© Horlichenko S. Peculiarities of the formation of technical channels of information leakage from modern x-rays // Ukrainian Scientific Journal of Information Security, 2023, vol. 29, issue 2, pp. 80-87. ©

ЗАХИСТ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ОБЛАДНАННЯ / SOFTWARE & HARDWARE ARCHITECTURE SECURITY

DOI: 10.18372/2225-5036.29.17872

ОСОБЛИВОСТІ ФОРМУВАННЯ ТЕХНІЧНИХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ ВІД СУЧАСНИХ ІКС

Сергій Горліченко

Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський Політехнічний Інститут імені Ігоря Сікорського"

ГОРЛІЧЕНКО Сергій Олександрович
Рік та місце народження: 1989 рік, м. Херсон, Україна.
Освіта: Військовий інститут телекомунікацій та інформатизації Національного технічного університету України Київський Політехнічний Інститут, 2011 рік.
Посада: науковий співробітник з 2019 року.
Наукові інтереси: інформаційна безпека.
Публікації: понад 15 друкованих публікацій, серед яких наукові статті, тези та матеріали доповідей на конференціях.
E-mail: serhii.horlichenko@gmail.com.
Orcid ID: 0000-0002-8999-7526.

***Анотація**. Інформаційно-комунікаційні системи постійно розвиваються і вдосконалюються, впроваджуючи нові технології і можливості. Однак, разом з стрімким розвитком з'являється також і більша загроза безпеці інформації. Тому важливо вдосконалювати методи та алгоритми технічного захисту ІКС для забезпечення їх захищеності та безпеки. Було проведено аналіз різних підходів до визначення сутності терміну "витоки інформації", а також проведена систематизація інформації щодо класифікації технічних каналів, через які відбувається витік інформації. Вивчено сутність процесу формування технічних каналів витоку інформації, висвітлено різноманітні методи захисту інформації від таких витоків. Також було проаналізовано міжнародне та внутрішнє законодавство, яке регулює сферу захисту інформації, зокрема в Україні. Акцентовано увагу на важливості забезпечення безпеки інформації під час дії військового стану в Україні. В контексті сучасних викликів та загроз, пов'язаних з кібербезпекою. наголошено на необхідності зміцнення заходів захисту інформації, щоб забезпечити належний рівень захисту в умовах воєнного стану та потенційних загроз. Запропоновано подальший розгляд завдання щодо обґрунтування захищеності джерел конфіденційної інформації від витоку технічними каналами для всіх видів її аналого-цифрового перетворення, що реалізують сучасні ІКС, на основі заданих гранично допустимих ризиків інформаційної безпеки.*

***Ключові слова**: кібербезпека, інформаційна безпека, технічний захист інформації, виток інформації, технічний канал витоку, електромагнітні випромінювання, інформаційно-комунікаційні системи.*

Постановка проблеми

З кожним днем роль комп'ютерів зростає все більше і більше. Найчастіше ми використовуємо комп'ютери для передачі, обміну або зберігання особистої інформації. У зв'язку з цим важливим моментом при роботі з інформацією на комп'ютерах є знання і дослідження можливих каналів витоку інформації.

Витоки інформації – неправомірна передача конфіденційних відомостей (матеріалів, важливих для різних компаній або держави, персональних даних громадян), яка може бути умисною або випадковою. Будь-які відомості, що знаходяться в комп'ютері, мають свою важливість, тому викрадення особистих даних може завдати значної економічної або репутаційної шкоди власнику інформації.

Маючи доступ до логінів і паролів, а також до банківських карток і рахунків, зловмисники можуть вкрасти гроші громадян, промислові секрети і таємниці підприємств. Інформація витікає в результаті безконтрольного поширення секретів за межі кабінету, будівлі, підприємства.

Втрата цінних відомостей може статися при неправильному використанні норм і правил політики безпеки. Недотримання правил захисту і зберігання

даних приводить до їх витоку і поширення в мережі Інтернет [2].

Дія сучасних засобів комунікацій, які в даний час забезпечують функціонування кіберпростору і головним чином є електронними, супроводжується комплексом побічних ефектів, що мають потенціал створити технічні канали витоку інформації. Такі технічні канали витоку інформації можуть стати причиною, що інформаційні сигнали можуть вийти за межі електронних систем в яких вони циркулюють, та це може призвести до порушення конфіденційності інформації [16, 20, 21].

