурси інформаційних систем (ІС), передусім розподілені бази даних та знань, є привабливими з погляду розміщеної на них інформації, не тільки для авторизованих користувачів інформаційної системи, а також для окремих осіб або певних груп осіб, які прагнуть бути її користувачами. Ця привабливість зумовлена характером і обсягом інформації, що вводиться, обробляється, зберігається та циркулює в ІС.

Якщо та або інша особа – користувач ресурсами ІС здійснює спробу несанкціонованого (не авторизованого) доступу до інформаційних ресурсів системи (з метою: ознайомлення, модифікації, знищення, зміни режимів використання або загального функціонування системи тощо), то такий користувач є порушником.

Порушення з боку цих осіб можуть бути як ненавмисними, так і зловмисними. Особливу небезпеку варто очікувати від зловмисних порушників, які в силу тих або інших причин перебувають під впливом:

- кримінальних осіб та їх угруповань;
- бізнесменів, комерсантів та їх об'єднань;
- політичних діячів і партій;
- агентів спецслужб інших держав, або самі входять до їх складу.

Припустимим характером дій з боку цих порушників варто вважати бажання й прагнення одержати необхідні для порушника дані для подальшого використання, модифікації або знищення з метою досягнення певних умов для себе, своїх підприємств, прихильників або конкурентів.

Крім того, необхідно враховувати, що використання ресурсів ІС, насамперед інформаційних, і їх модифікація або знищення можуть бути здійснені порушником (зловмисниками) навмисно, або ненавмисно (неправильні, непередбачені дії без

злих намірів, внаслідок недбалості тощо). При цьому порушники можуть бути внутрішніми (із числа співробітників, користувачів ІС) або зовнішніми (сторонні особи чи особи, які перебувають за межами контрольованої зони, або проникли в її межі несанкціонованим шляхом).

Кваліфікація порушника

Варто очікувати, що порушники мають певний рівень кваліфікації, достатній для успішної реалізації загроз ресурсам ІС, тобто:

– володіють інформацією щодо функціональних особливостей ІС, уміють користуватися штатними засобами;

– володіють високим рівнем знань в обслуговуванні ідентичних засобів ІС;

– володіють високим рівнем знань у галузі обчислювальної техніки й програмування на мовах розробки програмних засобів ІС, проектуванню й експлуатації подібних до ІС систем;

– володіють інформацією щодо функцій і механізмів захисту, які реалізовані як у системі захисту інформації ІС, так і у функціях і механізмах захисту, що вбудовані в базове та прикладне програмне забезпечення.

За рівнем можливостей, які надаються штатною інфраструктурою інформаційної мережі, виділяють чотири рівні порушників.

Класифікація ієрархічна, тобто кожний наступний рівень містить у собі функціональні можливості попереднього рівня:

– перший рівень відповідає найбільш низькому рівню можливостей порушника у системі – можливістю запуску фіксованого набору програм, які реалізують певні функції з обробки інформації;

– другий рівень визначається можливістю створення й запуску власних програм із новими функціями обробки й подальшого одержання потрібної порушнику інформації;

– третій рівень визначається можливістю управління функціонуванням ІС, тобто впливом на базове програмне забезпечення системи, а також на склад і конфігурацію технічного забезпечення інформаційної системи;

– четвертий рівень визначається інтегрованим обсягом можливостей співробітників, які здійснюють розробку, впровадження й експлуатацію технічних засобів інформаційної системи, а також можливістю введення до складу інформаційної системи власних технічних засобів із новими функціями, щодо обробки й отримання інформації.

Ступінь ризику

Нижче наведено приблизний перелік персоналу ІС і відповідний ступінь ризику щодо можливої реалізації загроз та нанесення шкоди залежно від зазначених робочих функцій працівників:

– найбільший ризик: системний адміністратор; адміністратор бази даних; адміністратор безпеки;

– високий ризик: оператор системи; оператор введення й підготовки даних; менеджер обробки даних; системний програміст;

– середній ризик: інженер системи; менеджер програмного забезпечення;

– обмежений ризик: прикладний програміст; інженер і оператор зв’язку; інженер з устаткування; оператор периферійного устаткування; бібліотекар

– захищати або відключати в локальній обчислювальній мережі протоколи канального або мережевого рівня, які не використовуються та розділяти мережу на сегменти;

– проводити регулярні тренінги, спрямовані на підвищення обізнаності користувачів у питаннях інформаційної безпеки (при цьому важливо проводити й оцінювання 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.

2.3.5. Основні принципи захисту інформації

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

– управління доступом до ІС, до її послуг та ресурсів;

– реєстрація й 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 таких 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 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 у системі, включаючи будь-які операції з конфіденційною інформацією і можливі порушення її захисту.

Принцип цілісності засобів захисту. Цей принцип передбачає, що засоби захисту інформації в ІС повинні чітко виконувати свої функції згідно з переліченими принципами й бути ізольованими від користувачів, а для свого супроводу повинні включати спеціальний захищений інтерфейс для засобів

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 й отримання повного контролю над усією IT-інфраструктурою або окремими критично важливими системами.

Здебільшого для отримання максимальних привілей у критично важливих системах від імені внутрішнього порушника досить підібрати обліковий запис із привілеями локального адміністратора на одній із робочих станцій або на сервері ЛОМ, запустити спеціалізоване ПО й отримати у відкритому вигляді облікові записи локальних адміністраторів інших вузлів. Цей 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 вразливостей захисту внутрішніх ресурсів належить недолікам захисту протоколів мережевого й 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. Цей недолік може бути використаний для прослуховування трафіку в мережі і проведення атак типу «людина посередині». У ході успішної реалізації атаки порушник може перехоплювати конфіденційну інформацію, змінювати дані в процесі передачі і блокувати мережеву взаємодію.

Друге місце серед вразливостей внутрішніх мереж посідає використання словникових паролів. Третє місце – недостатній рівень захисту привілейованих облікових записів.

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

Необхідно також відзначити, що вектори атак на корпоративні інфраструктури ґрунтуються на експлуатації поширених вразливостей і недоліків, для усунення яких зазвичай 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;

– регулярно оновлювати ПЗ і встановлювати оновлення безпеки ОС;

– для своєчасного виявлення атак використовувати SIEM-системи;

– мінімізувати привілеї користувачів і служб;

– для захисту веб-додатків використовувати web application firewalls;

системних магнітних носіїв; користувач-програміст; користувач-операціоніст;

– низький ризик: інженер по периферійному устаткуванню; бібліотекар магнітних носіїв користувачів.

Цілі й мета порушника:

– особиста авторизація, тобто одержати особисті легальні атрибути доступу, з бажано найширшими правами щодо доступу до ресурсів ІС, з метою їхнього використання, одержання необхідної інформації в потрібному обсязі, ознайомлення з конфіденційною інформацією, одержання можливості її модифікації або знищення згідно зі своїми намірами;

– авторизувати інших осіб, які б мали можливість одержати легальні атрибути доступу, з бажано найширшими правами щодо доступу до ресурсів ІС з метою їхнього використання, одержання необхідної інформації в потрібному обсязі, ознайомлення з конфіденційною інформацією, одержання можливості її модифікації або знищення згідно зі своїми намірами;

– знайти прихильників або довірених осіб серед персоналу або користувачів ІС, які мають можливість одержувати легальні атрибути доступу до ресурсів ІС з метою їхнього використання, одержання необхідної інформації в потрібному обсязі, ознайомлення з конфіденційною інформацією, одержання можливості її модифікації або знищення згідно зі своїми намірами.

У разі відсутності можливості або безуспішності реалізації вищенаведених дій порушник може мати наміри:

1. Одержання атрибутів доступу користувачів шляхом використання технічних засобів, крадіжок, купівлі, або одержання іншим шляхом.

2. Проникнення на місця розміщення тих або інших компонентів, елементів або ресурсів ІС (обчислювальних ресурсів, інформаційних ресурсів, базового й прикладного програмного забезпечення та програмного забезпечення системи технічного захисту інформації (ТЗІ), включаючи носії резервні копії, ресурсів введення/виводу інформації, телекомунікаційного устаткування, включаючи мережу передачі даних) шляхом подолання охорони або охоронної сигналізації та ін.

3. Зміни режимів функціонування ІС, її ресурсів та послуг системи.

4. Установки фізичних засобів у місцях розміщення елементів ІС (технічних закладок) чи інших засобів технічної розвідки (у тому числі віддалених, наприклад, в елементах комунікаційної мережі зв’язку) для перехвату інформації.

5. Установки фізичних засобів у місцях розміщення елементів ІС (технічних закладок) або інших засобів (у тому числі віддалених, наприклад, в елементах комунікаційної мережі зв’язку) для генерації хибних сигналів, інформаційних символів або спотворених повідомлень.

