УДК: 073
DOI: 10.36919/2312-7812.2.2023.119

Ю.М. Погребець

СТАН ВИКОРИСТАННЯ СЛУЖБОВОЇ ІНФОРМАЦІЇ ОРГАНАМИ ДЕРЖАВНОЇ ВЛАДИ УКРАЇНИ ТА ЇЇ ЗАХИСТ

В даній статті розглянуто стан використання службової інформації органами державної влади України, її поширення та збереження від несанкціонованого використання.

У статті висвітлено правову природу та джерела правового регулювання правового режиму службової інформації в Україні та стан її використання органами державної влади в умовах адаптації українського законодавства до законодавства Європейського Союзу.

This article examines the state of use of official information by the state authorities of Ukraine, its dissemination and preservation from unauthorized use.

The article examines the legal nature and sources of legal regulation of the legal regime of official information in Ukraine and the state of its use by state authorities in the context of the adaptation of Ukrainian legislation to the legislation of the European Union.

Ключові слова: службова інформація, органи державної влади, поширення інформаціїї, запиту на інформацію.

Keywords: official information, state authorities, dissemination of information, request for information.

Постановка проблеми. В умовах російсько-української війни захист національного інформаційного простору від негативних інформаційно-психологічних впливів, операцій і воєн, забезпечення інформаційної безпеки та інформаційного суверенітету набувають особливого значення і стають чинниками збереження національної ідентичності України та її функціонування як суверенної та незалежної держави.

Стан захищеності державного інформаційного простору є одним з показників ефективності роботи держави щодо захисту власних інформаційних ресурсів від протиправного втручання.

Інформаційна безпека має велике значення для забезпечення життєво важливих інтересів держави. Створення розвиненого і захищеного довкілля є неодмінною умовою розвитку суспільства і держави, яка повинна ґрунтуватися на ефективних адміністративних і правових заходах.

Останнім часом в Україні відбулися якісні зміни в процесах державного управління на всіх рівнях, що зумовлено інтенсивним впровадженням новітніх інформаційних технологій.

Швидке вдосконалення інформатизації та її проникнення в усі сфери життєво важливих інтересів, крім безперечних переваг, привели до виникнення ряду стратегічних проблем.

Зростає ризик несанкціонованого втручання в роботу комп›ютерних, інформаційних і телекомунікаційних систем. У цьому контексті заходи щодо захисту службової інформації мають особливе значення.

Аналіз останніх досліджень і публікацій. Теоретичну основу дослідження склали наукові здобутки таких провідних вчених в галузі права, як В. Авер'янова, В. Баскакова, В. Бєлєвцевої, В. Брижка, П. Гарасима, К. Джонсона, Є. Збінського, В. Ліпкана, Л. Колобова, І. Колеснікової, Р. Кохейна, О. Курмана, Дж. Ная, О. Семенюка, О. Смоляк, О. Огданської, В. Пилипчука, В. Тарана, В. Щербаченко та ін.

Мета статті полягає у розкриття теоретичного змісту службової інформації та порядку і проблемам її захисту.

Відповідно до вище вказаної мети дослідження статті слід вирішити наступні *завдання:*

- розкрити поняття службової інформації;
- проаналізувати стан використання службової інформації органами державної влади України;
- встановити способи та проблеми захисту службової інформації.

Виклад основного матеріалу дослідження. Службовою інформацією є інформація, що міститься в документах суб'єктів владних повноважень, які становлять внутрішньовідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню або прийняттю рішень, а також інформація зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці [2, с. 33].

Система обміну даними при передачі службової інформації повинна забезпечувати не тільки передачу інформації, але і її захист від крадіжки або зміни, а також можливість її швидкого відновлення.

Переважна більшість випадків втрати інформації відбувається через помилки користувача. Це досить поширена ситуація в організаціях з необізнаними користувачами, які не дотримуються базових заходів кібербезпеки.

Основне правило запобігання помилкам користувачів полягає в наступному: «Не натискайте, якщо ви не знаєте кінцевий результат [4, с. 86].

Також існують проблеми з втратою даних через недбале ставлення до технічного стану обладнання, що використовується для передачі інформації. Тому регулярне технічне обслуговування засобів зв›язку та автоматизованих систем управління створює умови для їх безперебійної та справної роботи [3, с. 106].

Сьогодні ми повинні постійно дотримуватися всіх правил безпеки, щоб звести до мінімуму можливість витоку інформації, а не жити в ілюзії, що всі захищені і зі мною не може трапитися нічого подібного. Навіть найкращий захист не дає стовідсоткової гарантії безпеки.

