**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**Західноукраїнський національний університет**

**Навчально-науковий інститут публічного управління**

Кафедра фінансів ім. С.І. Юрія

**ШВИРЛО Юрій Михайлович**

**Методи захисту інформації в органах ДПС України/Methods of information protection in State Tax Service of Ukraine**

Спеціальність: 281 – Публічне управління та адміністрування

освітньо-професійна програма – Державна служба

Кваліфікаційна робота

 Виконав студент групи

 ДСПУАзм-25

 Ю. М. Швирло

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 Науковий керівник:

 д.е.н., професор О.І. Тулай

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Кваліфікаційну роботу

допущено до захисту

«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_р.

Завідувач кафедри

\_\_\_\_\_\_\_\_\_\_\_\_\_ О. П. Кириленко

**ТЕРНОПІЛЬ-2021**

­­

ЗМІСТ

[Вступ 4](#_Toc89211298)

[Розділ 1.](#_Toc89211299) [Теоретичні та організаційно-правові засади захисту інформації 9](#_Toc89211300)

[1.1. Сутність, роль і значення безпеки інформаційних технологій 9](#_Toc89211301)

[1.2. Історичні та організаційно-правові засади регулювання інформаційної безпеки 17](#_Toc89211302)

[Висновки до розділу 1. 23](#_Toc89211303)

[Розділ 2.](#_Toc89211304) [Сучасні методи захисту інформації в органах дпс україни 25](#_Toc89211305)

[2.1. Класифікація методів захисту інформації 25](#_Toc89211306)

[2.2. Практика застосування методів отримання акустичної інформації 30](#_Toc89211307)

[2.3. Програмний захист інформації як невід’ємна складова збереження цілісності інформації в органах дпс україни 38](#_Toc89211308)

[Висновки до розділу 2. 48](#_Toc89211309)

[Розділ 3.](#_Toc89211310) [Перспективні напрями вдосконалення методів захисту інформації в органах дпс україни 50](#_Toc89211311)

[3.1. Напрями підвищення ефективності використання систем зашумлення 50](#_Toc89211312)

[3.2. Пріоритети вибору елементів системи захисту інформації у контексті новітніх тенденцій 55](#_Toc89211313)

[Висновки до розділу 3. 64](#_Toc89211314)

[Висновки 66](#_Toc89211315)

[Список використаних джерел 70](#_Toc89211316)

# ВСТУП

У період постійного зростання ролі інформаційних технологій значення якості інформації, що обробляється та зберігається в інформаційних системах, залишається пріоритетним у всіх галузях людської діяльності. Висока якісь інформації досягається завдяки її достовірності, точності та актуальності, тому інформаційні системи мають бути захищені від втручань та несанкціонованих змін та втрат. Таким чином захист інформації – це система методів, заходів та засобів, що дозволяють забезпечувати цілісність, конфіденційність і доступність інформації в процесі її збору, опрацювання та зберігання, а також в умовах постійного вплину загроз природного та техногенного характеру. Реалізація цих загроз призводить до пошкодження чи втрати інформації, що може нести економічні та соціальні негативні наслідки залежно від галузі.

 У сучасному світі інформація – це товар, який має доволі високу ціну. Чим цінніша інформація, тим ретельнішим і більш багатогранним має бути її технічний захист. Адже від належного ступеня захисту інформації залежить благополуччя, а коли мова йде про систему охорони здоров’я, навіть життя людей. Насправді питання захисту інформації сьогодні актуальне на усіх рівнях суспільства. Наприклад, на рівні державних органів важливо забезпечити збереження державних таємниць, а також захист інформації, отриманої від фізичних та юридичних осіб в межах реалізації захисту персональної інформації та комерційних таємниць. Для великих юридичних компаній важливо зберігати від несанкціонованих змін та поширення дані щодо стратегії розвитку, патентних розробок, комерційної інформації, персональних даних працівників. Малі підприємства також можуть бути зацікавлені у захисті інформації з метою збереження конкурентних переваг. Окремі фізичні особи також повинні застосовувати заходи інформаційної безпеки з метою захисту особистих персональних даних, даних власних платіжних карток та іншої фінансової інформації.

На практиці забезпечення інформаційної безпеки на рівні держави та підприємств є набагато складнішим у порівнянні з фізичними особами, оскільки обсяги і цінність інформації, із якою вони працюють, вища. Відповідно, рівень і кількість загроз, що виникають, також суттєвіші. В залежності від галузі діяльності та обсягу даних забезпечення інформаційної безпеки потребує значних фінансових витрат: працевлаштування та навчання спеціалістів, придбання дорогого технічного та програмного забезпечення, інформаційна робота з персоналом щодо дотримання правил інформаційної безпеки тощо.