6. Установки програмних засобів (програмних закладок або вірусів), копіювання інформації з метою її використання.

7. Установки програмних засобів (програмних закладок або вірусів) для модифікації системного програмного забезпечення, так і інформації ІС, шляхом введення програмних вірусів, спотворених сигналів, інформаційних символів або хибних повідомлень з метою перевантаження систем і порушення, таким чином, доступності компонентів ІС.

8. Здійснення спроб несанкціонованого доступу до обчислювальних та інформаційних ресурсів, базового та прикладного програмного забезпечення.

9. Здійснення спроб несанкціонованого доступу до системи захисту інформації як частини ІС, так і до її телекомунікаційної підсистеми, шляхом подолання системи управління доступом.

Рівень знань порушника

Порушник може знати:

– склад, розміщення, функціональні особливості, умови й режими функціонування елементів ІС, включаючи траси прокладених або можливих ліній зв'язку, комунікаційних мереж зв'язку й трафіки відповідних каналів передачі даних;

– порядок, засоби й режими здійснення охорони елементів ІС, місця їх розміщення і навколишню територію;

– порядок, засоби й режими здійснення організаційно-правових і технічних заходів захисту ресурсів ІС;

– основні закономірності формування в ІС баз даних і потоків запитів до них;

– за характером дій зловмисник може здійснювати: активні або пасивні дії, стосовно ресурсів і функціональних властивостей захищеності інформаційних об'єктів ІС.

Під активною загрозою розуміється спроба навмисної несанкціонованої зміни стану функціонування ІС, а під пасивною загрозою – спроба несанкціонованого проникнення в систему без зміни її стану.

За характером дій порушників можна класифікувати на:

– випадкових порушників – авторизованих користувачів, які порушили політику безпеки тієї або іншої послуги ненавмисно, а помилково, шляхом виконання непередбачених дій з об'єктом захисту, шляхом випадкового подолання засобів управління доступом тощо;

– терплячих зловмисників – авторизованих користувачів, які порушили політику безпеки тієї або іншої послуги навмисно, але без рішучих дій, маскуючись, шляхом підбору атрибутів доступу інших користувачів з метою схованого подолання засобів управління доступом тощо;

– рішучих зловмисників, які мають на меті порушити ту або іншу властивість інформації. Зловмисники прагнуть перебороти: засоби організаційного обмеження доступу, охоронної сигналізації, керування доступом до фізичних ресурсів, елементи будівельних конструкцій, тощо й одержати можливість фізичного доступу до засобів обробки, зберігання або передачі інформаційних ресурсів з метою виводу їх з ладу, зміни режимів функціонування, крадіжки носіїв інформації та ін.;

– зловмисників, які використовують засоби віддаленого доступу до інформаційних об'єктів з умов: витоку інформації технічними каналами, реалізації спеціальних впливів на інформацію з технічних каналів, впливу на мережеве устаткування локальних або розподілених мереж, у тому числі й засоби телекомунікаційних мереж, які використовуються елементами ІС.

Дії порушників можуть бути спрямованими на порушення функціональних властивостей захищеності інформаційних об'єктів, зокрема на порушення:

– конфіденційності, цілісності й доступності інформаційних об'єктів;

– функцій спостереження за діяльністю користувачів і процесів, однозначної ідентифікації користувачів, ресурсів і процесів.

2. Словникові паролі.
3. Недостатній рівень захисту привілейованих облікових записів.
4. Зберігання важливої інформації у відкритому вигляді.
5. Недоліки захисту протоколів NBNS і LLMNR.
6. Недостатньо ефективна реалізація антивірусного захисту.
7. Використання слабких алгоритмів шифрування при зберіганні паролів.
8. Уразливі версії програмного забезпечення.
9. Надлишкові привілеї додатків або СУБД.
10. Використання відкритих (незахищених) протоколів передачі даних.

Водночас 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. У середньому у 27 % випадків фахівцям не вдається подолати мережевий периметр і отримати доступ до ресурсів внутрішньої локальної обчислювальної мережі. Такі результати пов'язані з тим, що деякі замовники регулярно проводять тестування на проникнення й 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 й 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. У процесі оцінювання обізнаності співробітників у 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

– системний підхід;

– адаптивне управління (вибір оптимального способу досягнення мети, це спосіб управління, за 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 усіх етапів розробки проекту, контрольних точок, необхідних ресурсів.

Такий підхід забезпечує розробку інтегрованих рішень, побудованих на об'єктивних даних про роботу підприємства, своєчасне узгодження всіх принципових питань між замовником, генеральним підрядником та іншими учасниками робіт і спрямований на збереження зроблених у систему інвестицій.

Корпоративні інформаційні системи великих компаній регулярно зазнають змін - оновлюється конфігурація обладнання, змінюється топологія мереж, з'являються нові вузли й цілі системи. Для більшості корпорацій із розподіленою інфраструктурою процес безперервного забезпечення комплексного захисту інформаційних активів стає непростим завданням через високу складності архітектури і великої кількості взаємозв'язків всередині окремих підсистем. За результатами аналітики у 2017 році найбільш поширені уразливості на мережевому периметрі корпоративних інформаційних систем розподілені таким чином (рис. 2.2):

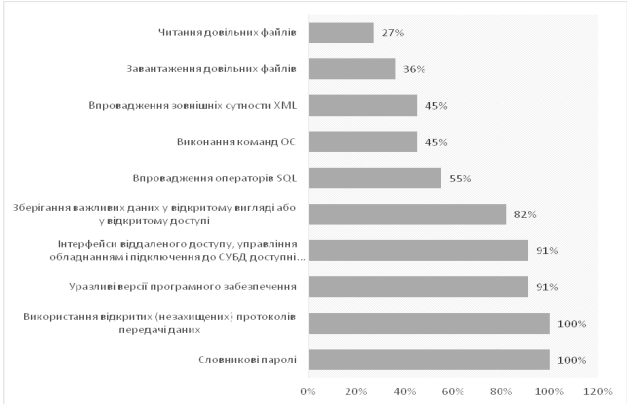

Рис. 2.2. Найбільш поширені уразливості на мережевому периметрі (частка систем)
Джерело за даними аналітики компанії Positive Technologies 2017 рік.

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

1. Недоліки захисту службових протоколів, що призводять до перенаправлення трафіку і перехоплення інформації про конфігурацію мережі.

Така класифікація дає змогу чітко визначити методи та засоби запобігання несанкціонованим діям порушників, а також визначити організаційно-правові заходи, які потрібні для побудови комплексної системи захисту інформації.

Порушники можуть використовувати такі методи та засоби:

– агентурні методи одержання відомостей через підкуплених користувачів і персонал, а також через прихильників чи довірених осіб із числа штатних працівників або таких, які мають доступ до ресурсів ІС;

– пасивні технічні засоби перехоплення інформаційних сигналів;

– штатні засоби ІС або недоліки проектування системи захисту інформації від несанкціонованого доступу (НСД);

– методи й засоби активного впливу на елементи ІС, які змінюють конфігурацію ІС (підключення додаткових або модифікація штатних технічних засобів, підключення або «врізання» у канали передачі даних, впровадження й використання спеціального ПЗ і т. ін.).

За місцем здійснення порушень дії зловмисника можна класифікувати:

– без одержання доступу на контрольовану територію із використанням технічних засобів віддаленого доступу через засоби: Internet, електронної пошти, модемного зв'язку чи дистанційної розвідки (наприклад: по оптичних, акустичних каналах, каналах побічних електромагнітних випромінювань і т. ін.), або з використанням засобів одержання інформації з мережі передачі даних (наприклад: шляхом підключення або «врізання» в лінії зв'язку);

– з одержанням доступу на контрольовану територію ІС або до робочих місць кінцевих користувачів, але без доступу до технічних засобів ІС, також із використанням технічних засобів дистанційної розвідки з подальшим несанкціонованим доступом до будинків, або приміщень, у яких розміщені елементи ІС;

– з одержанням доступу до робочих місць кінцевих користувачів ІС із подальшим несанкціонованим доступом до пристроїв введення/виводу інформації, копіювання, до канального або устаткування, яке утворює канал і до інших елементів ІС;

– з одержанням доступу до засобів управління ІС і засобів управління комплексною системою захисту інформації з подальшими розширеними можливостями доступу до ресурсів ІС та послуг системи.

2.1.6. Побудова моделі порушника

Для подальшої організації надійного захисту інформації організації повинні не тільки оцінити весь спектр можливих погроз, але і спробувати виявити категорії порушників і ті методи, які вони використовують.