Зловмисники постійно маскують так званих черв›яків в інших програмах, які ми несвідомо встановлюємо на наші комп›ютери, що призводить до загрози цілісності інформації - її крадіжці, знищенню або зміні.

Цей метод є одним з найпопулярніших, оскільки він використовує не тільки вразливості, але і психологічні особливості користувача, його бажання безкоштовно завантажувати мультимедійні файли (музику, відео, програмне забезпечення) і проста цікавість.

Причини витоків інформації також зазвичай пов›язані з недосконалістю політики зберігання інформації, а також з її порушеннями, включаючи відхилення від правил поводження зі штампованими документами, технічними засобами, зразками продукції та носіями, що містять офіційну інформацію.

До таких факторів і порушень відносяться [1]:

- недостатнє знання користувачами основ захисту інформації та нерозуміння необхідності їх ретельного дотримання;

- використання несанкціонованих або несертифікованих технічних засобів для обробки секретної інформації, оскільки в кращому випадку це обладнання може бути неповним, а в гіршому - містити закладки фізичного або програмного рівня;

- слабкий контроль за дотриманням правил захисту інформації з боку штатних або позаштатних служб захисту інформації та кібербезпеки, а також інженерно-технічних підрозділів, які не можуть забезпечити працездатність обладнання і відсутність належного контролю за дотриманням правил захисту інформації з боку штатних або позаштатних служб захисту інформації та кібербезпеки, а також технічних і інженерних підрозділів, які некоректний моніторинг пристроїв або ліній [7, с. 113].

Всі ці фактори завдають набагато більшої шкоди, ніж ціла група нападників. Нарешті, безвідповідальні люди своїми діями можуть становити небезпеку для витоку інформації, функціонування системи аж до припинення її роботи.

Захист інформації - одна з вічних проблем. Протягом всієї історії людства шляхи розв›язання цієї проблеми визначалися рівнем розвитку технологій. У сучасному інформаційному суспільстві технології відіграють роль активатора цієї проблемно-комп›ютерна злочинність стала характерною рисою сучасності. Комп›ютерні злочини — це злочини, пов›язані з втручанням в роботу комп›ютера, і злочини, пов›язані з використанням комп›ютерів в якості необхідних технічних засобів.

Серед причин комп›ютерних злочинів і пов›язаних з ними розкрадань інформації можна виділити наступні:

- швидкий перехід від паперових технологій зберігання і передачі інформації до електронних із-за одночасної затримки технологій захисту інформації, записаних на машинних носіях;

- широке використання локальних комп'ютерних мереж, створення глобальних мереж і розширення доступу до інформаційних ресурсів;

- постійне ускладнення програмних засобів, що приводить до зниження їх надійності та збільшення числа вразливостей [8, с. 92].

Сьогодні ніхто не може дати точну цифру загального збитку від комп›ютерних злочинів, але експерти сходяться на думці, що відповідні суми вимірюються мільярдами доларів. Серед основних моментів слід виділити наступні:

- збитки, викликані ситуацією, коли співробітники організації не можуть виконувати свої обов'язки через непрацездатну систему (мережу; вартість вкрадених і скомпрометованих даних;

- вартість відновлення системи, перевірки її цілісності та усунення вразливостей.

Також варто враховувати моральні та психологічні наслідки для користувачів, співробітників та власників інтелектуальної власності та інформації. Порушення безпеки так званих «критичних застосувань у державному та військовому управлінні, ядерній енергетиці, медицині, ракетно-космічній промисловості та фінансах може мати

серйозні наслідки для навколишнього середовища, економіки та безпеки держави, здоров›я та навіть життя людей. 2 економічні та правові питання, приватні та комерційні секрети, національна безпека - все це вимагає захисту інформації та інтелектуальної власності.

Захист інформації - це сукупність організаційних і технічних заходів і правових норм, спрямованих на запобігання шкоди інтересам власника інформації та осіб, які використовують інформацію. Пов›язані терміни «інформаційна безпека» та «інформаційно-технічна безпека» також використовуються в літературі. Забезпечення безпеки інформаційних технологічно-складне завдання, яке включає законодавче регулювання використання інформаційних технологій, вдосконалення технологій для їх розробки, розробку системи сертифікації та забезпечення належних організаційно-технічних умов експлуатації.

Розв›язання цієї проблеми вимагає значних витрат, тому основне завдання - співвіднести необхідний рівень безпеки та витрати на технічне обслуговування. Для цього необхідно визначити потенційні загрози, ймовірність їх виникнення і можливі наслідки, вибрати відповідні засоби та створити надійну систему захисту.

