МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Київський університет імені Бориса Грінченка

**Гулак Г. М., Жильцов О. Б., Киричок Р. В.,
Коршун Н. В., Складанний П. М.**

ІНФОРМАЦІЙНА та КІБЕРНЕТИЧНА БЕЗПЕКА ПІДПРИЄМСТВА

Підручник

Львів
Видавець Марченко Т. В.
2024

УДК 004.056
І-74

Рекомендовано до друку Вченою радою
Київського університету імені Бориса Грінченка
(протокол №10 від 30.11.2023 р.)

Автори:

Гулак Г. М., Жильцов О. Б., Киричок Р. В., Коршун Н. В., Складанний П. М.

Рецензенти:

Смірнов О. А. – завідувач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету, доктор технічних наук, професор;

Опірський І. Р. – завідувач кафедри захисту інформації Національного університету «Львівська політехніка», доктор технічних наук, професор;

Ковальчук Л. В. – провідний науковий співробітник Інституту проблем моделювання в енергетиці Національної академії наук України, доктор технічних наук, професор.

Гулак Г. М., Жильцов О. Б., Киричок Р. В., Коршун Н. В., Складанний П. М.

І-74 **Інформаційна та кібернетична безпека підприємства :** підруч. / Г. М. Гулак, О. Б. Жильцов, Р. В. Киричок, Н. В. Коршун, П. М. Складанний – Львів : Видавець Марченко Т. В., 2024. – 370 с.

ISBN 978-617-7937-91-2

Широке використання в процесі інформатизації суспільства сучасних технологій автоматизованої обробки інформації та управління технологічними процесами створило не тільки об'єктивні передумови підвищення ефективності всіх видів діяльності особи, суспільства та держави, але і ряд проблем захисту інформації. Складність вирішення цих проблем обумовлена необхідністю створення систем захисту інформації в умовах обмежених фінансових, матеріальних, людських та часових ресурсів.

В цих умовах розуміння потенціалу різних методів та технологій захисту, їх взаємного зв'язку та взаємного доповнення, глибоке знання принципів та методів управління організаційно-технічними системами створюють надійне підґрунтя ефективного розв'язання згаданих проблем керівниками та виконавцями служб захисту інформації, практиками та дослідниками протягом всього життєвого циклу автоматизованих систем обробки даних.

Для студентів, що навчаються за спеціальністю 125 – Кібербезпека, аспірантів, науковців та практиків.

УДК 004.056

ISBN 978-617-7937-91-2

ЗМІСТ

РОЗДІЛ 9

РОЗДІЛ 10

РОЗДІЛ 11

РОЗДІЛ 12

РОЗДІЛ 17

РОЗДІЛ 18

РОЗДІЛ 19

Навчальне видання

ГУЛАК Геннадій Миколайович,
ЖИЛЬЦОВ Олексій Борисович,
КИРИЧОК Роман Васильович,
КОРШУН Наталія Володимирівна,
СКЛАДАННИЙ Павло Миколайович

ІНФОРМАЦІЙНА та КІБЕРНЕТИЧНА БЕЗПЕКА ПІДПРИЄМСТВА

Підручник

Підп. до друку 30.11.2023 р.
Формат 70x100/16. Папір друк. №2. Гарнітура PT Serif.
Умовн. друк. арк. 30,06. Наклад 300 прим.

Видавець Марченко Т. В.
м. Львів-53, 79053, Україна, тел.: +38 (050) 370-19-57
e-mail: magnol06@ukr.net
https://magnolia.lviv.ua

Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців, виготівників і розповсюджувачів видавничої
продукції: серія ДК № 6784 від 30.05.2019 року,
видане Державним комітетом інформаційної політики,
телебачення та радіомовлення України.

Надруковано у друкарні видавця Марченко Т. В.

РОЗДІЛ 2

Елементи загальної теорії захисту інформації

2.1. Характеристика інформації як об'єкта захисту

Інформація, що включає відомості про осіб, предмети, різноманітні факти, події або явища, а також процеси, незалежно від форми їхнього подання, як об'єкт захисту має низку особливостей, зокрема:

- інформація нематеріальна – мається на увазі те, що її параметри неможливо виміряти відомими фізичними методами й приладами, тобто вона не має маси та енергії;
- зберігається й передається за допомогою матеріальних носіїв, у ролі яких можуть виступати деякі фізичні процеси (коливання молекул, електричний струм, електромагнітні хвилі, хімічні сполуки тощо);
- будь-який матеріальний об'єкт може містити інформацію про себе або інші об'єкти;
- інформація має певну цінність, що, без сумніву, є найбільш важливою її властивістю з погляду захисту. При цьому цінність інформації визначається ступенем її корисності для власника.