Аналіз останніх досліджень і публікацій

Однією з найважливіших стратегічних спрямованостей, включених до діючої наразі національної безпекової політики в Україні, є підвищення потужностей національної системи кібербезпеки та ефективної протидії викликам кібернетичної небезпеки у сучасному контексті забезпечення безпеки. Ці заходи націлені на досягнення повноправного членства України в Європейському Союзі та НАТО і включають в себе впровадження міжнародних стандартів і застосування відповідних підходів з орієнтацією на ризики, спрямовані на забезпечення безпеки інформації на державному рівні [16-20].

Питання аналізу технічних каналів витоку інформації висвітлені в роботах таких вчених, як: Opirsky I. R. [15], Полотай О. І. [7], Воронов В. Р. [1], Попович Н. І. [9], Іванченко С. О. [20], Kuhn G. [21].

Разом з стрімким розвитком з'являється також і більша загроза безпеці інформації. Тому важливо вдосконалювати методи та алгоритми технічного захисту ІКС для забезпечення їх захищеності та безпеки.

Мета та постановка завдання

Мета дослідження полягає в аналізі технічних каналів витоку інформації від сучасних інформаційно-комунікаційних систем.

Технічний канал витоку інформації (ТКВІ) – сукупність джерела небезпечного сигналу, середовища поширення небезпечного сигналу та засобу технічної розвідки.

Тобто, технічним каналом витоку інформації є фізичний шлях небезпечного сигналу (носія інформації) від джерела небезпечного сигналу до зловмисника [3].

В даний час технічний захист інформації набуває все більшого значення. Це обумовлено, перш за все, активним розвитком методів і засобів отримання інформації, що дозволяють несанкціоновано отримувати все більший обсяг інформації на безпечній відстані, оснащенням службових і житлових приміщень, з використанням автомобілів та інших транспортних засобів, різноманітною електро- і радіоелектронною апаратурою.

Одним з аспектів управління інформаційною безпекою [22], є проведення аналізу ризику, пов'язаного з безпекою, що включає в себе оцінку загрози порушення захищеності інформації через можливі технічні канали витоку.

Розуміючи сутність кожного виду технічних каналів витоку інформації із сучасних інформаційно-комунікаційних систем дозволить розробити ефективні методи протидії та вберегти дані для його власника.

Виклад основного матеріалу дослідження

Сьогодні витік інформації є значною загрозою для діяльності будь-якого підприємства в любій країні світу. Втрата репутації чи довіри клієнтів, величезні фінансові збитки, банкрутство підприємства аж до ліквідації суб'єкта господарської діяльності – все це можливі наслідки витоку інформації. Саме тому функціонування системи інформаційно-комунікативного забезпечення діяльності підприємства має бути спрямованою на реалізацію заходів із запобігання витоку інформації, а менеджерів підприємств – на пошук шляхів їх реалізації. Для встановлення вимог та організації захисту інформації від витоку технічними каналами нами здійснена їх класифікація за певними ознаками. Зокрема відокремлені типи ТКВІ за такими ознаками:

– за видом інформаційної діяльності об'єкту інформаційної діяльності (ОІД) [5];

– за принципом (фізичним ефектом, процесом) формування небезпечного сигналу (носія інформації);

– за середовищем поширення небезпечного сигналу;

– за способом перехоплення (зняття) небезпечного сигналу засобами технічної розвідки зловмисника.

За видом інформаційної діяльності виділяють такі типи ТКВІ:

– технічні канали витоку мовної інформації;

– технічні канали витоку інформації, що обробляється;

– технічні канали витоку візуальної інформації, матеріально-речовинні канали витоку інформації.

Узагальнені підходи до класифікації технічних каналів витоку інформації представлено на рис. 1.