Основні принципи інформаційної безпеки полягають у забезпеченні цілісності інформації, її конфіденційності й водночас доступності для всіх авторизованих користувачів [9, с. 18].

З цієї точки зору основними випадками порушень інформаційної безпеки можна назвати наступні:

- несанкціонований доступ — доступ до інформації, здійснюваний з порушенням правил контролю доступу;

- витоку інформації є результатом дій порушника, в результаті яких інформація стає відомою (доступною) особам, які не мають права на доступ до неї;

- несанкціонований доступ-доступ до інформації, що здійснюється з порушенням правил контролю доступу;

- витік інформації є результатом дій порушника, в результаті яких інформація стає відомою (доступною) особам, які не мають права на доступ до неї;

- несанкціонований доступ-доступ до інформації, що здійснюється з порушенням правил контролю доступу;

- витік інформації є результатом дій порушника, в результаті яких інформація стає відомою.

Витік інформації - це дія, в результаті якого інформація в перестає існувати для фізичних або юридичних осіб, які мають на неї повне або обмежене право власності;

фальсифікація інформації - умисні дії, що призводять до спотворення інформації, яка повинна оброблятися або зберігатися в системі;

блокування інформації; витік інформації - це дія, в результаті якого інформація в перестає існувати для фізичних або юридичних осіб, які мають на неї повне або обмежене право власності;

фальсифікація інформації - умисні дії, що призводять до інформації - дії, що призводять до припинення доступу до інформації; є несправність - дії або обставини, що призводять до спотворення процесу обробки інформації [2, с.42].

Причини виникнення цих випадків:

- відмова обладнання (відмова кабельної системи, відключення живлення, сервер, робочі станції, мережеві карти, дискові системи);

- неправильна робота програмного забезпечення (втрата або зміна даних в разі збою програмного забезпечення, втрата даних в результаті зараження системи комп'ютерними вірусами);

- умисні дії сторонніх осіб (несанкціоноване копіювання);

- неправильна робота програмного забезпечення (втрата або зміна даних в разі збою програмного забезпечення, втрата даних в результаті зараження системи комп'ютерними вірусами);

- умисні дії неуповноважених осіб (несанкціоноване копіювання);

- неправильна робота програмного забезпечення (втрата або зміна, втрата даних в результаті зараження системи комп'ютерними вірусами);

- знищення, фальсифікація або блокування інформації, порушення, створення витоків інформації);

- помилки обслуговуючого персоналу і користувачів (випадкове знищення або зміна даних; неправильне використання програмного та апаратного забезпечення, що приводить до порушення нормальної роботи системи, появи вразливостей, знищення чи зміни даних, ущемлення інтересів інших законних користувачів;

- неефективно організована система захисту; неправильне зберігання і зберігання даних, що не відповідають вимогам безпеки; неправильне зберігання і зберігання даних, що не відповідають вимогам безпеки тощо);

- неправильне використання програмного та апаратного забезпечення, що приводить до порушення нормальної роботи системи, виникнення вразливостей, знищення чи зміни даних, ущемлення інтересів інших законних користувачів і т. д.; система захисту організована неефективно; неправильне зберігання архівних даних тощо);

- умисні дії обслуговуючого персоналу і користувачів (все, що було сказано в двох попередніх абзацах, а також розкриття конфіденційної інформації стороннім особам)

Майте на увазі, що дії, які не призводять безпосередньо до втрати або витоку інформації, але впливають на роботу системи, також можуть розглядатися як порушення безпеки.

Недосконалість, а по ряду питань відсутність нормативно-правової бази значно ускладнює розгортання діяльності в області технічного захисту інформації (ТЗІ). У зв›язку з тим, що ТЗІ є підсистемою, яка є частиною загальної системи інформаційної безпеки, ми вважаємо, що правові проблеми ТЗІ не можуть бути вирішені без розв›язання правових проблем загального рівня. В результаті аналізу правової бази України у сфері інформаційних відносин можна виділити наступні основні правові проблеми загальної системи інформаційної безпеки.

По-перше, відсутнє чітке визначення прав та обов›язків учасників інформаційних відносин, у тому числі з питань обмеженого доступу.

По-друге, оскільки інформація може відображатися в / на різних носіях і створюватися різними способами, не існує достатньо чіткого регулювання того, як виникає право власності на інформацію.

Порядок встановлення права власності на інформацію, отриману, зокрема, за допомогою технічних засобів, у тому числі комп›ютерних технологій, законодавчо чітко не визначений.