Існує чимало підходів до формалізації оцінки цінності інформації, однак сьогодні в цьому процесі залишається значна частка суб'єктивізму.

Володіння дійсною (достовірною) інформацією дає її власникові певні переваги. *Дійсною,* або *достовірною,* вважається інформація, яка з достатньою для власника (користувача) точністю відображає об'єкти та процеси навколишнього світу в певних часових і просторових межах.

Недостовірна, перекручена, інформація, що свідомо спотворює дійсність, може заподіяти отримувачу або її розпоряднику значний матеріальний і моральний збиток. Зазначимо, що викривлена навмисно інформація має назву *дезінформація*.

Законом «Про інформацію» гарантується право власника інформації на її використання й захист від доступу до неї інших осіб (організацій).

Головним критерієм для ухвалення рішення про обмеження доступу до інформації та щодо способів її убезпечення є цінність цієї інформації.

Існує *два основних підходи щодо убезпечення інформації,* які реалізуються шляхом:

- захисту інформації від її витоку, руйнування/блокування в автоматизованих системах або інших фізичних середовищах, коли носієм інформації виступають фундаментальні явища природи: електричні, магнітні, електромагнітні, оптичні та хімічні процеси;
- охорони інформації. При цьому, на відміну від захисту інформації, охороні підлягає тільки документована інформація, тобто зафіксована на матеріальному носії з реквізитами, що дасть змогу її ідентифікувати.

Враховуючи права власника інформації обмежувати до неї доступ та за умовами її правового режиму, документована інформація з обмеженим доступом (ІзОД) поділяється на *конфіденційну* та *службову*, а також різного роду таємниці: адвокатську, банківську, державну, комерційну, лікарську, нотаріальну.

Загалом ступінь обмеження доступу – це адміністративний або законодавчий захід відповідно до міри відповідальності особи за витік або втрату конкретної ІзОД, що регламентована спеціальним документом, враховуючи державні, військові, стратегічні, економічні, комерційні, службові інтереси.

Відповідно до закону «Про державну таємницю», державну таємницю можуть містити відомості, що належать та являють цінність для держави. Таким даним може бути встановлено один із трьох можливих ступенів обмеження доступу – «таємно», «цілком таємно», «особливої важливості».

Конфіденційні відомості, що належать державі, – *службова інформація*. Переліки службової інформації затверджуються в кожному державному органі наказами відповідних посадових осіб.

Адвокатську, банківську, комерційну, лікарську, нотаріальну таємниці можуть містити відомості, що належать приватній особі, підприємству, установі, корпорації тощо.

Слід зазначити, що інформація має властивість адитивності, об'єднання (збільшення обсягу) різноманітної інформації підвищує загалом її цінність, сумарна сукупність проаналізованої та певним чином впорядкованої відкритої інформації може перевести її в категорію службової, узагальнені службові відомості в остаточному підсумку можуть виявитися секретними.

Цінність інформації є динамічною та постійно змінюється в часі. Як правило, з плином часу її цінність зменшується. Залежність цінності інформації від часу визначається за формулою:

$$C(t) = C_0 10^{-t/\tau}, \quad (2.1)$$

де C_0– початкова цінність інформації (у момент її виникнення або одержання); t – час від моменту виникнення інформації до моменту визначення її вартості; τ – час від моменту виникнення інформації до моменту її остаточного старіння.

Час τ у формулі (2.1), через який інформація стає застарілою, змінюється в дуже широкому діапазоні. Так, наприклад, з погляду диспетчерських служб в авіації дані про положення літаків у просторі застарівають за лічені секунди. Водночас інформація про закони природи залишається актуальною протягом багатьох тисячоліть.

Інформацію можна купувати та продавати. Тобто цілком правочинно розглядати інформацію як товар, що має певну ціну. Ціна як цінність інформації пов'язана з корисністю останньої для конкретних осіб, організацій або держав.