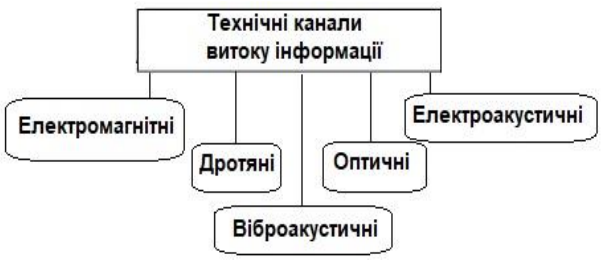

Рис. 1. Схематичне зображення структури технічних каналів витоку інформації

Існують підходи до класифікації технічних каналів витоку інформації, згідно яких виділяють:

– радіоканали – електромагнітні випромінювання радіодіапазону (рис. 2);

Рис. 2. Схематичне зображення структури технічних каналів витоку інформації

– електричні – напруга і струм в струмопровідних комунікаціях;

– акустичні – розповсюдження звукових коливань в будь-якому звукопровідному матеріалі;

– оптичні – електромагнітні випромінювання в інфрачервоній, видимій і ультрафіолетовій частині спектру [4];

– матеріально-речові – папір, фотографії, магнітні носії (рис. 3).

Рис. 3. Класифікація матеріально-речових каналів витоку інформації

Для електромагнітних каналів витоку інформації характерними є такі побічні випромінювання:

– електромагнітні випромінювання технічних засобів обробки інформації. Носієм інформації є електричний струм (сила струму, напруга, частота або фаза якого змінюється за законом інформаційного сигналу);

– електромагнітні випромінювання на частотах роботи високочастотних генераторів технічних засобів обробки інформації, допоміжних засобів обробки інформації. В результаті зовнішніх впливів інформаційного сигналу на елементах генераторів наводяться електричні сигнали, які можуть викликати ненавмисну модуляцію власних високочастотних коливань генераторів і випромінювання в навколишній простір [6];

– електромагнітні випромінювання на частотах самозбудження підсилювачів низької частоти технічного засобу витоку інформації. Самозбудження можливе за рахунок випадкових перетворень негативних зворотних зв'язків в паразитні позитивні, що призводить до переведення підсилювача з режиму посилення в режим автогенерації сигналів, причому сигнал на частотах самозбудження виявляється промодульованим інформаційним сигналом.

Можливими причинами виникнення електричних каналів витоку інформації можуть бути:

– наведення електромагнітних технічних засобів обробки інформації. Вони виникають при випромінюванні елементу технічних засобів обробки інформації інформаційних сигналів, а також при наявності гальванічного зв'язку, де є сполучні лінії технічних засобів обробки інформації і сторонніх провідників або лінії допоміжних засобів обробки інформації [8];

– просочування електромагнітних сигналів в ланцюзі електроживлення. Таке можливе при наявності магнітного зв'язку між вихідними трансформатором підсилювача і трансформатором електроживлення, а також за рахунок нерівномірного навантаження на випрямляч, що призводить до зміни споживаного струму за законом зміни інформаційного сигналу;

– просочування інформаційних сигналів в ланцюзі заземлення за рахунок гальванічного зв'язку з землею різних провідників, що виходять за межі контрольованої зони, в тому числі нульового проводу мережі електроживлення, екранів, металевих труб систем опалення та водопостачання, металевої арматури;

– отримання інформації з використанням заставних пристроїв відбувається з допомогою мініпередавачів, що встановлюються в технічних засобах обробки інформації, випромінювання яких модулюється інформаційним сигналом і приймаються за межами контрольованої зони [16].

Також не останню роль відіграє людський фактор, коли співробітник через недогляд відкриває доступ до закритих даних всім бажаючим.

Для аналізу ризику для захисту від витоку конфіденційної інформації використовуються: системи аутентифікації та ідентифікації, системи криптографічного захисту дискових даних, а також інформації, що передається по мережах, програмні рішення для управління ключами шифрування.

Засоби аутентифікації та ідентифікації дозволяють обмежити доступ до ресурсів мережі. Для цього у користувача запитується якась інформація, відома тільки йому, після чого відкривається доступ.

Для реалізації цієї можливості використовуються: біометрія-фізіологічні особливості людей (відбитки пальців, зображення райдужної оболонки ока і так далі); конфіденційна інформація – паролі, ключі та інше [11].

Під технічним каналом витоку акустичної (мовної) інформації розуміють сукупність об'єкта розвідки (виділеного приміщення), технічного засобу акустичної (мовної) розвідки, за допомогою якого перехоплюється мовна інформація, і фізичного середовища, в якій поширюється інформаційний сигнал. Залежно від фізичної природи виникнення інформаційних сигналів, середовища їх поширення технічні канали витоку акустичної (мовної) інформації можна розділити на: прямі акустичні (повітряні), акустовібраціонние (вібраційні), акустооптичні (лазерні), акустоелектричні і акустоелектромагнітні (параметричні) (рис. 4).