На державному рівні від захисту інформації залежить національна безпека. Інформація, яка є державною таємницею, або інша інформація, поширення якої законодавчо обмежено, повинна зберігатися та опрацьовуватися в інформаційно-телекомунікаційних мережах, що включають спеціально спроектовані та впроваджені комплексі системи захисту інформації, які відповідають чинному законодавству у галузі технічного захисту інформації. Атестація системи захисту інформації проводиться державними ліцензіатами та реєструється в Адміністрації Державної служби спеціального зв’язку та захисту інформації України. При розробці системи захисту інформації для потреб органів державного управління допустимо застосовувати лише ті засоби, пристрої та програмне забезпечення, які пройшли державну експертизу та мають сертифікат відповідності. Порядок проведення державної експертизи комплексних систем захисту інформації, в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах і засобів технічного захисту інформації встановлюється Державною службою спеціального зв’язку та захисту інформації України.

Протягом останніх років спостерігається суттєвий розвиток методів обміну інформацією на великих відстанях (зростання частки і ролі мобільних мереж, збільшення швидкості передавання інформації у мережах), а також зростає кількість способів та засобів представлення інформації.

В умовах лібералізації та інтенсифікації економічних відносин, зростання швидкості економічного життя, збільшується частка оперативної інформації, а відтак дуже суттєвим залишається вербальне спілкування як засіб обміну інформацією. Аудіальна інформація майже завжди передує формуванню інших видів інформації (наприклад, звітів), адже вона безпосередньо зв’язує людей і слугує інструментом узгодження дій, формування доручень, вказівок, планів. Таким чином загострюється потреба в забезпеченні захисту живої аудіальної інформації, а також інформації, що передається із застосуванням провідних ліній зв’язку. Зазвичай, комерційні та державні некомерційні організації у цілях реалізації захисту такої інформації надають перевагу створенню корпоративної захищеної мережі на базі мереж зв’язку загального користування. Цей спосіб полягає у забезпечені захисту інформації безпосередньо на місці розташування користувача, а також в каналах зв’язку. Такі заходи, зазвичай, реалізуються власними силами компанії чи організації.

Завдання захисту розмов, які відбуваються у приміщенні на території організації, пов’язане не лише із певними витратами, але й деякими незручностями для осіб, що приймають участь у переговорах. Досвід захисту розмов прийшов у інші сфери людської діяльності із військової галузі. З часом розвивалося промислове шпигунство, що вимагало відповідних засобів захисту. Розвідувальні дії з метою отримання аудіальної (чи будь-якої іншої) інформації найчастіше здійснюються шляхом отримання доступу до каналів передачі такої інформації. Звісно, за таких умов виникає потреба в захисті інформації від несанкціонованого доступу, зміни, копіювання, знищення, псування та інших злочинних і небажаних дій. Ефективне забезпечення захисту інформації відбувається, в основному, шляхом аналізу та виявлення потенційних загроз та розробки і впровадження заходів протидії виявленим загрозам.

Зважаючи на всі перелічені фактори та обставини вважаємо за доцільне постійно розширювати та вдосконалювати дослідження в галузі інформаційної безпеки, зокрема у галузі державного управління.

***Метою роботи є*** розвиток теоретичних знань та практичних засобів у галузі захисту інформації, виявлення та дослідження шляхів вдосконалення пріоритетних елементів системи захисту інформації в роботі органів ДПС України.

Відповідно до мети роботи сформульовано наступні ***завдання***:

* дослідити сутність та роль безпеки інформаційних технологій в сучасному суспільстві;
* розкрити особливості законодавчого регулювання галузі захисту інформації в історичному та організаційно-правовому контекстах;
* узагальнити підходи до класифікації методів захисту інформації;
* проаналізувати особливості практичного застосування методів отримання акустичної інформації;
* охарактеризувати найпоширеніші та найефективніші засоби програмного захисту інформації;
* виявити напрями підвищення ефективності застосування систем зашумлення;
* окреслити та аргументувати пріоритети вибору елементів системи захисту інформації.

***Об’єкт дослідження*** – процес захисту інформації в органах ДПС.

***Предмет дослідження*** – теоретичні та практичні засади формування методів захисту інформації.

Для досягнення мети роботи буде застосовано комплекс загальнонаукових та спеціальних ***наукових методів***, зокрема:

* аналіз, синтез, дедукція, індукція, порівняння, теоретичне узагальнення, аналогія – для дослідження теоретичної бази, сутності, змісту явищ та понять, класифікаційних підходів;
* історичний та логічний методи – для дослідження процесу розвитку інформаційних загроз та засобів забезпечення інформаційної безпеки, а також історичного аспекту нормативно-правового регулювання галузі;
* метод морфологічного аналізу та узагальнений евристичний метод – для дослідження основних характеристик технічних приладів, що використовуються як рішення у галузі інформаційної безпеки, пошуку та виявлення особливостей їх застосування, оцінки їх ефективності за визначених умов;
* методи спостереження та експерименту – для перевірки теоретичних суджень на практиці та демонстрації доцільності впровадження.

***Інформаційну базу*** дослідження складають Закони України, постанови КМУ та нормативні документи у галузі технічного захисту інформації (НД ТЗІ), державні стандарти України стосовно створення та функціонування комплексних систем захисту інформації, стандарти міжнародної організації зі стандартизації, що регулюють питання захисту інформації.