Інформація може бути цінною для її власника, але непотрібною для інших. У цьому разі вона не може бути товаром, а отже, і не має ціни.

Інформація може бути отримана шляхом:

- здійснення наукових досліджень;
- покупки;
- протиправного здобування.

Як і будь-який товар, інформація має собівартість, що визначається витратами на її одержання. Собівартість залежить від вибору шляхів отримання інформації й мінімізації витрат при здобутті необхідних відомостей вибраним шляхом. Інформація може одержуватися з метою отримання прибутку або переваг перед конкурентами, для цього вона:

- продається на ринку;
- впроваджується в виробництво для одержання нових технологій, товарів та послуг, що приносять прибуток;
- використовується в наукових дослідженнях з метою створення ноу-хау підприємства;
- застосовується під час вибору раціональних управлінських рішень.

Було зазначено, що обсяг інформації впливає на її цінність. Зауважимо, що оцінки кількості інформації в одиницях двійкового її подання в кілобайтах (1 Кб = 1000 байт), мегабайтах (1 Мб = 10^6 байт), гігабайтах

(1 Гб = 10^9 байт) і навіть в терабайтах (1 Тб = 10^{12} байт) не можуть показати реальну картину щодо кількості інформації на конкретному носії з погляду цінності останньої. Причина цього, зокрема, зумовлена наявністю в поданні інформації певної надлишковості, дублювання відомостей та наявності очевидних фактів.

Наприклад, надлишковість у письмових повідомленнях дає змогу скоротити довжину тексту на третину завдяки пропуску голосних літер практично без втрати змісту, як-от: «Інформаційне повідомлення доставлене» / «Нфрмцн пвдмлнн дствлн». Тобто коротке повідомлення має таку саму цінність, як і довге.

Дублювання інформації може бути в явному вигляді в разі передавання каналом зв'язку елементів графічних форм її подання, повторення одиниць вимірювання тощо, так і в неявному, що зумовлено логічними зв'язками між окремими елементами повідомлення, наявність яких дає змогу дійти правильних висновків.

Наприклад, у повідомленні «Швидкість вітру в районі аеропорту перевищує 40 м/с. Виліт усіх рейсів відмінений» друге речення для спеціаліста є зайвим. Так, у першому реченні фактично йдеться про потужний шторм у районі аеропорту. Тож друге для спеціаліста вже не містить інформації, оскільки для більшості цивільних літальних апаратів заборона на зліт настає у разі втричі меншої швидкості вітру з будь-яких напрямків.

Очевидний факт міститься, наприклад, у повідомленні «В січні температура повітря в районі Північного полюсу не зростає вище позначки 0°С». Воно є неінформативним для освіченої людини і не має цінності.

Таким чином, існує проблема складності об'єктивної оцінки кількості інформації.

Для обчислення кількості інформації використовують кілька різних за своєю суттю підходів.

І. *Ентропійний підхід* базується на математичних методах теорії інформації. У теорії інформації кількість останньої оцінюється мірою зменшення в одержувача невизначеності (ентропії) вибору або очікування подій після отримання інформації. Кількість інформації тим більша, чим нижча ймовірність настання події.

Цей метод широко застосовується при визначенні кількості інформації, що передається каналами зв'язку. При отриманні інформації здійснюється вибір між символами алфавіту в одержаному повідомленні.

Нехай повідомлення, прийняте каналом зв'язку, складається з N символів. Тоді кількість інформації I в ньому, не враховуючи зв'язків між

символами в повідомленні, може бути обчислена за формулою, що запропонована американським математиком Клодом Шенноном:

$$I = -N \sum_{i=1}^{n} P_i \cdot \log_2 P_i, \text{ (2.2)}$$

де P_i – імовірність появи в повідомленні символу з номером *i; n* – кількість різних символів в алфавіті мови.

Нехай, наприклад, для передачі повідомлень використовуються лише чотири символи *{ A, B, C, D}*, що трапляються з імовірністю:

$$P_A = 1/2, \quad P_B = 1/4, \quad P_C = 1/8, \quad P_D = 1/8,$$

що можна інтерпретувати таким чином: літери бувають у середньому – *A* в половині випадків, чверть випадків припадає на літеру *B*, ще чверть ділять порівну між собою літери *C* та *D*.