Рис. 4. Підходи до класифікації акустичних каналів витоку інформації

Основними технічними каналами витоку інформації при обробці конфіденційних даних (КД) будемо вважати акустичний (віброакустичний) або видовий канал, побічні електромагнітні випромінювання і наведення (ПЕМВН).

Сучасні засоби обробки та передачі інформації, комп'ютерні системи є електронними, а тому їх робота завжди супроводжується побічними електромагнітними випромінюваннями та наведеннями, які можуть утворювати технічні канали витоку інформації. При роботі з сучасними ІКС такий витік інформації є небажаним і представляє собою загрозу щодо порушення її конфіденційності.

Акустоелектричні канали витоку виникають у результаті перетворення акустичних сигналів в електричні на елементах технічних засобів по принципу мікрофонного ефекту. Причиною виникнення акустоелектричних каналів витоку інформації є технічні засоби, що встановлюються в виділеному приміщенні, серед яких найбільш часто зустрічаються мобільні телефони. В телефонних апаратах існують елементи, які здійснюють перетворення акустичних сигналів в електричні, тим самим створюючи акустоелектричний канал витоку інформації за рахунок властивостей нелінійності, а також методом «високочастотного нав'язування». Мікрофонним ефектом володіють такі елементи технічних засобів, що входять до їх електричної схеми: конденсатори, резистори, п'єзокристали [13].

Головною особливістю радіозв'язку є використання процесу модуляції для перетворення інформаційного сигналу у сигнал, який може бути переданий по каналу зв'язку. Для передавання інформаційного сигналу на відстань використовується сигнал-носій. Сигнал-носій ще називають сигналом, що модулюється (несучим сигналом або коливанням), інформаційний сигнал-модулюючим сигналом. У результаті накладання інформаційного сигналу та сигналу-носія утворюється модульований сигнал, який і передається по каналу зв'язку. Як правило, частота несучого коливання завжди більша, ніж частота інформаційного сигналу, а передавання високочастотного сигналу вимагає суттєво менших енергетичних затрат, ніж низькочастотного інформаційного сигналу.

Джерелом утворення акустичного каналу витоку інформації є вібруючі, коливні тіла й механізми, такі як голосові сигнали людини, рухомі елементи машин, телефонні апарати, звукопідсилювальні системи. Акустичні канали витоку інформації утворюються за рахунок: – поширення акустичних коливань у вільному повітряному просторі; – впливу звукових коливань на елементи й конструкції будинків; – впливу звукових коливань на технічні засоби обробки інформації.

Отже, акустичні сигнали можуть поширюватися у будь-якому пружному середовищі. Саме цим пояснюється можливість проходження акустичних сигналів через елементи будівельних конструкцій (стіни, стеля, підлоги, двері, скло вікон, труби і т. п.). Для того, щоб передати звук по каналах зв'язку або записати на носій інформації, акустичний сигнал необхідно перетворити у відповідний електричний сигнал за допомогою мікрофона. Сучасні динамічні, конденсаторні та електретні мікрофони забезпечують високу якість запису та відтворення акустичної інформації.

Для несанкціонованого одержання звукової інформації можуть використовуватися й інші елементи електричних та електронних приладів за рахунок акустоелектричних перетворень, що є результатом так званого «мікрофонного ефекту». Принцип цього ефекту можна пояснити на прикладі звичайного телефону. Відомо, що на телефон від лінії подається постійний струм з напругою 45 В. Також відомо, що у вхідному каскаді телефону завжди є трансформатор, що під'єднаний до лінії. Телефон знаходиться у повітряному середовищі, яке добре передає акустичні сигнали. На трансформатор діє акустичні сигнали розмов, що ведуться у приміщенні з телефоном. При цьому по телефону у цей час розмови не ведуться, але дія акустичних хвиль на трансформатор завдяки явищу магнітострикції збуджує у ньому змінне магнітне поле, яке в свою чергу, спричинює виникнення струму самоіндукції в обмотках трансформатора. А

цей струм можна зняти безпосередньо з телефонної лінії, під'єднаної до телефонного апарату [12].