По-третє, відсутність чіткого визначення правових норм, що визначають право людини на володіння інформацією про себе [6, с. 56].

Обробка даних в таких базах даних все частіше здійснюється з використанням комп›ютерних технологій з використанням хмарних технологій. Отже, існує потенційна небезпека неконтрольованого або навмисного поширення інформації з цих баз даних про конкретну людину без її відома, в тому числі по технічних каналах.

По-четверте, нам необхідно досить чітке визначення характеру, типу та обсягу такої інформації з обмеженим доступом як конфіденційної (для службового користування, конфіденційної комерційної, професійної інформації: медичної, юридичної, банківської таємниці); встановлення порядку віднесення інформації до такої інформації та зняття обмежень; визначення прав, обов›язків і відповідальності суб›єктів інформаційних відносин при визначенні категорії такої інформації, її використання та захисту.

Щоб бути абсолютно точним, слід зазначити, що, своєю чергою, правові проблеми загальної системи інформаційної безпеки не можуть бути вирішені без розв›язання правових проблем всього комплексу інформаційних відносин [7, с. 92].

В цілому, люди становлять найбільшу загрозу безпеці інформації, тому саме їх навмисні або випадкові дії необхідно передбачити при організації системи захисту.

Співробітники служб комп›ютерної безпеки ділять всіх порушників на чотири групи щодо жертви: сторонні, які не знають компанію; сторонні, які знають компанію і колишніх співробітників; співробітники, які не є програмістами; співробітники-програмісти. Межа між програмістами та звичайними користувачами з точки зору небезпеки нещодавно була стерта.

Останні складають більшість співробітників, зазвичай мають базову комп›ютерну підготовку і можуть використовувати спеціальне програмне забезпечення, яке має дружній інтерфейс і є на піратських компакт-дисках, в спеціальних розділах BBS і на сайтах Internet і FidoNet. На думку експертів, тільки чверть співробітників досить лояльні, чверть вороже ставляться до компанії і не мають моральних обмежень, лояльність інших залежить від обставин.

Отже, однією з основних причин порушення інформаційної безпеки є відсутність попиту творчого потенціалу в поєднанні з недостатньою обізнаністю про всі наслідки протиправних дій.

Цей фактор існує незалежно від національності або сфери професійної діяльності. Звичайно, жодна з особистих проблем не може стати причиною для незаконної діяльності, але сьогодні суспільство тільки починає виробляти належне ставлення до комп›ютерних злочинців [4, с.-9].

Поширюється думка, що легше запобігти комп›ютерному злочину, ніж розслідувати його пізніше. Однак це не розв›язувати проблему повністю, оскільки, крім бажання розважитися та самоствердитися, є також недбалість, холодний комерційний розрахунок, садизм та хвороблива уява. Тому комп›ютерні злочини залишаються об›єктом уваги фахівців.

Висновок. В статті розкрито поняття службової інформації, проаналізовано стан використання службової інформації органами державної влади України, встановлено способи та проблеми захисту службової інформації

Сьогодні службова інформація потребує неабиякого захисту. Адже, вищезазначені загрози дуже актуальні на цей момент, оскільки ще з початку 2014 року Російська Федерація активно розробляє і вдосконалює методи та засоби збору інформації, злому комп›ютерних систем і тому подібного.

Сьогодні навіть робляться спроби злому систем, які використовуються в зоні проведення антитерористичної операції, і це не просто грошові втрати, це людські життя, це наші солдати, захисники, батьки, брати та сестри.

Вони виконують бойові завдання, захищають нас, щоб ми могли спокійно спати ночами.

Все це є ще одним підтвердженням того, що захист інформації та кібербезпека - це не гра, а реальне людське життя.

Тому кожен державний службовець на своєму робочому місці, де обробляється інформація, повинен пам›ятати й дотримуватися правил і заходів кібернетичної безпеки.