Тоді кількість інформації у повідомленні з 8 символів можна обчислити за формулою (2.2):

$$I = -8 \cdot \left(1/2 \cdot \log_2 1/2 + 1/4 \cdot \log_2 1/4 + 1/8 \cdot \log_2 1/8 + 1/8 \cdot \log_2 1/8 \right) = 4 + 4 + 3 + 3 = 14 \ (\textit{біт}).$$

Аналіз формули Шеннона доводить, що кількість інформації у двійковому поданні (у бітах або байтах) залежить від двох величин: кількості символів у повідомленні та частоти появи в останніх того чи іншого символу з алфавіту, що використовується. Цей підхід не відображає, наскільки корисна отримана інформація, але дає змогу порівняти відносну інформативність різних повідомлень та визначити витрати на їх передачу.

II. *Тезаурусний підхід* (або семантична теорія інформації) був запропонований математиком Ю. А. Шрейдером, що народився в Україні. Цей підхід заснований на розгляді інформації як знань. Згідно з ним, кількість інформації, що отримується людиною з повідомлення, можна оцінити ступенем зміни її знань.

У словниковій практиці тезаурусом прийнято називати одномовний асоціативний словник, в якому вказані різні смислові зв'язки між словами. Він, як і будь-який довідник, відображає відомості, накопичені до певного моменту часу деяким суб'єктом (приймачем). Зокрема, тезаурус характеризує здатність цього суб'єкта сприймати ті чи інші повідомлення.

Тезаурус, за Шрейдером, – це структуровані знання, представлені у вигляді понять і відносин між ними. Структура тезауруса ієрархічна (тобто має багаторівневу архітектуру). Поняття й відносини, групуючись, утворюють інші, більш складні.

Знання окремої людини, організації, держави утворюють властиві їм тезауруси. Тезауруси організаційних структур утворюються тезаурусами складових їхніх елементів.

Так, тезаурус організації утворюють насамперед тезауруси співробітників, а також інших носіїв інформації, таких як документи, устаткування, продукція тощо. Для передачі знань потрібно, щоб тезауруси передавального та приймаючого елемента перетиналися, по-іншому – мали спільні знання, інакше власники тезаурусів не зрозуміють одне одного.

Тезауруси фізичних і юридичних осіб є їхнім капіталом. Тому власники тезаурусів прагнуть зберегти й збільшити свій словник. Збільшення тезауруса здійснюється за рахунок навчання, покупки ліцензій, запрошення кваліфікованих співробітників і навіть розкрадання інформації.

У суспільстві спостерігаються дві тенденції: розвиток тезаурусів окремих елементів (людей, організованих структур) і вирівнювання тезаурусів елементів суспільства. Вирівнювання тезаурусів відбувається як у результаті цілеспрямованої діяльності (наприклад, навчання), так і стихійно. Стихійне вирівнювання відбувається за рахунок випадкової передачі знань, включаючи незаконну.

Цей підхід має значний потенціал для створення кібернетичних організмів – машин, здатних подібно людині самостійно формувати нові знання. Проте складність його реалізації для практичної оцінки кількості інформації та, відповідно, її цінності занадто велика.

III. *Практичний підхід*, незважаючи на наведені вище недоліки, все ж таки базується на понятті «обсяг інформації». При цьому кількість інформації може вимірюватися в кількості біт (байт), кількості сторінок тексту тощо. Проте цілком очевидно, що одна сторінка будь-якого формату може містити більше або менше інформації, принаймні з двох причин.

По-перше, різні люди можуть розмістити на сторінці різну кількість відомостей про один і той самий об'єкт, процес або явище матеріального світу. По-друге, різні люди можуть отримати з того самого тексту різну кількість корисної, зрозумілої для них інформації. Навіть та сама людина у різні роки життя одержує різну кількість інформації при читанні книги.

У результаті копіювання носія без зміни інформаційних параметрів кількість інформації не змінюється, а ціна загалом знижується. Таким прикладом може слугувати копіювання тексту з використанням якісних копіювальних пристроїв. Текст копії, за умови відсутності збоїв копіювального пристрою, міститиме таку саму інформацію, як і текст оригіналу. Але при копіюванні зображень вже ж складно уникнути спотворень, їхня кількість може бути тільки більшою або меншою.