Віброакустичний канал витоку створюється з тієї причини, що акустичний сигнал створює повітряну хвилю, яка впливає на поверхню твердого матеріалу об'єкту інформаційної діяльності (ОІД) (пружне середовище) і це приводить його до вібрації. В залежності від густини матеріалу вібрація може розповсюджуватись на досить великі відстані. Чим більша густина, тим більша дальність розповсюдження сигналу.

У приміщенні, де є мовна інформація, такими твердими тілами та пружними середовищами є зовнішні конструкції приміщення (стіни, двері та вікна, стеля, підлога) та всі інші предмети (труби системи опалення, водопостачання тощо), що трапляються на шляху змінного повітряного тиску і які виходять за межі приміщення, або мають щільний контакт з предметами за межами приміщення. Безпосередньо отримувачами акустичної інформації є лазерні стетоскопи, електронні стетоскопи, спрямовані мікрофони. Лазерні стетоскопи дистанційно реєструють коливання віконного скла ОІД, з наступним зворотнім перетворенням сигналу. Середовищем поширення є повітря. Електронні стетоскопи реєструють, з наступним перетворенням у акустичний сигнал, вібрацію стін, дверей, також вікон, стель, підлог, труб системи опалення, водопостачання тощо. Для цього потрібен безпосередній контакт приладу з вказаними конструкціями.

Оптичні канали витоку інформації утворюються випромінюванням, перевипромінюванням та відбиванням в інфрачервоній, видимій та ультрафіолетовій областях спектру (рис. 3). Нині існують ефективні оптичні системи, що дозволяють з відстані близько сотні кілометрів розрізняти навіть номерні знаки автомобіля, тому сфотографувати документ із відстані кількох сотень метрів не є проблемою. Волоконно-оптичний зв'язок – вид дротового електрозв'язку, який використовує в якості носія інформаційного сигналу електромагнітне випромінювання оптичного або інфрачервоного діапазону, а в якості направляючих систем волоконно-оптичні кабелі.

В основі функціонування волоконно-оптичних ліній зв'язку лежить принцип поширення світлових хвиль оптичними хвилеводами на велику відстань. При цьому електричні сигнали, що несуть інформацію, перетворюються в світлові імпульси, які з мінімальним затуханням передаються по волоконно-оптичному кабелю. Оптоволоконні лінії є комбінацією матеріалів з різними оптичними та механічними характеристики, поєднуючи в собі механічну міцність та високий коефіцієнт заломлення світла. При передачі інформації по оптоволоконних лініях використовується модуляція інтенсивності світла, відповідно канали витоку формуються в залежності від інтенсивності світлового потоку. Оптоволоконні канали витоку інформації можна розділити на три типи:

– порушення повного внутрішнього відбивання. Перший канал витоку формується при виході частини випромінювання з хвилеводу внаслідок порушення повного внутрішнього відбивання при поширенні світлового променю всередині хвилеводу.

– реєстрація розсіяного випромінювання. Сигнал при передачі по волоконно-оптичній лінії зв'язку не потребує підсилення (завдяки дуже малим втратам у каналі передачі). Але так як ретрансляція інформації відбувається на значні відстані, необхідна генерація світлових імпульсів значної потужності. Високі потужності вхідного світлового потоку в зонах ретрансляторів розсіюються, утворюючи канал витоку інформації.

– параметричні методи реєстрації випромінювання. Канал витоку формується при зміні властивостей самого оптоволокна. Оптичне випромінювання, яке є носієм інформації, викликає зміну фізичних параметрів самого оптоволокна. Модуляцію властивостей оптоволокна в залежності від інтенсивності світлових імпульсів можна реєструвати спеціальними високочутливими приймачами. До основних характеристик оптичного хвилеводу можна віднести показник заломлення, показник поглинання, зміну геометричних розмірів, властивості поверхні волокна.

У більшості випадків, виявлення технічних каналів витоку інформації розуміють як визначення і знаходження джерела конфіденційної інформації і приймача конфіденційної інформації. Так, якщо мова йде про приховані канали витоку інформації, наприклад таких як закладні прослуховуючі пристрої, що впроваджуються в технічні засоби, пристрої знімання інформації і т.д., то застосовуються спеціальні засоби виявлення цих закладних пристроїв. Для виявлення таких пристроїв проводять спеціальні перевірки технічних засобів обробки інформації, а також всього об'єкту в цілому включаючи меблі, стіни і перекриття.