***Наукова новизна*** одержаних результатів полягає в поглибленні теоретичних, організаційно-правових засад організації та функціонування системи захисту інформації в органах державної влади; формулюванні авторського підходу до класифікації методів захисту інформації; здійсненні оцінювання ефективності методів захисту аудіальної інформації, задля попередження перехоплення такої інформації під час виконання посадових обов’язків державними службовцями; виявленні пріоритетів розвитку систем захисту інформації у державних органах.

***Практичне значення.*** Кваліфікаційна робота стане продовженням досліджень у галузі формаційної безпеки, що мають дати поштовх до вдосконалення методології захисту інформації та впровадження новітніх технічних та програмних рішень у роботу державних органів. Висновки та пропозиції наукового дослідження будуть використовуватись у практичній діяльності територіального органу Державної фіскальної служби України в частині визначених пріоритетних напрямів вибору елементів системи захисту інформації.

# РОЗДІЛ 1

# ТЕОРЕТИЧНІ ТА ОРГАНІЗАЦІЙНО-ПРАВОВІ ЗАСАДИ ЗАХИСТУ ІНФОРМАЦІЇ

## 1.1. Сутність, роль і значення безпеки інформаційних технологій

Аналіз досліджень та нормативно правової бази дозволяє сформувати певне загальне розуміння інформаційної безпеки [9, с. 38; 19, с. 123; 31; 35; 64]. В контексті захисту інформації – це стан захищеності баз даних та систем їх обробки, при якому реалізуються такі важливі критерії як конфіденційність, доступність і цілісність інформації [20, с. 123]. На далі детальніше звернемо увагу, чому саме ці критерії важливі та які є інші важливі критерії інформаційної безпеки. Зі сторони суспільної значущості – це «стан захищеності потреб в інформації особи, суспільства й держави, при якому забезпечується їх існування та прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз» [20, с. 123].

Інформаційна безпека держави характеризується постійним станом захищеності, що в результаті забезпечує стійкість ключових сфер людської діяльності (економіки, науки, технологій, державного управління, військової справи, соціальної сфери тощо) по відношенню до потенційних та наявних інформаційних загроз – викривлення чи втрати інформації.

Поняття інформаційної безпеки включає безпеку таких галузей, як інформаційні, телекомунікаційні та інформаційно-телекомунікаційні системи, а також безпеку інформації у паперовому, усному чи електронному вигляді. Тобто слід розуміти, що захист інформації стосується усіх типів та аспектів даних та інформації.

При дослідженні ролі інформаційної безпеки важливо звернути увагу на поняття функціональної безпеки (англ. Function Safety). Воно тісно пов’язане з інформаційною безпекою, але має дещо інший зміст. По відношенню до інформації та інформаційних систем забезпечення функціональної безпеки означає, що система розроблена і функціонує таким чином, аби коректно і у повному обсязі реалізовувати ті і лише ті цілі та завдання, що були передбачені власником чи замовником [25, c. 114]. Забезпечення захисту інформації тісно пов’язане із розумінням і чіткою реалізацією вимог до інформації.

Власне інформаційна безпека (англ. Information Security) полягає у захищеності та безпечності процесу технічної обробки та зберігання інформації. Тобто фактично інформаційна безпека є властивістю функціонально безпечної системи. Забезпечення цієї властивості повинно попереджати несанкціонований доступ до даних та не допускати їхню втрату у разі виникнення збоїв.

Під інформаційною безпекою, зазвичай, мають на увазі інформаційну безпеку в найбільш загальному сенсі, тобто розглядають її як комплекс заходів, покликаний зменшити кількість і ймовірність шкідливих сценаріїв чи можливих збитків у разі настання таких сценаріїв [24, c. 36]. В такому контексті інформаційна безпека – це економічний фактор, який повинен враховуватися у роботі підприємства чи організації, а інформація або дані при цьому виступають у ролі як певного товару або цінності, що має ціну і підлягає захисту. Оскільки вона може становити інтерес для третіх сторін, відтак – має бути доступною лише для працівників чи інших авторизованих користувачів.

Інформаційні системи включають у себе три компоненти: програмне забезпечення, технічне (апаратне) забезпечення та персонал, що забезпечує цільове застосування системи, реалізовує механізми захисту, розробляє та впроваджує стандарти інформаційної безпеки. Механізми захисту можна виділити у чотири групи:

* технічні, які забезпечують обмеження доступу до інформації за допомогою апаратно-технічних засобів.
* інженерні, які дозволяють попередити пошкодження чи руйнування носія інформації внаслідок намірених зловмисних чи випадкових дій або природного вплину шляхом застосування інженерно-технічних засобів (наприклад, обмежуючі конструкції, пожежна сигналізація та система пожежогасіння, охорона приміщень);
* криптографічні, які обмежують доступ до інформації за допомогою математичних перетворень з використанням спеціальних програмно-апаратних засобів котрі можуть приховувати зміст інформації, її походження та виконавця тощо;
* організаційні, які забезпечують обмежений доступ на територію підприємства чи організації, в окремі її корпуси, приміщення, кабінети за допомогою організаційних заходів (правила надання доступу, пропускний режим, автентифікація, інструкції для користувачів та адміністраторів, затвердження політики інформаційної безпеки).