У той же час, відповідно до законів ринку, чим більше товару з'являється, тим він дешевше. Це правило цілком слушне і відносно копій інформації. Дію цього закону можна простежити на прикладі піратського поширення програмних продуктів, відеопродукції тощо.

2.2. Інформація як об'єкт права власності

Особливості захисту інформації зумовлюються також різним статусом суб'єктів інформаційних відносин (особа, підприємство, суспільство, держава).

Різні суб'єкти інформаційних відносин щодо певної інформації можуть виступати як (можливо одночасно):

- джерела (постачальники) інформації;
- користувачі (споживачі) інформації;
- власники (розпорядники) інформації;
- фізичні й юридичні особи, про яких збирається інформація;
- власники систем збору й обробки інформації та учасники процесів обробки й передачі інформації.

Виникає складна система взаємостосунків між цими суб'єктами права власності.

Інформація як об'єкт права власності може бути скопійована за допомогою матеріального носія. Як наслідок, така інформація може легко переміщуватися до іншого суб'єкта права власності, без очевидного (помітного) порушення права власності на інформацію.

Переміщення матеріального об'єкта до іншого суб'єкта права власності неминуче і, як правило, спричиняє втрату цього об'єкта первинним суб'єктом права власності, тобто відбувається очевидне порушення права власності останнього.

Право власності включає такі повноваження власника, що становлять зміст (елементи) права власності:

- право розпорядження;
- право володіння;
- право користування.

Однак для розгляду інформації як предмета захисту необхідно розглянути особливості інформації як об'єкта права власності.

Суб'єкт права власності на інформацію може передати частину своїх прав (розпоряджень), не втрачаючи їх, іншим суб'єктам.

Для інформації право розпорядження передбачає виключне право визначати, кому вона може бути надана; право володіння – мати цю

інформацію в незмінному вигляді; право користування – право використовувати цю інформацію у своїх інтересах.

Отже, окрім суб'єкта права власності на інформацію до неї можуть мати доступ й інші суб'єкти права власності – як законний, тобто санкціонований, так і незаконний, несанкціонований. Таким чином, мета захисту інформації полягає ще й у захисті прав власності на неї.

У рамках підручника передбачається, що інформація використовується, зберігається, передається й обробляється в різних комп'ютерних системах. Водночас під *комп'ютерною системою (КС)* слід розуміти сукупність апаратного та програмного забезпечення (технічної та програмної платформ) та необхідної документації до неї.

Матеріальною основою існування інформації в КС, як правило, є електронні й електронно-механічні пристрої (підсистеми), а також машинні носії. Як машинні носії інформації можуть використовуватися папір, магнітні та оптичні носії, електронні схеми. Програмні засоби, що входять до складу КС, самі по собі є інформаційними ресурсами.

Таким чином, необхідно захищати пристрої й підсистеми, а також машинні носії інформації. Тому під поняттям *об'єкт захисту інформації* слід розуміти сукупність усіх носіїв інформації, що являє собою комплекс фізичних, апаратних, програмних і документальних засобів.

У різних інформаційних системах користувачі інформаційних систем є обслуговуючим персоналом і можуть бути її джерелами й носіями. Тому поняття об'єкта захисту трактується в більш широкому сенсі. Під об'єктом захисту розуміють не тільки інформаційні ресурси, апаратні й програмні засоби, персонал, що їх обслуговує, і користувачів, але й приміщення, будинки та територію навколо них.

2.3. Поняття, сутність, цілі захисту інформації

Як вже зазначалося в першому розділі, поняття «захист інформації» є невід'ємною складовою інформаційної безпеки.

Існує кілька тлумачень захисту інформації, зумовлених деякою неузгодженістю окремих нормативно-правових актів. Для розуміння процесів, методів і засобів захисту під захистом інформації у вузькому значенні розумітимемо сукупність дій та заходів, спрямованих на забезпечення безпеки інформації в контексті забезпечення конфіденційності, доступності й цілісності під час її збору, передачі, обробки й зберігання; у ширшому – комплекс організаційних, правових і технічних заходів щодо запобігання загрозам безпеці інформації й мінімізації негативних наслідків їх реалізації.