Розглянемо тепер модель порушника. Порушник (user violator) – користувач, який здійснює несанкціонований доступ до інформації. Оскільки під порушником розуміється людина, то цілком зрозуміло, що створення його формалізованої моделі – дуже складне завдання. Тому, безперечно, йдеться тільки про неформальну, або описову модель порушника.

Зазначимо, що існує визначення: хакер (hacker) і кракер (cracker). Основна відмінність складається в постановці цілей злому комп'ютерних систем: перші

ставлять дослідницькі задачі з оцінки та знаходження слабких місць з метою подальшого підвищення надійності комп'ютерної системи. Кракери виконують вторгнення в систему з метою руйнування, крадіжки, псування, модифікації інформації та роблять правопорушення з корисливими намірами швидкого збагачення. Але ці два поняття зводяться до одного поняття – порушник.

Порушник – це особа, яка може отримати доступ до роботи з включеними до складу ІС засобами. Вона може помилково, унаслідок необізнаності, цілеспрямовано, свідомо чи несвідомо, використовуючи різні можливості, методи та засоби, здійснити спробу виконати операції, які призвели або можуть призвести до порушення властивостей інформації, що визначені політикою безпеки.

У кожному конкретному випадку для кожного об'єкта визначаються ймовірні загрози й моделі потенційних порушників – «провідників» цих загроз, включаючи можливі сценарії їх здійснення. Цей етап дуже складний, оскільки від служби безпеки (СБ) вимагається для кожного об'єкта вибрати з кількох можливих типів порушників один, на який і буде орієнтована СБ, що проектується.

Модель порушника відображає його практичні та потенційні можливості, апріорні знання, час та місце дії тощо.

При розробці моделі порушника визначаються:

– припущення щодо категорії осіб, до яких може належати порушник;

– припущення щодо мотивів дій порушника (цілей, які він має);

– припущення щодо рівня кваліфікації та обізнаності порушника і його технічної оснащеності (щодо методів та засобів, які використовуються у процесі здійснення порушень);

– обмеження та припущення щодо характеру можливих дій порушників (за часом та місцем дії та інші).

Припускається, що за своїм рівнем порушник – це фахівець вищої кваліфікації, який має повну інформацію про систему.

Зазвичай розглядаються 5 типів порушників. Спочатку їх поділяють на дві групи:

– зовнішні;

– внутрішні порушники.

Серед зовнішніх порушників виділяють такі:

– добре озброєна й оснащена силова група, що діє ззовні швидко й напролом;

– поодинокий порушник, що не має допуску на об'єкт і намагається діяти потайки й обережно, оскільки він усвідомлює, що сили реагування мають переваги.

Серед потенційних внутрішніх порушників можна відзначити:

– допоміжний персонал об'єкта, що допущений на об'єкт, але не допущений до життєво важливого центру ІС;

– основний персонал, що допущений до життєво важливого центру (найбільш небезпечний тип порушників);

– співробітників служби безпеки, які часто формально і не допущені до життєво важливого центру, але реально мають достатньо широкі можливості для збору необхідної інформації і вчинення акції.

Має також розглядатися можливість змови між порушниками різних типів, що ще більше ускладнює задачу формалізації моделей порушника.

2.3.4. 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. Загалом КІС – це система з можливістю масштабування, призначена для комплексної автоматизації всіх видів господарської діяльності великих і середніх підприємств, у 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 й 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 із можливістю застосування промислових СУБД;

– забезпечення безпеки методами контролю й 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 поділяються на такі 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 (ставлення клієнта до компанії, ступінь його задоволеності, інноваційний потенціал компанії і співробітників, якість бізнес-процесів та ін.);

– комплексний підхід до управління;

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 у своїх інтересах, при цьому обслуговуючий персонал, включаючи технічний і оперативний склад, є співробітниками цієї 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 цієї 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 й обробляється в системі. Здебільшого загрози інформаційній безпеці розрізняються за способом їх реалізації.

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

Загрози, які не пов'язані з навмисними діями зловмисників і реалізуються у випадкові моменти часу, називають випадковими або ненавмисними.

Реалізація загроз цього класу призводить до найбільших втрат (за статистичними даними - до 80% від збитку, що наноситься інформаційних ресурсів ІС-якими загрозами). У результаті реалізації таких загроз можливе безпосереднє порушення цілісності та доступності інформації, а також створення передумов для зловмисних дій щодо інформації.

Характеризуючи загрози інформації в ІС, не пов'язані з навмисними діями в цілому, слід зазначити, що механізм їх реалізації вивчений досить добре, накопичений значний досвід протидії цим загрозам.

Характеристики загроз цього класу з плином часу змінюються незначно. Сучасна технологія розробки технічних і програмних засобів, ефективна система експлуатації ІС, що включає обов'язкове резервування інформації, дозволяють значно знизити втрати від реалізації загроз цього класу.

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.

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

Але необхідно зазначити, що такий поділ є дуже загальним, а також не всі групи мають важливе значення для всіх ІС.

Серед внутрішніх порушників можна виділити такі категорії персоналу:

– користувачі (оператори) системи;

– персонал, що обслуговує технічні засоби (інженери, техніки);

– співробітники відділів розробки та супроводження ПЗ (прикладні та системні програмісти);

– технічний персонал, що обслуговує будівлю (прибиральниці, електрики, сантехніки та інші співробітники, що мають доступ до будівлі та приміщення, де розташовані компоненти ІС);

– співробітники служби безпеки;

– керівники різних рівнів та посадової ієрархії.

Сторонні особи, що можуть бути порушниками:

– клієнти (представники організацій, громадяни);

– відвідувачі (запрошені з якого-небудь приводу);

– представники організацій, що займаються забезпеченням життєдіяльності організації (енерго-, водо-, теплопостачання і т. ін.);

– представники конкуруючих організацій (іноземних служб) або особи, що діють за їхнім завданням;

– особи, які випадково або навмисно порушили пропускний режим (не маючи на меті порушити безпеку);

– будь-які особи за межами контрольованої зони.

Можна виділити також три основні мотиви порушень:

– безвідповідальність;

– самоствердження;

– з корисною метою.

При порушеннях, викликаних безвідповідальністю, користувач цілеспрямовано або випадково здійснює руйнівні дії, які не пов’язані, проте, зі злим умислом. У більшості випадків – це наслідок некомпетентності, недбалості або невдоволення.

Деякі користувачі вважають одержання доступу до системних наборів даних значним успіхом, затіваючи свого роду гру «користувач – проти системи» заради самоствердження або у власних очах, або в очах колег.

Порушення безпеки ІС може бути викликане корисливим інтересом користувача системи. У цьому випадку він буде цілеспрямовано намагатися перебороти систему захисту для доступу до інформації в ІС. Навіть якщо ІС має засоби, що роблять таке проникнення надзвичайно складним, цілком захистити її від проникнення практично неможливо.

Усіх порушників можна класифікувати за рівнем знань про ІС:

– знає функціональні особливості ІС, основні закономірності формування в ній масивів даних і потоків запитів до них, уміє користуватися штатними засобами;

– має високий рівень знань і досвід роботи з технічними засобами системи;

– має високий рівень знань у галузі програмування й обчислювальної техніки, проектування й експлуатації автоматизованих інформаційних систем;

– знає структуру, функції і механізм дії засобів захисту, їх сильні та слабкі сторони.

За рівнем можливостей (методами та засобами, що використовуються):

– застосовує суто агентурні методи отримання відомостей;

– застосовує пасивні засоби (технічні засоби перехоплення без модифікації компонент системи);

– використовує тільки штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні магнітні носії інформації, які можуть бути потайки пронесені через пости охорони;

– застосовує методи та засоби активного впливу (модифікація та підключення додаткових технічних засобів, підключення до каналів передавання даних, впровадження програмних закладок та використання спеціальних інструментальних та технологічних програм).

За часом дії:

– у процесі функціонування (під час роботи компонент системи);

– у період коли система неактивна (у неробочий час, під час планових перерв у її роботі, перерв для обслуговування та ремонтів тощо);

– як у процесі функціонування, так і в період коли компонент системи неактивний.

Визначення конкретних характеристик можливих порушників є значною мірою суб'єктивним. Модель порушника, що побудована з урахуванням особливостей конкретної предметної галузі і технології обробки інформації, може бути подана перелічуванням кількох варіантів його образу. Кожний вид порушника має бути охарактеризований згідно з класифікаціями, наведеними вище. Усі значення характеристик мають бути оцінені (наприклад, за 5-бальною системою) і зведені до відповідних форм.

Однак при формуванні моделі порушника на її виході обов'язково повинні бути визначені: імовірність реалізації загрози, своєчасність виявлення й відомості про порушення.