Розробка, впровадження і розуміння працівниками політик і процедур безпеки дуже важливі, оскільки саме ці документи є основною інформацією адміністраторам, користувачам і операторам про те, які засоби та рішення повинні забезпечити належний рівень безпеки.

Раніше уже згадувалося, що інформаційна безпека держави – це стан, за якого життєво-важливі інтереси людини, суспільства і держави захищені шляхом попередження загроз пов’язаних із використанням не повної чи недостовірної інформації або не своєчасного її отримання. Водночас здійснюється активний захист від зовнішніх інформаційних атак та нівелюється негативний інформаційний потік.

Інформаційна безпека організації передбачає цілеспрямовану діяльність її керівника та посадових осіб по досягненню стану захищеності інформаційного середовища організації шляхом використання дозволених методів і засобів.

Інформаційну безпеку особистості можна охарактеризувати як стан захищеності особистості, окремих соціальних груп та об’єднань людей від негативного впливу, здатного змінювати емоційний стани і психологічні характеристики людини, впливати на її поведінку та певною контролювати свободу вибору. Окрім того, цей стан передбачає захист персональних даних від неправомірного по ширення та використання без згоди особи.

Щоб розширити розуміння інформації як об’єкта захисту часто розглядають її властивості через модель CIA:

* конфіденційність (з англ. confidentiality) – властивість інформації, суть якої в тому, що інформація може бути отримана лише авторизованим користувачем. Натомість неавторизовані користувачі не можуть отримати такий доступ.
* цілісність (з англ. іntegrity) – властивість інформаційної системи, що унеможливлює її редагування неавторизованим користувачем.
* доступність (з англ. availability) – властивість інформації, що передбачає можливість доступу до неї авторизованим користувачем лише за наявності у нього відповідних повноважень (можливі також обмеження - в необхідний для нього час, в необхідному місці) [78, c 35-36].

Деякі інші моделі розширюють розуміння суті інформації в контексті її захисту залученням додаткових властивостей:

* апелювання (з англ. non-repudiation) – можливість встановити автора або власника інформації і довести, що це ніхто інший.
* підзвітність (з англ. accountability) – здатність інформаційної системи фіксувати активність та дії окремих користувачів та відстежувати авторів певних дій в системі.
* достовірність (з англ. reliability) – властивість інформації, яка характеризує її як об’єктивну, таку, що точного відображає події та факти.
* автентичність (з англ. authenticity) – це гарантія того, що інформація заснована на першоджерелах [15, c. 58].

До принципів забезпечення інформаційної безпеки відносять: законність, баланс інтересів особи, суспільства і держави; системність; комплексність; економічна ефективність; інтеграція з міжнародними системами безпеки; безперервність; відкритість алгоритмів і механізмів захисту; розумної достатності [26, с. 20-21].

Відповідно до Закону Україну «Про Основні засади розвитку інформаційного суспільства» [34] вирішення проблеми інформаційної безпеки держави має здійснюватися наступним шляхом:

* «створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів;
* підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їхніх наслідків, здійснення міжнародного співробітництва з цих питань;
* вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп’ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері;
* розгортання та розвитку Національної системи конфіденційного зв’язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація» [34].

В Україні забезпечення інформаційної безпеки на державному рівні здійснюється шляхом захисту інформації, для якої така необхідність захисту визначена національним законодавством.

У роботі раніше згадувалося про загрози безпеці інформації (англ. Security threat). У широкому розумінні це ризик викрадення, зміни або знищення інформації.

Загрози інформаційній безпеці можуть виникати наступним чином:

* внаслідок спостереження зловмисниками за джерелами інформації;
* прослуховування конфіденційних розмов людей і записів акустичних приладів (акустична розвідка);
* перехоплення електричних, магнітних і електромагнітних полів, електричних сигналів електричних і сигналів радіохвиль;
* шляхом несанкціонованого поширення (виносу) фізичних носіїв конфіденційної інформації (папери, флешки, твердотілі накопичувачі) за межі визначеного місця її зберігання;
* розголошення інформації людьми, що мають доступ до секретної або конфіденційної інформації;
* втрати носіїв з інформацією (документів, твердотілих накопичувачів, зразків матеріалів тощо);
* несанкціонованого передавання інформації через сигнали та поля, що створюються в електричних та радіоелектричних приладах в результаті циклу експлуатації, хибного конструювання (виготовлення) або недотримання правил експлуатації, впливу стихійних сил та техногенних катастроф, зокрема, вогню під час пожежі і води, вуглекислоти та піни в ході гасіння пожежі та витікання води в результаті пошкодження трубопроводів;
* збоїв в роботі технічних приладів для збирання, оброблення, зберігання і передавання інформації, що можуть виникати у результаті їх несправності, помилок, які здійснили користувачі або зловмисники з бажанням заволодіти інформацією;
* впливу потужних електромагнітних і електричних полів як штучного та і природного походження [78, с. 54-56].