В даний час на ринку засобів виявлення технічних каналів витоку конфіденційної інформації за допомогою закладних пристроїв можна знайти досить багато подібної апаратури, виробленої як в Україні так і за кордоном. До таких засобів відносяться:

– скануючі приймачі – детектори, налаштовані на розпізнавання різних частот, які можуть розпізнати мобільні пристрої, що знаходяться поблизу працюючого детектора;

– радіо-частотометри, здатні виявити радіовипромінюючі закладки;

– індикатори електромагнітних випромінювань, здатні виявити радіовипромінюючі закладки, а також проаналізувати провідні лінії зв'язку;

– комплекси різних пошукових засобів і багато інших засобів.

Таким чином правильно створена система захисту забезпечує інформаційну безпеку всієї організації, гарантує доступність, цілісність та конфіденційність важливих відомостей. Тому комплекс заходів необхідно орієнтувати на виявлення та запобігання за-

грозам, а також своєчасне та повне усунення наслідків дій зловмисників.

Усі методи захисту зазвичай використовують у вигляді комплексних заходів, оскільки окремий спосіб не дасть достатній рівень безпеки.

На сьогодні використовуються наступні методи захисту інформації [3]:

1. Організаційно-правові засоби. Різні інструменти, що застосовуються в ході будівництва IT-інфраструктури, що забезпечує зберігання даних – при побудові та ремонті будівель і приміщень, проектуванні систем. До них відносять діючі стандарти та договори (в т. ч. міжнародні);

2. Інженерно-технічні засоби. Базові інструменти відповідальні за фізичну безпеку. Це захист від несанкціонованого доступу, перехоплення та прослуховування інформації, стихійних лих, пожеж, контроль діяльності та пересування співробітників та інші заходи;

3. Криптографічні засоби. Шифрування інформації при її зберіганні та передачі. Криптографія допомагає забезпечити конфіденційність та підтвердити справжність даних, зберегти їх цілісність та заборонити доступ стороннім особам до програмного забезпечення;

4. Програмно-апаратні засоби. Це різноманітні інструменти, які дозволяють ідентифікувати співробітників, зашифрувати інформацію, просигналізувати про несанкціонований вхід, знищити дані на носіях. Апаратні засоби вбудовують в обладнання (різні схеми, регістри), фізичні реалізують у вигляді електронно-механічних пристроїв (магнітні замки, камери спостереження), а як програмні застосовують спеціальний софт.

Міжнародне законодавство ставить певні вимоги до захисту інформації та передбачає відповідальність за її порушення. Крім того, воно встановлює загальні стандарти та принципи захисту, що мають бути враховані державами та організаціями при розробці власних законів та політики в галузі захисту інформації.

Міжнародне законодавство з захисту інформації включає такі важливі документи:

1. Загальна декларація прав людини – стверджує право на свободу думки, совісті та висловлювання, що включає право на захист приватності та інформаційну свободу;

2. Конвенція про захист прав людини і основоположних свобод – забезпечує право на захист особистих даних, що збираються, обробляються та зберігаються в автоматизованих системах;

3. Конвенція Ради Європи про кіберзлочинність – містить положення про криміналізацію дій, що пов'язані з комп'ютерним шахрайством, незаконним доступом до комп'ютерних систем та поширенням комп'ютерних вірусів;

4. Регламент ЄС про захист персональних даних – встановлює стандарти захисту персональних даних громадян ЄС, що збираються та обробляються компаніями та організаціями;

5. Директива ЄС про захист інформації в мережах та інформаційних системах – містить положення про захист інформації від несанкціонованого доступу та впливу, встановлює вимоги до захисту інформаційних систем;

6. ISO/IEC 27001:2022 визначає вимоги щодо створення, впровадження, підтримки та постійного удосконалення системи управління інформаційною безпекою всередині організації. Цей стандарт також включає в себе керівні директиви для оцінки та обробки ризиків інформаційної безпеки, з урахуванням специфічних потреб організації.