Питання для самоконтролю

1. Що є джерелом та фактором загрози інформації?
2. Які є види загроз комп'ютерної інформації?
3. Які є групи джерел загроз безпеці інформації?
4. Наведіть класифікацію вразливостей безпеці інформації?
5. Які класи (види) загроз розрізняються в інформаційній сфері?
6. Які загрози відносяться до рівня порушення конфіденційності ?
7. Які загрози відносяться до рівня порушення цілісності ?
8. Які існують категорії джерел конфіденційної інформації?
9. Які є моделі порушень інформаційних ресурсів?
10. Яка мета та цілі порушника об'єктів інформаційної діяльності?
11. Наведіть класифікацію порушника за характером дій?

– 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. 2.1 рівнів.

Організація захисту на фізичному рівні повинна зменшити можливість несанкціонованих дій сторонніх осіб і персоналу підприємства, а також зменшити 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 й будуватись на основі використання сукупності вбудованих систем захисту операційної системи і систем управління базами даних та знань.

Рис. 2.1. Рівні захисту інформаційної системи

На локальному рівні організовується 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 й мінімізація кількості точок входу/виходу (точок взаємодії) між сегментами, створення надійної оболонки по периметру сегментів і інформаційної системи загалом, організація захищеного обміну інформацією між сегментами.

На мережевому рівні організовується захищений інформаційний обмін даними між автоматизованими робочими місцями, а також створюється надійна оболонка фізичного захисту периметра розташування ІС загалом. 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.

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 взаємної несуперечності. Підтримка цілісності бази даних містить перевірку цілісності й 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 із 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.

2.3.3. 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. ін.);

– 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 переважно 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 й контролю її захищеності.

Система захисту інформації повинна виконувати такі функції:

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

– забезпечення цілісності прикладного програмного забезпечення;

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

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

2.2. Забезпечення безпеки інформації та інформаційних ресурсів

2.2.1. Основні напрями забезпечення безпеки інформації

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

З урахуванням практики, що склалася на теперішній час, виділяють такі **напрями захисту інформації**:

– правовий захист – це спеціальні закони, інші нормативні акти, правила, процедури та заходи, що забезпечують захист інформації на правовій основі;

– організаційний захист – це регламентація виробничої діяльності та відносин виконавців на нормативно-правовій основі, яка виключає або послаблює нанесення будь-яких збитків виконавцям;

– інженерно-технічний захист – це використання різноманітних технічних засобів, що перешкоджають нанесенню збитків.

Крім того, заходи захисту, орієнтовані на забезпечення безпеки інформації, можуть бути охарактеризовані багатьма параметрами, що відображають, крім напрямів, орієнтацію на об’єкти захисту, характер загроз, способи дій, їх поширення, охоплення та масштабність.

Так, за характером загроз заходи захисту орієнтовані на захист інформації від розголошення, витоку та несанкціонованого доступу. За способом дії їх можна поділити на попередження, виявлення, припинення та відновлення збитків або інших утрат. За охопленням заходи захисту можуть поширюватись на територію, будівлю, приміщення, апаратуру або окремі елементи апаратури. Масштабність заходів захисту характеризується як об’єктовий, груповий або індивідуальний захист.

2.2.2. Правовий захист

Поняття **права** визначається як сукупність загальнообов’язкових правил і норм поведінки, які встановлені або санкціоновані державою, щодо певних сфер життя та діяльності державних органів, підприємств (організацій) та населення (окремої особи).

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

У нашій державі такими правилами (актами, нормами) є Конституція України, закони України, цивільне, адміністративне, кримінальне право, викладене у відповідних кодексах. Що стосується відомчих нормативних актів, то вони визначаються наказами, керівництвами та інструкціями, які видаються відомствами, організаціями та підприємствами, що діють у межах певних структур.

Сучасні умови вимагають і визначають необхідність комплексного підходу до формування законодавства із захисту інформації, його складу та змісту, співвіднесення його зі всією системою законів та правових актів України.

Вимоги інформаційної безпеки повинні органічно входити до всіх рівнів законодавства, у тому числі в конституційне законодавство, основні загальні закони, закони з організації державної системи управління, спеціальні закони, відомчі правові акти і т. ін. Зазвичай використовується наступна структура правових актів, які орієнтовані на правовий захист інформації.

Конституційне законодавство – норми, що стосуються питань інформатизації та захисту інформації, входять до нього як складові елементи.

Загальні закони, кодекси (про власність, про надра, про права громадян, про громадянство, про податки, про антимонопольну діяльність і т. ін.), які включають норми з питань інформатизації та інформаційної безпеки.

Закони про організацію управління стосовно окремих структур господарства, економіки, системи державних органів та визначення їхнього статусу. Такі закони включають окремі норми з питань захисту інформації. Поряд із загальними питаннями інформаційного забезпечення та захисту інформації конкретного органу ці норми повинні встановлювати його обов'язки з формування, актуалізації та безпеки інформації, що представляє загальнодержавний інтерес.

Спеціальні закони, які відносяться до конкретних сфер відносин, галузей господарства, процесів. До їхнього числа входять Закони України «Про інформацію», «Про захист інформації в автоматизованих системах» і т. ін. Власне склад і зміст цього блоку законів і створює спеціальне законодавство як основу правового забезпечення інформаційної безпеки.

Підзаконні нормативні акти із захисту інформації.

Правоохоронне законодавство України, яке містить норми про відповідальність за правопорушення у сфері інформатизації.

Спеціальне законодавство в галузі безпеки інформації може бути представлене сукупністю законів. В їхньому складі особливе місце посідають Закони України «Про інформацію» та «Про захист інформації в автоматизованих системах», які закладають основи правового визначення всіх найважливіших компонентів інформаційної діяльності:

– інформації та інформаційних систем;

– суб'єктів – учасників інформаційних процесів;

– правовідносин виробників та споживачів інформаційної продукції;

– власників (джерел) інформації - обробників та споживачів на основі відносин власності при забезпеченні гарантій інтересів громадян та держави.

Ці закони також визначають основи захисту інформації в системах обробки і при її використанні з урахуванням категорій доступу до відкритої інформації і до інформації з обмеженим доступом. Ці закони містять, крім того, загальні норми з організації та ведення інформаційних систем, включаючи банки даних державного призначення, порядок державної реєстрації, ліцензування, сертифікації, експертизи, а також загальні принципи захисту та гарантій прав учасників інформаційного процесу.

Питання правового режиму інформації з обмеженим доступом реалізуються у двох самостійних законах про державну та комерційну (проект) таємниці.

Таким чином, правовий захист інформації забезпечується нормативно-законодавчими актами, сукупність яких за рівнем являє собою ієрархічну систему від Конституції України до функціональних обов'язків і контрактів конкретного

потенціалу, які перебувають у власності суспільства і які у разі 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 такі характеристики: конфіденційність, доступність та цілісність інформації (даних) в інформаційній системі.

Конфіденційність – 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 розуміється 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 в можливості їхнього отримання користувачем або програмою. Визначається певними факторів: можливістю працювати за терміналом, володінням паролем, знанням мови запитів та ін.

Цілісність – це внутрішня єдність, пов'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, за якого 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 й не зруйновані (стерті).

комплектуючі та ін. 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.

2.3.2. 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. Усе 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, як і будь-яка інша, має певну структуру, склад, фахівців, засоби, обладнання й 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 такі складові:

1. Користувачі.

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

3. Носії інформації:

- на паперовій основі;
- звуконосії;
- відеоносії;
- магнітні носії;
- спеціальні технічні носії.

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

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

Вихідною матеріальною основою роботи інформаційної системи виступають інформаційні ресурси. Ресурсами, як відомо, називають елементи економічного

виконавця, які визначають перелік відомостей, що підлягають охороні, і заходи відповідальності за їх розголошення.

Одним із нових напрямків правового захисту є страхове забезпечення. Воно призначене для захисту власної інформації та засобів її обробки як від традиційних загроз (крадіжки, стихійні лиха), так і від загроз, що виникають у ході роботи з інформацією. До них належать розголошення, витік та несанкціонований доступ до конфіденційної інформації.

Метою страхування є забезпечення страхового захисту фізичних та юридичних осіб від страхових ризиків у вигляді повного або часткового відшкодування збитків і втрат, які спричинені стихійними лихами, надзвичайними подіями в різних галузях діяльності, протиправними діями з боку конкурентів та зловмисників шляхом виплати грошової компенсації або надання сервісних послуг (ремонт, відновлення) при настанні страхової події.