На основі цих прикладів можна зрозуміти, що усі загрози можна згрупувати на підставі природи причин їх виникнення (походження). Таким чином основні загрози інформаційній безпеці пропонуємо поділяти за змістом на такі три групи:

* загрози впливу неякісної інформації (неправдивої, фальшивої, дезінформації, інформаційні атаки) на окрему людину, організацію, державу;
* загрози несанкціонованого і неавторизованого впливу сторонніх осіб на інформаційну систему (вплив на процес збору, опрацювання, передавання та зберігання інформації);
* загрози інформаційним правам і свободам людини (праву на пошук, збирання, розповсюдження, зберігання, передавання і будь-яке інше використання інформації; праву на інтелектуальну власність (патенти, розробки, технічні проекти) і майнову власність на фізичні носії інформації; право на персональну таємницю; право на таємницю листування тощо).

У наявних джерелах не існує єдиної загальноприйнятої класифікації загроз, хоча існує багато інших її варіантів. Нижче розглянемо перелік поширених класифікацій:

1. за ціллю (на що спрямована загроза);
2. за принципом (яким чином реалізовується) впливу на інформаційну систему;
3. за характером (які зміни, дії відбуваються) на систему;
4. за причинами виникнення;
5. за об’єктом атаки;
6. за засобами реалізації загрози;
7. за станом об’єкту захисту [18, с. 9-11].

Окрім цього загрози логічно ділити на випадкові (або ненавмисні) і навмисні залежно. Джерелом перших можуть бути людські помилки при роботі, поломки технічних засобів, неправильні дії адміністраторів локальної обчислювальної мережі тощо. Навмисні загрози, на противагу випадковим, виникають у зв’язку із прагненням нанести шкоду користувачам та/або власникам інформації або отриманням неправомірної вигоди. Такі загрози, в свою чергу, діляться на активні і пасивні. Пасивні загрози, зазвичай, пов’язані із несанкціонованим використанням інформаційних ресурсів, але при цьому не впливають на загальний стан та функціонування мережі. Прикладами таких загроз є спроби шпигунства з метою отримання інформації, що є об’єктом захисту, шляхом підслуховування, копіювання тощо. Активні загрози спрямовані на те, аби порушити нормальну роботу локальної обчислювальної мережі. Як правило, це відбувається шляхом цілеспрямованого впливу на її технічні, програмні та інформаційні ресурси. Прикладами активних загроз слугують фізичне пошкодження або радіоелектронне заглушення мережевих ліній комунікації, виведення з ладу окремих технічних пристроїв або програмного забезпечення системи, спотворення відомостей про користувачів, викривлення інформації у базах даних тощо. Джерелами активних загроз можуть бути як цілеспрямовані дії зловмисників, так і програмні віруси, що поширюються мережею безсистемно.

За даними дослідження Comparitech, яка сьогодні є однією із провідних організацій у галузі дослідження інформаційної безпеки, Україна має одні із найвищих оцінок стану інформаційної безпеки у світі (в основі оцінки – 15 критеріїв, пов’язаних із частотою і кількістю атак, а також кількістю заражених пристроїв) [54]. Природно, що важливою і , можливо, основною причиною решти ризиків є піратство. В Україні та деяких інших країнах СНД не сформована культура справедливого використання ліцензійних програм, а також відсутнє ефективне законодавче регулювання цієї галузі. В той же час широко поширеним є зараження неліцензійних копій програм шкідливм кодом. Масштаби піратства у Україні описує те явище, що зачасу в особистих цілях для захисту люди використовують неліцензійні копії антивірусного забезпечення. Також поширенню шкідливих програм як на особистих, так і на робочих комп’ютерах сприяє низька компетентність людей у галузі інформаційної безпеки. Користувачі, які не розуміють, що не слід відкривати дивні посилання, отримані від невідомих відправників, (або нехтують цим розумінням), часто можуть стати об’єктами атак.

Шкода від роботи шкідливих програм буває різною: пошкодження операційних систем та програмних засобів, некоректна робота веб-браузерів, за шифрування важливих файлів та документів, втрата персональних даних та прав доступу до інформації, зникнення грошей з рахунків та карток.

Отже, розуміння суті інформаційної безпеки та коректне визначення основних властивостей інформації в контексті її захисту є важливими для формування ефективної стратегії інформаційної безпеки. Остання у свою чергу є важливим елементом національної безпеки країни, тож роль інформаційної безпеки неможливо применшити.

## 1.2. Історичні та організаційно-правові засади регулювання інформаційної безпеки

Стрімкий і постійний ріст та розвиток інформаційних технологій починаючи із 1960-их років зробив інформаційну безпеку вагомим питанням у сучасному світі. Тож варто звернути увагу на основні віхи її розвитку, щоб зрозуміти, як галузь прийшла до теперішнього стану. Не зважаючи на усі нові методи захисту, уряди різних країн та великі приватні компанії страждали від кібер-атак протягом останнього десятиліття. А це говорить про те, що певний шлях розвитку пройшли не лише методи та технології захисту інформації, а й хакери та комп’ютерні віруси.