В Україні діє кілька законодавчих актів, що регулюють захист інформації:

1. Закон України «Про захист персональних даних» – регулює збір, зберігання, використання та поширення персональних даних громадян України та інших осіб, що перебувають на території України;

2. Закон України «Про інформацію» – визначає права та обов'язки суб'єктів інформаційних відносин, регулює порядок доступу до інформації, що належить до публічної та обмеженої доступності;

3. Кримінальний кодекс України – містить статті, що криміналізують незаконний доступ до комп'ютерних систем, шахрайство з використанням інформаційних технологій, поширення комп'ютерних вірусів та ін.;

4. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» – визначає порядок захисту інформації в інформаційно-телекомунікаційних системах, включаючи захист від несанкціонованого доступу та впливу;

5. Закон України «Про кібербезпеку» – встановлює загальні принципи державної політики в галузі кібербезпеки, визначає порядок реагування на кібератаки та відновлення функціонування інформаційних систем.

Ці закони визначають основні принципи захисту інформації в Україні та передбачають відповідальність за їх порушення.

Також технічний захист сучасних ІКС є надзвичайно важливим під час правового режиму воєнного стану, який діє в Україні з 24 лютого 2022 року, під час якого наша держава стикається з серйозними загрозами і викликами для своєї безпеки, та територіальної цілісності. У таких умовах правильне управління інформацією та її захист є ключовим елементом успішного забезпечення національної безпеки.

Захист інформації під час воєнного стану передбачає розвиток та впровадження новітніх технологій захисту інформації, включаючи криптографічні методи та системи захисту мереж, а також навчання військових та цивільних службовців з питань інформаційної безпеки та кіберзахисту. Також важливо мати

ефективний механізм контролю за розповсюдженням дезінформації та пропаганди.

Отже, захист інформації під час воєнного стану в Україні є надзвичайно важливим завданням, що вимагає відповідального та проактивного підходу державних органів, військових та цивільних службовців, а також громадських організацій та громадян.

Висновки. На початку дослідження проаналізовано підходи до сутності поняття «витоки інформації». Систематизовано інформацію стосовно класифікації технічних каналів витоку інформації та вказано головні причини виникнення технічних каналів витоку інформації.

Окрім цього, розглянуто міжнародне та українське законодавство у сфері захисту інформації з чого можна зробити висновок, що під час дії правового режиму воєнного стану в Україні виникає низка викликів, пов'язаних з інформаційною безпекою. Це можуть бути кібератаки на державні системи та мережі, дезінформація, пропаганда, підривна діяльність та інші загрози. Важливо мати ефективну систему захисту ІКС від таких загроз, що забезпечує збереження конфіденційності, цілісності та доступності інформації.

Також стає зрозуміло, що одним з найбільш ризикованих технічних каналів витоку інформації від сучасних ІКС при обробці конфіденційних даних можна вважати канал побічних електромагнітних випромінювань і наведень, що ставить перед нами актуальне завдання щодо обґрунтування захищеності джерел конфіденційної інформації від витоку технічними каналами для всіх видів їх аналого-цифрового перетворення, що реалізують сучасні ІКС, на основі заданих гранично допустимих ризиків інформаційної безпеки.

Список літератури

[1]. Бурий А. С., Ловцов Д. А. Перспективи стандартизації інформаційного простору «розумного міста». Інформаційно-економічні аспекти стандартизації та технічного регулювання. № 2 (66). 2022, С. 4-11.

[2]. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник; за заг. ред. професора В. Б. Толубка. К.: ДУТ, 2015. 288 с.

[3]. Заболоцький Т. Кіберпростір як інструмент соціального впливу на сучасну молодь. Ввічливість. Humanitas, 2021. № (1). С. 22-27.

[4]. Завгородня Ю. В. Кіберпростір як сучасна платформа для вирішення конфліктів. History, political science, philosophy and sociology: European development direction. Riga, Latvia: Baltija Publishing. 2021. С. 53–56.

[5]. Капітон А. Перспективи розвитку кіберпростору та його соціально-психологічні наслідки. Системи управління, навігації та зв'язку. Збірник наукових праць. Полтава: ПНТУ, 2021. Т. 3 (65). С. 89–91. DOI: https://doi.org/10.26906/SUNZ.2021.3.089.

[6]. Мальцева І. Р. Аналіз деяких кіберзагроз в умовах війни. Кібербезпека: освіта, наука, техніка. 2022. № 4 (16). С. 37-43. DOI: 10.28925/2663–4023.2022.16.3744.

[7]. Пантєлєєва Н. М. Кіберзагрози в умовах цифрової економіки. Фінансовий простір. 2019. № 1. С. 130-139.