1. *Литвинюк А. А.* Основи інформаційної безпеки. Комплексна система захисту інформації: структура, встановлення та підтримка функціонування. http://www.cvk.gov.ua /visnyk/pdf/2008_4/visnik_st_08.pdf. (дата звернення: 30.11.2022); 2. *Логінова Н. І.* Правовий захист інформації: навч. посібн. / Н. І. Логінова, Р. Р. Дробожур. Одеса: Фенікс, 2015. - 264 с.; 3. *Манжай О. В., Манжай І. А.* Правові засади захисту інформації: підручник. Харків: Панов, 2020. - 162 с.; 4. *Марущак А. І.* Питання ефективності діяльності державних органів у сфері захисту інформаційного простору України. Інформація і право. 2017. № 4. С. 86-92; 5. Методологія захисту інформації. Аспекти кібербезпеки: підручник / Г. М. Гулак К.: Видавництво НА СБ України, 2020. - 256 с.; 6. Нацполіція не підтвердила інформацію щодо витоку даних українців через мобільний застосунок «Дія». URL: https://diia.gov.ua/news/nacpoliciya-nepidtverdila-informaciyushchodo-vitoku-danih-ukrayinciv-cherez-mobilnij-zastosunok-diya.(дата звернення: 20.11.2022); 7. *Носов В. В., Манжай О. В.* Окремі аспекти протидії інформаційній війні в Україні. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2015. № 1(29). - С. 26-29; 8. *Носов В. В., Манжай І. А.* Організаційно-практичні аспекти побудови комплексної системи захисту інформації для системи з інформацією, що публікується в глобальній мережі. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2019. № 2(34). С. 56-68; 9. Організаційно-правові основи захисту службової інформації: навч. посіб. / І. П. Касперський, С. О. Князєв, О. І. Матяш та ін. К.: Нац. акад. СБУ, 2017. -120 с.; 10. Організація захисту інформації з обмеженим доступом: навч. посіб. / А. М. Гуз, І. П. Касперський, С. О. Князєв та ін. К.: Нац. акад., СБУ, 2018.- 252 с.; 11. Організація захисту інформації з обмеженим доступом: підручник / А. М. Гуз, О. Д. Довгань, А. І. Марущак та ін..; за заг. ред. Є. Д. Скулиша. К.: Наук.-вид. відділ НА СБ України, 2011.- 376 с.; 12. Організація охорони державної таємниці в Україні: навчальний посібник / А. М. Супруненко, І. І. Башта, А. М. Лисеюк, К. С. Свіріна; Університет державної фіскальної служби України. Ірпінь: УДФСУ, 2020.-370 с.;

1. *Lytvynyuk A. A.* Fundamentals of information security. Comprehensive system of information protection: structure, installation and maintenance of functioning. http://www.cvk.gov.ua/visnyk/pdf/2008_4/visnik_st_08.pdf. (application date: 11/30/2022).; 2. *Loginova N. I.* Legal protection of information: training. manual / N.I. Loginova, R.R. Drobozhur. - Odesa: Phoenix, 2015. - 264 p.; 3. *Manzhai O. V., Manzhai I. A.* Legal principles of information protection: textbook. Kharkiv: Panov, 2020. - 162 p.; 4. *A. I. Marushchak.* The question of the effectiveness of the activities of state bodies in the sphere of protection of the information space of Ukraine. Information and law.

2017. No. 4. P. 86-92; 5. Information protection methodology. Aspects of cyber security: a textbook / G. M. Gulak K.: NA SB Publishing House of Ukraine, 2020. - 256 p.; 6. The National Police did not confirm the information regarding the leak of data of Ukrainians through the Diya mobile application. URL: https://diia.gov.ua/news/nacpoliciya-ne-pidtverdila-informaciyushchodo-vitoku-danih-ukrayinciv-cherez-mobilnij-zastosunok-diya. (application date: 11/20/2022); 7. *Nosov V.V., Manzhai O.V.* Separate aspects of countermeasures against information warfare in Ukraine. Legal, normative and metrological support of the information protection system in Ukraine. 2015. No. 1(29). P. 26-29.; 8. *Nosov V.V., Manzhai I.A.* Organizational and practical aspects of building a complex information protection system for a system with information published on the global network. Legal, normative and metrological support of the information protection system in Ukraine. 2019. No. 2(34). P. 56-68; 9. Organizational and legal basis of protection of official information: training. manual / I. P. Kaspersky, S. O. Knyazev, O. I. Matyash and others. K.: Nat. Acad. SBU, 2017. -120 p.; 10. Organization of protection of information with limited access: training. manual / A. M. Huz, I. P. Kaspersky, S. O. Knyazev and others. K.: Nat. Acad., SBU, 2018. - 252 p.; 11. Organization of protection of information with limited access: textbook / A. M. Huz, O. D. Dovgan, A. I. Marushchak, etc.; in general ed. E. D. Skulisha. K.: Scientific ed. department of NA SB of Ukraine, 2011.- 376 p.; 12. Organization of protection of state secrets in Ukraine: study guide / A. M. Suprunenko, I. I. Bashta, A. M. Lyseyuk, K. S. Svirina; State Fiscal Service University of Ukraine. Irpin: UDFSU, 2020.-370 p.