Умовно історію розвитку кібербезпеки можна розділити на десятиліття [48]:

1. 1960-ті роки – застосування паролів. У цей час вперше організації починають робити кроки у галузі захисту інформації. Зважаючи на відсутність Інтернету, основний фокус був спрямований на фізичних засобах захисту і обмеженні доступу людей до інформації.
2. 1970-ті роки – перший антивірус Reaper. Виникненню першого вірусу і антивірусу передувало створення мережі Arpanet, яку вважають попередником сучасного Інтернету. Цією мережею поширювався нешкідливий код Creeper, написаний у 1971 році Бобм Томасом. При переміщенні він надсилав користувачу повідомлення «I'M THE CREEPER : CATCH ME IF YOU CAN» («Я – Кріпер: впіймай мене, якщо можеш»). Це була єдина дія коду. Пізніше колега Боба Рей Томлінсон написав програму Reaper, яка поширювалася із використанням точно тієї ж технології, але якщо виявляла Creeper, видаляла його [49; 71]. Саме ці коди вважаються першими прототипами комп’ютерного вірусу та антивірусної програми.
3. 1980-ті роки – початок епохи Інтернету. Протягом наступних років комп’ютери ставали все більше сполученими, а віруси – більш досконалими. Мережа Arpanet стала більш відомою як Інтернет і в 1989 році стала доступною для широкого загалу. В той же час системи інформаційної безпеки не завжди справлялися зі шквалом інноваційних підходів хакерів. Наприклад, росіяни почали використовувати хакерів як елемент збройних сил і в 1986 році найняли німецького комп'ютерного хакера Маркуса Гесса для викрадення американських військових таємниць. Він зламав понад 400 військових комп'ютерів, включаючи мейнфрейми в Пентагоні, і мав намір продати їх секрети КДБ [49]. На щастя, йому завадили. Через два роки, в 1988 році, народився «черв'як» Морріса – один з головних поворотних моментів в історії інформаційної безпеки. Його здатність до самокопіювання була настільки агресивно, що робила цільові комп’ютери непрацездатними і сповільнювала Інтернет. Тобто це була перша в історії DoS- атака (від англ. «denial-of-service» - атака на відмову в обслуговуванні) [74]. Завданий збиток був настільки серйозним, що Роберт Морріс став першою особою, якій успішно висунули звинувачення згідно із Законом про комп'ютерне шахрайство та зловживання. В результаті була також сформована Команда комп’ютерного реагування на надзвичайні ситуації або скорочено CERT, щоб запобігти повторним проблемам з кібербезпекою.
4. 1990-ті роки – «епоха Файрволів». Коли Інтернет став загальнодоступним, люди все частіше вказували свої персональні дані онлайн. Зловмисники побачили у цьому потенціальне джерело заробітку і почали викрадати дані окремих людей та урядів через мережу. До середини 1990-их років загрози у мережі стали настільки поширеними, що виникла потреба у загальнодоступності антивірусних програм, а також мережевих екранів (брандмауерів, або так званих файрволів). Перший програмний файрвол був розроблений дослідником НАСА у відповідь на вірусну атаку на їхню базу у Каліфорнії. Він створив програму-файрвол за прототипом фізичної стіни, що зупиняє поширення вогню між будівлями у разі пожежі [49].
5. 2000-ні роки – визнання кіберзлочинів кримінальними правопорушеннями [74]. В цей час уряди почали карати хакерство набагато жорскіше, призначивший у вигляді відповдальності великі тюремні терміни і суттєві штрафи. Це було великим кроком порівняно із 1980-ми роками, коли хакерам давали набагато легші покарання – від суворих попереджень до умовного терміну. Інформаційна безпека продовжувала розвиватися в міру експансії Інтернету, але, на жаль, вдосконалювалися і методи зламу. Хакери швидко змогли створити віруси, які націлені не тільки на певні організації, а й на цілі міста, країни і навіть континенти.
6. 2010-ті роки – зростання масштабу кіберзлочинів. Це десятиліття позначилося не просто продовженням розвитку кіберзлочинності та засобів захисту інформації, а особливо гучними справами у галузі кібербезпеки. У 2013 році Едвард Сновден, колишній агент ЦРУ та службовець уряду США, скопіював та розсекретив файли Агентства національної безпеки, що підтверджували факт прослуховування американськими спецслужбами громадян США та збирання даних про них, а також стеження за дипломатичними установами, офісами Європейського союзу та ООН. Інший інцидент пов'язаний із приватною компанією Yahoo, коли хакери вчинили злам, поставивши під загрозу розголошення особистої інформації всіх користувачів системи. Корпорація була оштрафована на 35 мільйонів доларів за невчасне розголошення новин про хакерську атаку, в результаті ціна продажу Yahoo зменшилася на 350 мільйонів доларів. У 2017 році поширився код WannaCry, відомий як перший вірус-вимагач. WannaCry був націлений на комп’ютери під управлінням операційної системи Microsoft Windows і вимагав платежі у криптовалюті Bitcoin. Лише за один день було інфіковано понад 230 000 комп’ютерів у 150 країнах. Особливого розголосу набула ситуація із зараженням комп’ютерів Британської системи охорони здоров’я [48; 49].