[8]. Ревак І. О. Особливості формування безпечного кіберпростору в умовах розвитку цифрової економіки. Інформаційні технології та економічна безпека. 2021. № 3-4. С. 164-169.

[9]. Стець В. Кіберпростір як об'єкт публічного управління в сфері забезпечення кібербезпеки. Публічне управління: традиції, інновації, глобальні тренди: матеріали Всеукраїнської наук. – практ. конф. за міжнар. участю. Одеса: ОРІДУ НАДУ, 2021. С. 290-292.

[10]. Стець В. В. Ккіберпростір як основний об'єкт публічного управління у сфері забезпечення кібербезпеки. Наукові перспективи. 2022. № 8 (26). С. 98-115.

[11]. Ткач Ю. Концептуальна модель безпеки кіберпростору. Технічні науки та технології. 2021. № 4 (22). С. 96-108. https: // doi. org / 10.25140 / 2411–5363–2020–4(22)–96–108.

[12]. Ткач Ю. М. Тенденції розвитку сучасного кіберпростору та його захищеності в умовах інформаційного протиборства. Безпека інформації. 2020. Т. 26 (2). С. 74-80.

[13]. Федонюк С. Міжнародні аспекти безпеки кіберпростору. Луцьк: Вежа-Друк, 2022. 178 с.

[14]. Фролова О. Міжнародне співробітництво в галузі забезпечення інформаційної безпеки. Вісник Львівського університету. Серія: Міжнародні відносини. 2019. Вип. 46. С. 123-136.

[15]. Hafiiak A. Problems of professional competence of future specialists on information and communication technologies in universities. Series: Education and Pedagogy. 2019. № 10 (2). pp. 15-18.

[16]. Указ Президента України №392/2020 Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України».

[17]. Закон України «Про основні засади забезпечення кібербезпеки України» (2017р.).

[18]. Закон України «Про інформацію» (1992р.).

[19]. Information technology. Security techniques. Information security management systems. Requirements [ISO/IEC 27001:2013].

[20]. Іванченко С.О. Обґрунтування ризику безпеки інформації щодо її захищеності від витоку технічними каналами / Сергій Олександрович Іванченко // Науково-технічний збірник "Правове, норма-

тивне та метрологічне забезпечення систем захисту інформації в Україні". – Київ, НТУУ "КПІ" НДЦ "Тезис", 2016. № 1 (31). С. 9-13.

[21]. Kuhn G. Compromising emanations: eavesdropping risks of computer displays. This technical report is based on a dissertation submitted June 2002 by the author for the degree of Doctor of Philosophy to the University of Cambridge, Wolfson College. URL: http://www.cl.cam.ac.uk/techreports.

[22]. Information technology. Security techniques. Information security management systems. Requirements [ISO/IEC 27001:2022].

УДК 621.39

Horlichenko S. Peculiarities of the formation of technical channels of information leakage from modern x-rays

Abstract. *Information and communication systems are constantly developing and improving, introducing new technologies and opportunities. However, along with rapid development comes a greater threat to information security. Therefore, it is important to improve the methods and algorithms of technical protection of ICS to ensure their security and safety. An analysis of various approaches to defining the essence of the term "information leaks" was carried out, as well as a systematization of information regarding the classification of technical channels through which information leaks occur. In addition, an overview of the main reasons that lead to the emergence of electrical channels of information leakage is provided. The essence of the process of formation of technical channels of information leakage is studied, and various methods of protecting information from such leaks are highlighted. International and domestic legislation regulating the sphere of information protection, in particular in Ukraine, was also analyzed. Attention is focused on the importance of ensuring information security during martial law in Ukraine. In the context of modern challenges and threats related to cyber security. The need to strengthen information protection measures to ensure an adequate level of protection in conditions of martial law and potential threats was emphasized.*

Key words*: cyber security, information security, technical information protection, information leak, technical leak channel, electromagnetic radiation, information and communication systems.*

Горліченко Сергій Олександрович, науковий співробітник Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "Київський Політехнічний Інститут імені Ігоря Сікорського".

Serhii Horlichenko, researcher of the Institute of Special Communication and Information Protection of the National Technical University of Ukraine "Ihor Sikorsky Kyiv Polytechnic Institute".

Отримано *21 липня 2023 року*, затверджено редколегією *28 серпня 2023 року*