Спираючись на державні правові акти та враховуючи відомчі інтереси на рівні конкретного підприємства (фірми, організації), розробляються власні нормативно-правові документи, орієнтовані на забезпечення інформаційної безпеки. До таких документів відносяться:

- положення про збереження конфіденційної інформації;
- перелік відомостей, які складають конфіденційну інформацію;
- інструкція про порядок допуску співробітників до відомостей, які становлять конфіденційну інформацію;
- положення про спеціальне діловодство та документообіг;
- перелік відомостей, які дозволені до опублікування у відкритому друці;
- положення про роботу з іноземними фірмами та їхніми представниками;
- зобов'язання співробітника про збереження конфіденційної інформації;
- пам'ятка співробітнику про збереження комерційної таємниці.

Наведені вище нормативні акти спрямовані на попередження випадків неправомірного оголошення (розголошення) секретів на правовій основі – у випадку їх порушення повинні вживатися відповідні заходи впливу.

Залежно від характеру інформації, її доступності для зацікавлених споживачів, а також економічної доцільності конкретних захисних заходів, можуть бути обрані такі форми захисту інформації:

- патентування;
- авторське право;
- признання відомостей конфіденційними;
- застосування норм зобов'язального права.

Існує певна різниця між авторським, правом та комерційною таємницею. Авторське право захищає тільки форму вираження ідеї. Комерційна таємниця відноситься безпосередньо до змісту. Авторське право захищає від копіювання незалежно від конфіденційних відносин із власником. До авторського права вдаються при широкій публікації своєї інформації, у той час як комерційну таємницю тримають у секреті. Очевидно, що порівняно з патентом та авторським правом комерційна таємниця та виробнича таємниці є найбільш зручними, надійними та гнучкими формами захисту інформації.

Крім вищевикладених форм правового захисту та права належності інформації, знаходить велике поширення офіційна передача права на користування нею у вигляді ліцензії.

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

Комерційна таємниця – це відомості, які не є державними секретами, пов'язані з виробництвом, технологією, управлінням, фінансами та іншою діяльністю, розголошення, витік та несанкціонований доступ до якої може призвести до збитків їхнім власникам.

До комерційної таємниці не відносяться:

– відомості, що охороняються державою;

– відомості, які є загальновідомими на законній підставі;

– відомості про негативні сторони діяльності;

– установчі документи та відомості про господарську діяльність.

Створюючи систему інформаційної безпеки, необхідно чітко розуміти, що без правового забезпечення захисту інформації будь-які наступні претензії до несумлінного співробітника, клієнта, конкурента та посадової особи будуть просто безпідставними.

Якщо перелік відомостей конфіденційного характеру не доведений своєчасно до кожного співробітника (природно, якщо він допущений до виконання посадових обов'язків) у письмовому вигляді, то співробітник, який викрав важливу інформацію при порушенні встановленого порядку роботи з нею скоріше всього не буде покараний.

Правові норми забезпечення безпеки та захисту інформації на конкретному підприємстві (фірмі, організації) відображаються в сукупності установчих, організаційних та функціональних документів.

Вимоги забезпечення безпеки та захисту інформації відображаються у Статуті (установчому договорі) у вигляді таких положень:

– підприємство має право визначати склад, обсяги та порядок захисту конфіденційних відомостей, вимагати від своїх співробітників забезпечення їх збереження та захисту від внутрішніх та зовнішніх загроз;

– підприємство зобов'язане забезпечувати збереження конфіденційної інформації.

Ці вимоги дають **адміністрації підприємства такі права**:

– створювати організаційні структури із захисту конфіденційної інформації;

– видавати нормативні та розпорядчі документи, які визначають порядок виділення відомостей конфіденційного характеру та механізми їхнього захисту;

– включати вимоги із захисту інформації в угоди з усіх видів діяльності;

– вимагати захисту інтересів підприємства з боку державних інстанцій;

– розробляти «Перелік відомостей конфіденційної інформації».

групою джерел. За специфікою призначення й виконання їх можна поділити 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 різноманітні 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 й системи. Усі 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 ПК і інформаційних систем як джерел конфіденційної інформації зумовлена певними об'єктивними особливостями, до числа яких відносяться:

– різке розширення сфери застосування інформаційної й обчислювальної техніки (ПК, 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 ПК та мереж: багатокористувальницький режим вилученого доступу до баз даних.

Привабливість полягає ще й у тому, що АСОІ містить досить значні асортименти інформації. В її базах даних є вся інформація про конкретне підприємство – від досьє на співробітників до конкретної продукції, її характеристики, 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 розповісти про використовувані матеріали, їхній 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

2.3. Захист інформаційних систем

2.3.1. Джерела конфіденційної інформації

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

Взагалі джерелами конфіденційної інформації можна вважати такі 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, як джерела конфіденційної інформації, посідають особливе місце, як активні елементи, здатні виступати не тільки власниками конфіденційної інформації, але й суб'єктами зловмисних дій. Люди є і власниками, і поширювачами інформації в межах 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 тощо) із зафіксованою на ньому інформацією, призначеною 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.

За спрямованістю 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 поділяються на первинні та вторинні. До первинних належать 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 учені, 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 ПК, 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

2.2.3. Організаційний захист

Організаційний захист – це регламентація виробничої діяльності та відносин виконавців на нормативній основі, що виключає або суттєво ускладнює неправомірне оволодіння конфіденційною інформацією та прояву внутрішніх та зовнішніх загроз.

Організаційний захист забезпечує:

– організацію режиму, охорони, роботу з кадрами, з документами;

– використання технічних засобів безпеки та інформаційно-аналітичну діяльність із виявлення внутрішніх і зовнішніх загроз діяльності підприємства (організації).

Організаційні заходи відіграють суттєву роль у створенні надійного механізму захисту інформації, оскільки можливості несанкціонованого використання конфіденційних відомостей значною мірою обумовлюються не технічними аспектами, а зловмисними діями та недбалістю користувачів або персоналу. Впливу цих аспектів практично неможливо запобігти за допомогою технічних заходів. Для цього необхідна сукупність організаційно-правових і організаційно-технічних заходів, які вилучали б (або зводили до мінімуму) можливість виникнення небезпеки конфіденційності інформації.

До **основних організаційних заходів** зазвичай відносять такі:

– організація режиму та охорони – їх мета:

– виключення можливості таємного проникнення на територію та в приміщення сторонніх осіб;

– забезпечення зручності проходу та переміщення співробітників та відвідувачів;

– створення окремих виробничих зон за типом конфіденційних робіт із самостійними системами доступу;

– контроль та дотримання часового режиму праці та перебування на території персоналу підприємства;

– організація та підтримка надійного пропускного режиму та контролю співробітників і відвідувачів і т. ін.;

– організація роботи зі співробітниками, яка передбачає підбір і розстановку персоналу, включаючи ознайомлення зі співробітниками, їх вивчення, навчання правилам роботи з конфіденційною інформацією, ознайомлення з мірою відповідальності за порушення правил захисту інформації;

– організація роботи з документами та документованою інформацією, включаючи організацію розробки та використання документів і носіїв конфіденційної інформації, їх облік, використання, повернення, зберігання та знищення;

– організація використання технічних засобів збирання, обробки, нагромадження та зберігання конфіденційної інформації;

– організація роботи з аналізу внутрішніх та зовнішніх загроз конфіденційній інформації та розробка заходів із забезпечення її захисту;

– організація роботи з проведення систематичного контролю за роботою персоналу з конфіденційною інформацією, порядком обліку, зберігання та знищення документів та технічних носіїв.

У кожному конкретному випадку організаційні заходи носять специфічну для цієї організації форму та зміст, які спрямовані на забезпечення безпеки інформації в конкретних умовах.

Особливості організаційного захисту комп'ютерних інформаційних систем

Організація захисту комп'ютерних інформаційних систем та мереж визначає порядок і схему функціонування основних їхніх підсистем, використання пристроїв та ресурсів, відносини користувачів між собою відповідно до нормативно-правових вимог та правил. Захист інформації на основі організаційних заходів відіграє значну роль у забезпеченні надійності та ефективності, оскільки несанкціонований доступ та витік інформації найчастіше зумовлені зловмисними діями, недбалістю користувачів або персоналу. Ці фактори практично неможливо виключити або локалізувати за допомогою апаратних і програмних засобів, криптографії та фізичних засобів захисту, тому сукупність організаційних, організаційно-правових та організаційно-технічних заходів, які застосовуються разом із технічними методами, мають за мету виключити, зменшити або повністю усунути збитки при дії різноманітних деструктивних факторів.