Кожен із цих етапів в міру розвитку технології вимагав певного регулювання питань інформаційної безпеки зі сторони держав. На первинних етапах розвитку майже усі проблеми захисту даних цікавили лише державу, адже комп’ютери та комп’ютерні мережі були урядовими, переважно військовими розробками і, відповідно, були пов’язані зі збереженням державної таємниці. В міру розвитку мережі та загроз у ній в держав виникла потреба оберігати не лише державні та комерційні таємниці, а й особисту інформацію громадян від неправомірного її поширення та використання.

Одним із перших суттєвих актів правового регулювання інформаційної безпеки був опублікований в 1983 і згодом повторно виданий в 1985 році Національним центром комп’ютерної безпеки Міністерства оборони США документ «Критерії оцінки достовірності обчислювальних систем Міністерства оборони», або так звана «Оранжева книга» [56]. Він став основою цілю серії стандартів для оцінки довірених систем, що видавалися в 1980-90-их роках.

 У «Оранжевій книзі» було визначено основні положення, згідно яких уряд визначав ступінь захищеності інформаційно-обчислювальних систем. Зокрема, виділено так звані гарантовано захищені обчислювальні системи і виділено сім їх класів, залежно від яких застосовуватися більш складні і суттєві методи і системи захисту [56, с. 11]. Тобто у документі було систематизовано види загроз безпеці інформаційних систем і методи захисту від них. Саме цей документ став основоположним у розробці подальших систем захисту інформації.

«Оранжева книга» ввела таке важливе поняття як ступінь довіри до системи. Безпечна система згідно із документом «здатна керувати доступом до інформації за допомогою відповідних засобів таким чином, що тільки авторизовані особи або процеси, які діють від їх імені, мають право читати, записувати, створювати і видаляти інформацію» [56 с. 9]. Тобто фактично повинна забезпечуватися можливість авторизації, щоб система розрізняла користувачів. На основі авторизації усі дії в системі реєструються від імені певного користувача. Також залежно від наданих рівнів доступу забезпечується здатність конкретного користувача читати, записувати, створювати та видаляти окремі файли. В документі було також описано особливості політики безпеки, яка повинна реалізовуватися через сукупність апаратного і програмного забезпечення. Саме політика безпеки дає можливість оцінити здатність забезпечити конфіденційність, доступність та цілісність інформації.

Хоч зміст Оранжевої книги і став загалом відомим, її юрисдикція (оновлені видання) на сьогодні обмежена лише Сполучними Штатами, в той час як багато країн використовує міжнародний стандарт ISO/IEC 15408 «Загальні критерії оцінки безпеки інформаційних технологій» (англ. Common Criteria for Information Technology Security Evaluation) [64; 65; 66]. Ще у 1990 році Міжнародна організація зі стандартизації ініціювала початок розробки цього стандарту. Через три роки організації США, Канади, Великої Британії, Нідерландів, Франції та Німеччини об’єдналися для розробки цього документа. Завданням проекту була стандартизація оцінки безпеки на міжнародному рівні. У січні 1996 року вперше було видано документ під назвою «Загальні критерії». Протягом другої половини 1990-их років ці «Критерії» переглядалися, доопрацьовувалися, доповнювалися і відповідно перевидавалися. В процесі покращення у червні 1999 року прийнято стандарт ISO/IEC 15408. Після цього процес доопрацювання та покращення стандарту не зупинявся і остання актуальна редакція стандарту була видана в трьох частинах у 2008-2009 роках.

Перша частина «Вступ та Загальна модель» описує загальну концепцію та принципи і загальну модель оцінювання безпеки інформаційних систем. Також у цій частині визначено порядок виявлення об’єктів, що підлягають захисту, вимог до системи інформаційної безпеки та засади написання високоякісних технічних завдань щодо розробки продуктів і систем захисту інформації [64].

Друга частина «Функціональні вимоги безпеки» закріплює комплекс функціональних елементів системи захисту інформації, наявність яких є свідченням дотримання вимог безпеки [65].

Третя частина «Вимоги для забезпечення довіри до систем безпеки» включає систему заходів, які слід вживати на усіх етапах життєвого циклу окремих програм та системи загалом для забезпечення впевненості у тому, що всі вимоги із другої частини цього стандарту виконуються [66].