Сутність захисту інформації полягає у виявленні, усуненні або нейтралізації джерел негативних впливів, причин і умов впливу на інформацію. Ці джерела становлять загрозу безпеці інформації. Мета й методи захисту інформації відображають її сутність.

Загальними *ознаками захисту інформації* є такі:

- вимоги до захисту інформації та порядок її захисту визначає власник інформації (держава, підприємство, громадянин);
- безпосередньо захист інформації в ІКС на основі договору із власником інформації організовує та проводить власник системи (тимчасовий розпорядник інформації) або уповноважені ним на те особи (юридичні або фізичні);
- захистом інформації її власник охороняє свої права на володіння й розпорядження інформацією, прагне захистити її від незаконного заволодіння й використання на шкоду його інтересам;
- захист інформації здійснюється шляхом проведення комплексу заходів щодо обмеження доступу до інформації, яка захищається, і створення умов, які виключають або суттєво ускладнюють несанкціонований, нелегальний доступ до інформації, що захищається, та її носіїв.

Водночас, захист інформації забезпечується за такими напрямами:

- ідентифікація загроз, що реалізується шляхом систематичного аналізу й контролю можливості появи реальних або потенційних загроз;
- виявлення загроз, суттю чого є визначення реальних загроз і конкретних протиправних дій;
- попередження загроз шляхом впровадження превентивних заходів для забезпечення інформаційної безпеки, спрямованих на уникнення умов їх виникнення;
- нейтралізація загроз завдяки застосуванню коригуючих заходів та засобів;
- локалізація загроз передбачає виключення можливості поширення загроз за межі певної припустимої області;
- ліквідація загрози або конкретних протиправних дій ;
- ліквідація наслідків загроз і протиправних дій та відновлення попереднього стану.

Ідентифікація загроз передбачає проведення заходів щодо збору, накопичення й аналітичної обробки відомостей про можливу підготовку протиправних дій з боку кримінальних структур або конкурентів на ринку виробництва й збуту товарів і продукції.

Виявлення загроз – це дії з визначення конкретних загроз і їхніх джерел, що заподіюють той або інший вид збитку інформаційним ресурсам, виявлення фактів розголошення інформації з обмеженим доступом (у т. ч. випадків несанкціонованого доступу до джерел комерційних секретів), порушення цілісності або доступності інформації.

Попередження можливих загроз і протиправних дій може бути забезпечене різними заходами й засобами, починаючи від створення клімату глибоко усвідомленого ставлення співробітників до проблеми безпеки й захисту інформації, до створення багаторубіжної системи захисту фізичними, апаратними або програмними засобами технічного та криптографічного захисту інформації.

Попередження загроз можливе й шляхом одержання інформації про протиправні акти, що готуються, заплановані розкрадання, підготовчі дії та інші елементи злочинних діянь.

Припинення або локалізація загроз – це дії, спрямовані на усунення діючої загрози й конкретних протиправних дій.

Ліквідація наслідків має на меті відновлення стану, що передував настанню загрози. Наприклад, відновлення інформаційного ресурсу завдяки раніше зробленим його копіям на резервних носіях інформації.

Усі ці способи мають на меті захистити інформаційні ресурси від протиправних зазіхань та:

- запобігти витоку інформації з обмеженим доступом, виключити можливість несанкціонованого доступу до носіїв конфіденційної інформації;
- забезпечити цілісність та доступність інформації;
- засвідчити авторство визначеної інформації.

З огляду на викладене можемо дійти висновку про те, що захист інформації є діяльністю із застосуванням певної сукупності методів, засобів і заходів, які спрямовані на забезпечення інформаційної безпеки держави, суспільства й особистості у всіх областях їхніх життєво важливих інтересів.

Кожен вид інформації, що захищається, має свої особливості в галузі регламентації, організації й здійснення цього захисту.

Інформація, що захищається, може включати відомості, що становлять державну, комерційну, службову й інші охоронювані законом таємниці, як і будь-який інший вид інформації, вона необхідна для управлінської, науково-виробничої й іншої діяльності.

Таким чином, захист інформації – це комплекс заходів, здійснених власником інформації щодо забезпечення своїх прав на володіння й розпорядження інформацією, створення умов, що обмежують її поширення,