Організаційні засоби захисту комп'ютерних інформаційних систем та мереж найчастіше застосовуються в таких випадках:

– при проектуванні, будівництві та обладнанні приміщень, вузлів мереж та інших об'єктів інформаційної системи для запобігання впливу стихійного лиха, можливості недозволеного проникнення в приміщення і т. ін.;

– при доборі та підготовці персоналу – у цьому випадку передбачається перевірка осіб, які приймаються на роботу, створення умов, за яких персонал був би зацікавлений у збереженні інформації, навчання правилам роботи із закритою інформацією, ознайомлення з мірою відповідальності за порушення правил захисту;

– при зберіганні та використанні документів та інших носіїв (маркування, реєстрація, визначення правил видачі та повернення, ведення документації тощо);

– при дотриманні надійного пропускного режиму до технічних засобів комп'ютерних мереж та систем при роботі змінами (призначення відповідальних за захист інформації у змінах, контроль за роботою персоналу, ведення автоматизованих журналів роботи, знищення встановленим порядком закритих виробничих документів);

– при внесенні змін у програмне забезпечення (суворе санкціонування, розгляд та затвердження проектів змін, перевірка їх на задоволення вимог захисту, документальне оформлення змін і т. ін.);

– при підготовці та контролі роботи користувачів.

Служба захисту інформації

Одним із найважливіших організаційних заходів є створення спеціальних штатних служб захисту інформації в закритих інформаційних системах у вигляді адміністратора безпеки мережі та адміністратора безпеки розподілених баз та банків даних, які містять відомості конфіденційного характеру.

Цілком очевидно, що організаційні заходи повинні чітко плануватися, спрямовуватися та здійснюватися певною організаційною структурою, певним спеціально створеним для цих цілей структурним підрозділом, укомплектованим відповідними фахівцями з безпеки діяльності та захисту інформації.

Найбільш розповсюдженим способом шифрування мовного сигналу є аналогове скремблювання та цифрове шифрування.

Аналогове скремблювання – це перетворення аналогового сигналу з будь-якими статистичними властивостями в сигнал, що змінюється за випадковим або псевдовипадковим законом. При аналоговому скремблюванні характеристики вхідного мовного повідомлення змінюються таким чином, що перетворене повідомлення стає неприйнятим для слухової системи людини, але займає ту ж саму смугу частот. Це дозволяє передавати скрембльовані сигнали звичайними телефонними каналами зв'язку.

Останнім часом знайшли значне поширення системи шифрування, у яких застосовується *цифрове шифрування мовної інформації*, яка представлена у цифровій формі.

Для передавання мови в цифровій формі стандартними телефонними каналами різко скорочують смугу мовного сигналу за допомогою пристроїв, які називають *вокодерами.*

Шифрування мовної інформації у цифровій формі здійснюється відомими методами (заміною, перестановками, аналітичними перетвореннями, гамуванням і т. ін.) або за допомогою стандартних алгоритмів криптографічного перетворення. Перевагою цифрового шифрування є висока надійність закриття мовної інформації, оскільки перехоплений сигнал являє собою випадкову цифрову послідовність. Недоліком є необхідність використання модемів, нестійка робота пристроїв шифрування в каналах із великим загасанням сигналу та з високим рівнем завад.

Апаратні, програмні, апаратно-програмні та криптографічні засоби реалізують ті чи інші послуги інформаційної безпеки різноманітними механізмами захисту, які забезпечують дотримання конфіденційності, цілісності, доступності та повноти інформації.

Питання для самоконтролю

1. Які напрями захисту інформації ви знаєте?
2. Сформулюйте поняття права.
3. Яка структура правових актів, які орієнтовані на правовий захист інформації?
4. Дати визначення ліцензії.
5. Що таке комерційна таємниця?
6. Що забезпечує організаційний захист?
7. Назвіть основні організаційні заходи.
8. Функції служби безпеки підприємства (фірми, організації).
9. Завдання служби безпеки підприємства (фірми, організації).
10. Що таке інженерно-технічний захист? Його завдання.
11. Фізичні засоби захисту та їх завдання.
12. Які апаратні засоби захисту інформації Ви знаєте?
13. Що таке криптографія?
14. Назвіть переваги цифрового шифрування.

Криптографічні засоби захисту

Криптографія (від грец. – «секретний, прихований» і – «пишу, креслю, малюю») – спосіб тайнопису, заснований на використанні шифру, де під шифром зазвичай розуміють сукупність обернених перетворень тексту повідомлень, які виконуються з метою схову від зловмисника (противника) інформації, яка міститься в повідомленні.

Криптографія включає декілька розділів сучасної математики, а також спеціальні галузі фізики, теорії інформації та зв'язку і деяких інших суміжних дисциплін.

Як наука про шифри, криптографія довгий час була засекречена, оскільки застосовувалася переважно для захисту державних і воєнних секретів. Проте на теперішній час методи та засоби криптографії використовуються для забезпечення інформаційної безпеки не тільки держави, але і приватних осіб та організацій. Справа тут зовсім не обов'язково в секретах. Дуже багато різноманітних відомостей циркулює по всьому світу в цифровому вигляді. І над цими відомостями буквально «висять» загрози несанкціонованого ознайомлення, нагромадження, підміни, фальсифікації і т. ін. Найбільш надійні методи захисту від таких загроз дає саме криптографія.

Для криптографічного перетворення інформації використовуються різноманітні шифрувальні засоби, такі як засоби шифрування документів, засоби шифрування мови, засоби шифрування телеграфних повідомлень та передачі даних.

Вихідна інформація, яка передається каналами зв'язку, може являти собою мову, дані, відеосигнали, називається незашифрованим повідомленням.

У пристрої шифрування повідомлення шифрується і передається незахищеним каналом зв'язку. На приймальній стороні повідомлення дешифрується для відновлення вихідного повідомлення.

Параметр, який може застосовуватися для добування окремого повідомлення називається **ключем.**

У сучасній криптографії розглядаються два типи *криптографічних алгоритмів* (ключів). Це класичні криптографічні алгоритми, засновані на використанні секретних ключів та нові криптографічні алгоритми з відкритими ключами, засновані на використанні двох типів ключів: секретного (закритого) та відкритого.

У *криптографії з відкритими ключами* є, як правило, два ключі, один з яких неможливо визначити з іншого. Якщо ключ розшифровування обчислювальними методами неможливо одержати з ключа зашифровування, то секретність інформації, зашифрованої за допомогою несекретного (відкритого) ключа, буде забезпечена. Проте цей ключ повинен бути захищеним від підміни або модифікації. Ключ розшифровування також повинен бути секретним і захищеним від підміни або модифікації.

Якщо, навпаки, обчислювальними методами неможливо одержати ключ зашифровування з ключа розшифровування, то ключ розшифровування може бути не секретним.

Розділення функцій шифрування та розшифровування на основі розділення на дві частини додаткової інформації, необхідної для виконання операцій, є тією цінною ідеєю, яка лежить в основі криптографії з відкритим ключем.

Найчастіше таким структурним підрозділом є **служба безпеки підприємства** (фірми, організації), на яку покладаються **такі функції**:

– організація та забезпечення охорони персоналу, матеріальних та фінансових цінностей та захисту конфіденційної інформації;

– забезпечення пропускного та внутрішньооб'єктного режиму на території, у будівлях та приміщеннях, контроль дотримання вимог режиму співробітниками, суміжниками, партнерами та відвідувачами;

– керівництво роботами з правового та організаційного регулювання відносин із захисту інформації;

– участь у розробці основоположних документів з метою закріплення в них вимог забезпечення безпеки та захисту інформації, а також положень про підрозділи, трудові договори, угоди, підряди, посадові інструкції та обов'язки керівництва, спеціалістів, робітників та службовців;

– розробка та здійснення разом з іншими підрозділами заходів із забезпечення роботи з документами, що містять конфіденційні відомості; при всіх видах робіт організація та контроль виконання вимог «Інструкції із захисту конфіденційної інформації»;

– вивчення всіх сторін виробничої, комерційної, фінансової та іншої діяльності для виявлення та наступної протидії будь-яким спробам нанесення збитків, ведення обліку та аналіз порушень режиму безпеки, накопичення та аналіз даних про зловмисні прагнення конкурентної та інших організацій, про діяльність підприємства та його клієнтів, партнерів, суміжників;

– розробка, ведення, оновлення та поповнення «Переліку відомостей, що носять конфіденційний характер» та інших нормативних актів, які регламентують порядок забезпечення та захисту інформації;

– забезпечення суворого виконання вимог нормативних актів із забезпечення виробничих секретів підприємства;

– здійснення керівництва службами та підрозділами безпеки підвідомчих підприємств, організацій, закладів та іншими структурами;

– організація та регулярне проведення обліку співробітників підприємства та служби безпеки з усіх напрямів захисту інформації та забезпечення безпеки виробничої діяльності;

– ведення обліку та суворого контролю виділених для конфіденційної роботи приміщень, технічних засобів у них, що мають потенційні канали витоку інформації та канали проникнення до джерел інформації, які перебувають під охороною;

– забезпечення проведення всіх необхідних заходів із припинення спроб нанесення моральних та матеріальних збитків з боку внутрішніх та зовнішніх загроз;

– підтримка контактів із правоохоронними органами та службами безпеки сусідніх підприємств для вивчення криміногенної ситуації в районі (зоні) та надання взаємної допомоги в кризових ситуаціях.

Служба безпеки є самостійною організаційною одиницею підприємства, що підпорядковується безпосередньо керівникові підприємства. Очолює службу безпеки начальник служби безпеки в посаді заступника керівника підприємства з безпеки.

Організаційно *служба безпеки* може складатися з таких *структурних одиниць:*

– підрозділу режиму та охорони;
– спеціального підрозділу з обробки документів конфіденційного характеру;
– інженерно-технічних підрозділів;
– інформаційно-аналітичних підрозділів.

У такому складі служба безпеки здатна забезпечити захист конфіденційної інформації від будь-яких загроз.

На *служби безпеки* покладаються такі *завдання*:

– визначення кола осіб, які відповідно до положення, яке вони посідають на підприємстві, прямо чи непрямо мають доступ до відомостей конфіденційного характеру;

– визначення ділянок зосередження конфіденційних відомостей;

– визначення кола сторонніх підприємств, пов'язаних із даним підприємством кооперативними зв'язками, на яких у силу виробничих відносин можливий вихід з-під контролю відомостей конфіденційного характеру;

– виявлення кола осіб, не допущених до конфіденційної інформації, але які проявляють підвищений інтерес до таких відомостей;

– виявлення кола підприємств, у тому числі іноземних, що зацікавлені в доступі до відомостей, які охороняються, з метою нанесення економічних збитків даному підприємству, усунення економічного конкурента або його компрометації;

– розробка системи захисту документів, що містять відомості економічного характеру;

– визначення на підприємстві ділянок, уразливих в аварійному відношенні, вихід із ладу яких може нанести матеріальні збитки підприємству та зірвати поставки готової продукції або комплектуючих підприємствам;

– визначення на підприємстві технологічного обладнання, вихід (або виведення) якого з ладу може призвести до великих економічних втрат;

– визначення та обґрунтування заходів правового, організаційного та інженерно-фізичного захисту підприємства, персоналу, продукції та інформації;

– розробка необхідних заходів, спрямованих на вдосконалення системи економічної, соціальної та інформаційної безпеки;

– впровадження в діяльність підприємства новітніх досягнень науки та техніки, передового досвіду у галузі забезпечення економічної та інформаційної безпеки;

– організація навчання співробітників служби безпеки відповідно до їх функціональних обов'язків;

– вивчення, аналіз та оцінка стану забезпечення економічної та інформаційної безпеки підприємства та розробка пропозицій та рекомендацій для його удосконалення;

– розробка техніко-економічних обґрунтувань, спрямованих на придбання технічних засобів, одержання консультації у спеціалістів, розробку необхідної документації з метою удосконалення системи заходів із забезпечення економічної та інформаційної безпеки.

Організаційні заходи є вирішальною ланкою формування та реалізації комплексного захисту інформації та створення системи безпеки підприємства.

Програмні засоби захисту мають такі різновиди спеціальних програм:

– ідентифікації технічних засобів, файлів та аутентифікації користувачів;
– реєстрації та контролю роботи технічних засобів та користувачів;
– обслуговування режимів обробки інформації з обмеженим доступом;
– захисту операційних систем ПК та прикладних програм користувачів;
– знищення інформації у запам'ятовуючих пристроях після використання;
– допоміжні програми захисту різноманітного призначення.

Ідентифікація технічних засобів і файлів, яка здійснюється програмно, реалізується на основі аналізу реєстраційних номерів різних компонентів та об'єктів інформаційної системи та співставлення їх із значеннями адрес та паролів, що зберігаються в запам'ятовуючому пристрої системи управління.

Для забезпечення надійності захисту за допомогою паролів робота системи захисту зорганізується таким чином, щоб імовірність розкриття секретного пароля та встановлення відповідності тому чи іншому ідентифікатору файла або термінала була як можна меншою. Для цього потрібно періодично змінювати пароль, а кількість символів у ньому встановлювати достатньо великою.

Ефективним способом ідентифікації елементів з адресами та аутентифікації користувачів є алгоритм «запит-відповідь», відповідно до якого система захисту видає користувачеві запит на пароль, після чого він повинен дати на нього певну відповідь. Оскільки моменти введення запиту та відповіді на нього непередбачені, це ускладнює процес відгадування пароля, що забезпечує високу надійність захисту.

Одержання дозволу на доступ до тих чи інших ресурсів можна здійснити не тільки на основі використання секретного пароля та наступних процедур аутентифікації та ідентифікації. Це можна зробити більш детальним способом, який враховує різні особливості режимів роботи користувачів, їхні повноваження, категорії даних і ресурсів, що запитуються. Цей спосіб реалізується спеціальними програмами, які аналізують відповідні характеристики користувачів, зміст завдань, параметри технічних і програмних засобів, пристроїв пам'яті тощо.

Конкретні дані запиту, які поступають у систему, порівнюються в процесі роботи програми захисту з даними, які занесені в реєстраційні секретні таблиці (матриці). Ці таблиці, а також програми для їхнього формування та обробки зберігаються в зашифрованому вигляді та перебувають під особливим контролем адміністратора безпеки інформаційної мережі.

Для розмежування доступу окремих користувачів до певної інформації застосовуються індивідуальні заходи секретності цих файлів та особливий контроль доступу до них користувачів. Гриф секретності може формуватися у вигляді кодових слів, що складаються з трьох розрядів, які зберігаються у файлі або в спеціальній таблиці. У цій же таблиці записується ідентифікатор користувача, який створив цей файл, ідентифікатори терміналів, з яких може здійснюватися доступ до цього файлу, а також їхні права на користування файлом (зчитування, редагування, стирання, оновлення, виконання і т. ін.). Важливо не допустити взаємовплив користувачів у процесі звернення до файлів. Якщо, наприклад, один запис має право редагувати декілька користувачів, то кожному з них необхідно зберегти саме його варіант редакції (робиться декілька копій запису з метою можливого аналізу та встановлення повноважень).

два-три додаткових розряди, за допомогою яких кодуються категорії секретності користувачів, програм, даних).

Програми та дані, які завантажуються в ОЗП, потребують захисту, що гарантує їх від несанкціонованого доступу. Часто використовуються біти парності, ключі, постійна спеціальна пам'ять. При зчитуванні з ОЗП необхідно, щоб програми не могли бути знищені несанкціонованими діями користувачів або внаслідок виходу з ладу апаратури. Відмови повинні своєчасно виявлятися та усуватися, щоб запобігти виконанню спотвореної команди ЦП та втрати інформації.

Для попередження зчитування даних в ОЗП, які залишилися після обробки, застосовується спеціальна програма стирання. У цьому випадку формується команда на стирання ОЗП та вказується адреса блоку пам'яті, який повинен бути звільнений від інформації. Ця схема записує нулі або будь-яку іншу послідовність символів у всі комірки цього блока пам'яті, забезпечуючи надійне стирання раніше завантажених даних.

Апаратні засоби захисту застосовуються й у терміналах користувачів. Для попередження витоку інформації при приєднанні незареєстрованого терміналу необхідно перед видачею запитуваних даних здійснити ідентифікацію (автоматичне визначення коду або номера) терміналу, з якого поступив запит. У багатокористувальницькому режимі цього терміналу його ідентифікації недостатньо. Необхідно здійснити аутентифікацію користувача, тобто встановити його дійсність та повноваження. Це необхідно й тому, що різні користувачі, зареєстровані в системі, можуть мати доступ тільки до окремих файлів, і суворо обмежені повноваження їхнього використання.

Для ідентифікації термінала найчастіше застосовується генератор коду, включений до апаратури терміналу, а для аутентифікації користувача - такі апаратні засоби як ключі, персональні кодові картки, персональний ідентифікатор, пристрої розпізнавання голосу користувача або форми його пальців. Проте найбільш поширеними засобами аутентифікації є паролі, перевірені не апаратними, а програмними засобами впізнавання.

Апаратні засоби захисту інформації - це різноманітні технічні пристрої, системи та споруди, призначені для захисту інформації від розголошення, витоку й несанкціонованого доступу.

Програмний захист інформації - це система спеціальних програм, які входять до складу програмного забезпечення та реалізують функції захисту інформації.

Виділяють такі напрями використання програм для забезпечення безпеки конфіденційної інформації:

- захист інформації від несанкціонованого доступу;
- захист інформації від копіювання;
- захист програм від вірусів;
- захист інформації від вірусів;
- програмний захист каналів зв'язку.

За кожним із вказаних напрямів існує достатня кількість якісних, розроблених професіональними організаціями програмних продуктів, представлених на інформаційному ринку.

2.2.4. Інженерно-технічний захист

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

Основне завдання інженерно-технічного захисту – це попередження розголошення, витоку, несанкціонованого доступу та інших форм незаконного втручання в інформаційні ресурси.

Різноманітність цілей, завдань, об'єктів захисту та заходів, що проводяться, передбачають розгляд деякої системи класифікації засобів інженерно-технічного захисту за видом, орієнтацією та іншими характеристиками.

Наприклад, засоби інженерно-технічного захисту можна класифікувати за об'єктами впливу, характером заходів, способами реалізації, масштабом охоплення, класом засобів зловмисників, яким здійснюється протидія з боку служби безпеки.

За функціональним призначенням засоби інженерно-технічного захисту поділяються на такі групи: фізичні засоби захисту, апаратні засоби захисту, програмні засоби захисту, криптографічні засоби захисту.

Фізичні засоби включають різноманітні пристрої та споруди, які перешкоджають фізичному проникненню (або доступу) зловмисників на об'єкти захисту та матеріальних носіїв конфіденційної інформації та здійснюють захист персоналу, матеріальних носіїв, фінансів та інформації від протиправних дій.

До **апаратних засобів** відносяться прилади, пристрої, та інші технічні рішення, які використовуються в інтересах захисту інформації. Основне завдання апаратних засобів – забезпечення стійкого захисту від розголошення, витоку і несанкціонованого доступу через технічні засоби забезпечення діяльності організації (підприємства).

Програмні засоби охоплюють спеціальні програми, програмні комплекси та системи захисту інформації в інформаційних системах різноманітного призначення та засобах обробки (збирання, нагромадження, зберігання, обробки та передачі) даних.

Криптографічні засоби – це спеціальні математичні та алгоритмічні засоби захисту інформації, що передається системами та мережами зв'язку, зберігається та обробляється на ЕОМ із використанням різноманітних методів шифрування.

Апаратні методи та засоби захисту знайшли достатньо широке розповсюдження. Проте із-за того, що вони не мають достатньої гнучкості, часто втрачають свої захисні властивості при розкритті принципу їхньої дії й у подальшому не можуть бути використані.

Програмні методи та засоби більш надійні, період їхнього гарантованого використання значно більший, ніж апаратних методів та засобів.

Криптографічні методи та засоби посідають важливе місце і є надійним засобом забезпечення захисту інформації на тривалі періоди.

Очевидно, що такий поділ засобів захисту інформації достатньо умовний, оскільки на практиці дуже часто вони взаємодіють і реалізуються у вигляді програмно-апаратних засобів із широким використанням алгоритмів закриття інформації.

Фізичні засоби захисту – це різноманітні пристрої, конструкції, апарати, вироби, призначені для створення перепон на шляху руху зловмисників.

До фізичних засобів відносяться механічні, електромеханічні, електронні, електронно-оптичні, радіо- і радіотехнічні та інші пристрої для заборони несанкціонованого доступу (входу, виходу), пронесення (винесення) засобів і матеріалів та інших можливих видів злочинних дій.

Ці засоби застосовуються для вирішення таких завдань:

– охорона території підприємства та спостереження за нею;
– охорона будівель, внутрішніх приміщень та контроль за ними;
– охорона обладнання, продукції, фінансів та інформації;
– здійснення контрольованого доступу до будівель та приміщень.

Усі фізичні засоби захисту об'єктів можна поділити на три категорії: засоби попередження, засоби виявлення та системи ліквідації загроз. Охоронна сигналізація та охоронне телебачення, наприклад, відносяться до засобів виявлення загроз; загорожі навколо об'єктів – це засоби попередження несанкціонованого проникнення на територію, а підсилені двері, стіни, стелі, грати на вікнах та інші заходи служать захистом також і від проникнення, і від інших злочинних дій (підслуховування, обстрілу, кидання гранат і т. ін.). Засоби пожежогасіння належать до систем ліквідації загроз.

У загальному випадку за фізичною природою та функціональним призначенням усі засоби цієї категорії можна поділити на такі групи:

– охоронні та охоронно-пожежні системи;
– охоронне телебачення;
– охоронне освітлення;
– засоби фізичного захисту.

До засобів фізичного захисту належать:

– природні та штучні перепони (бар'єри);
– особливі конструкції периметрів, проходів, віконних та дверних прорізів, приміщень, сейфів, сховищ і т. ін.;
– зони безпеки.

Природні та штучні бар'єри призначені для протидії незаконному проникненню на територію об'єкта. Проте основне захисне навантаження лягає все ж таки на штучні бар'єри, такі як паркани та інші види огорож. Практика показує, що огорожі складної конфігурації здатні затримати зловмисника на достатньо тривалий час. На сьогодні нараховується значний арсенал таких засобів: від простих сітчастих до складних комбінованих огорож, які здійснюють певний вплив відлякування на порушника.

Особливі конструкції периметрів, проходів, віконних сплетінь, приміщень, сейфів, сховищ є обов'язковими з точки зору безпеки для будь-яких організацій та підприємств. Ці конструкції повинні протистояти будь-яким способам фізичного впливу з боку кримінальних елементів:

– механічним деформаціям, руйнуванню свердлінням, термічному та механічному різанню тощо;
– несанкціонованому доступу шляхом підробки ключів, відгадування коду й т. ін.

Одним із головних технічних засобів захисту проходів, приміщень, сейфів та сховищ є замки. Вони бувають простими (з ключами), кодовими (у тому числі з

часовою затримкою на відкривання) і з програмним пристроями, що відкривають двері та сейфи в певний час.

Важливим засобом фізичного захисту є планування об'єкта, його будівель та приміщень за зонами безпеки, які враховують міру важливості різних частин об'єкта з погляду нанесення збитків від різного виду загроз. Оптимальне розташування зон безпеки та розташування в них ефективних технічних засобів виявлення, відбиття та ліквідації наслідків протиправних дій є основою концепції інженерно-технічного захисту об'єкта.

Зони безпеки повинні розташовуватися на об'єкті послідовно, від огорожі навкруг території об'єкта до сховищ цінностей, створюючи ланцюг перешкод (рубежів), які доведеться долати зловмисникові. Від складності та надійності перепони на його шляху залежить проміжок часу, необхідного на подолання кожної зони, та ймовірність того, що розташовані в кожній зоні засоби виявлення (охоронні пости, охоронна сигналізація та охоронне телебачення) виявлять наявність порушника та подадуть сигнал тривоги.

Основу планування та обладнання зон безпеки об'єкта становлять принцип рівноміцності меж зон безпеки. Сумарна міцність зон безпеки буде оцінюватися найменшою з них.

Останніми роками велика увага надається створенню *систем фізичного захисту,* сполучених із системами сигналізації. Так, відома електронна система сигналізації для використання з дротовим загородженням. Система складається з електронних датчиків та мікропроцесора, який керує блоком обробки даних. Загородження довжиною до *100 м* може встановлюватися на відкритій місцевості або розташовуватися на стінах, горищах та на наявних огорожах.

Фізичні засоби є першою перешкодою (бар'єром) для зловмисника при реалізації ним заходових методів доступу.

Апаратні засоби захисту

До апаратних засобів захисту інформації відносяться найрізноманітніші за принципом дії, побудовою та можливостями технічні конструкції, які забезпечують припинення розголошення, захист від витоку та протидію несанкціонованому доступові до джерел конфіденційної інформації.

Апаратні засоби захисту інформації – це різноманітні технічні пристрої, системи та споруди, призначені для захисту інформації від розголошення, витоку і несанкціонованого доступу.

Для захисту центральних процесорів (ЦП) застосовується кодове резервування – створення додаткових бітів у форматах машинних команд (розрядів секретності) і резервних регістрів (у пристроях ЦП). Одночасно передбачаються два можливих режими роботи процесора, які відділяють допоміжні операції від операцій безпосереднього вирішення задач користувача. Для цього служить спеціальна програма переривань, яка реалізується апаратними засобами.

Одним із заходів апаратного захисту ПК та інформаційних мереж є обмеження доступу до оперативної пам'яті за допомогою встановлення меж або полів. Для цього створюються регістри контролю та регістри захисту даних. Застосовуються також додаткові біти парності – різновид методів кодового резервування.

Для позначення ступеню конфіденційності програм і даних, категорій користувачів використовуються біти, які називаються бітами конфіденційності (це