На сьогодні існує ряд інших міжнародних стандартів, що розроблялися та вдосконалювалися на вимоги нових особливостей інформаційних систем з метою забезпечення їх безпеки, зокрема:

1. Багаточастинний стандарт ISO/IEC 9798 «Інформаційні технології. Методи та засоби забезпечення безпеки. Автентифікація об’єкта» («Information technology. Security techniques. Entity authentication» [68].
2. ISO/IEC 10745:1995 «Інформаційні технології. Взаємозв’язок відкритих систем. Модель захисту інформації верхніх рівнів» («Information technology. Open Systems Interconnection. Upper layers security model») [61].
3. ISO/IEC 11577:1995 «Інформаційні технології. Взаємозв’язок відкритих систем. Протокол захисту інформації на мережевому рівні» («Information technology. Open Systems Interconnection. Network layer security protocol») [62].
4. ІSO/ІEC 10164-7:1992 «Інформаційні технології. Взаємозв’язок відкритих систем. Адміністративне керування системи. Частина 7. Функції повідомлення про порушення інформаційної безпеки» («Information technology. Open Systems Interconnection. Systems Management. Part 7: Security alarm reporting function») [60].
5. ІSO/ІEC 11586 «Інформаційні технології. Взаємозв’язок відкритих систем. Загальні функції захисту верхніх рівнів» («Information technology. Open Systems Interconnection. Generic upper layers security») [63].

Система інформаційної безпеки в органах державного управління України створюється і розвивається відповідно до Конституції України та інших чинних нормативно-правових актів, що регулюють окремі питання інформаційної сфери, зокрема Указ Президента України від 6 травня 2015 року «Про Стратегію національної безпеки України», Указ Президента України від 15 березня 2016 року № 96 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [36], Указ Президента України «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» [37] тощо.

Нормативно-правовими актами визначено національні інтереси та пріоритети України в інформаційній сфері, потенційні загрози національній безпеці України у сфері інформаційних технологій, основні суб’єкти та об’єкти кібербезпеки в Україні, поняття та структуру національної системи кібербезпеки, напрями та шляхи забезпечення кібербезпеки.

Таким чином стає добре зрозуміло, що сучасний стан нормативного регулювання галузі захисту інформації продиктований історичними віхами розвитку інформаційних загроз. Такі загрози розвивалися та поширювалися на країни усього світу, державний та приватний сектори, створюючи ситуацію, коли необхідність законодавчого регулювання стала питанням національної безпеки. Тому на сьогодні питання інформаційної безпеки є чітко врегульованими в тому числі в Україні, проте розвиток загроз інформаційній безпеці не зупиняється, тому нормативне регулювання потрібно оновлювати відповідно до нових ризиків.

**Висновки до розділу 1.**

У результаті дослідження теоретичних та правових засад ми дійшли до наступних висновків.

У підрозділі 1.1 досліджено суть та підходи до розуміння інформаційної безпеки через розуміння її характеристик, властивостей та рівнів. Також проаналізовано основні та додаткові властивості інформації як об’єкта забезпечення безпеки. Було досліджено поняття загрози в галузі інформаційної безпеки, зокрема визначено відмінності між загрозою безпеці інформації та загрозою інформаційній безпеці, наведено приклади кожної із них. Як підсумок, проаналізовано різні методи забезпечення інформаційної безпеки залежно від можливих загроз.

У підрозділі 1.2 проаналізовано взаємозв’язок розвитку загроз у галузі інформаційної безпеки та появу нових технологічних та програмних засобів захисту. Це стимулювало розвиток нормативно-правового регулювання питань інформаційної безпеки та питань оцінки рівня безпеки інформаційної системи, зокрема видання першого керівництва у галузі інформаційної безпеки «Оранжевої книги». Згодом міжнародною організацією з питань стандартизації було розроблено ряд стандартів у цій галузі, які використовуються безпосередньо більшістю країн або є основою для власних національних стандартів. В Україні стан нормативного регулювання інформаційної безпеки на разі оцінюється міжнародними організаціями як задовільний і навіть високий.

# РОЗДІЛ 2

# СУЧАСНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ В ОРГАНАХ ДПС УКРАЇНИ

## 2.1. Класифікація методів захисту інформації

Забезпечення захисту інформації сьогодні досягається комплексом різних методів її захисту відповідно до наявних ризиків, а також рівня чутливості інформації. У вітчизняних та іноземних джерелах ці методи класифікуються із застосуванням різних підходів. Варто також зауважити, що на сьогодні часто окремі проекти і рішення є комплексними, тому їх може бути важко віднести до якоїсь конкретної класифікаційної групи. Наприклад, антивірусне програмне забезпечення може бути використане як для окремого робочого місця, так для мережевого з’єднання типу клієнт-сервер. Водночас, воно ж може використовуватися в різних екосистемах. Тому варто окремо розглянути підходи до класифікації методів захисту інформації, а також класифікацію окремих популярних рішень у галузі захисту інформації. На основі вище викладеного нами виділено наступні класифікаційні ознаки методів захисту інформації (рис. 2.1).

Системи захисту інформації включають програмне забезпечення, що розробляється відповідно до специфічної архітектури. Три основних види архітектури – це окреме робоче місце, мережі типу «клієнт-сервер», а також однорангові мережі. Для першого типу архітектури система захисту інформації встановлена лише на окрему машину. Прикладом таких систем є перші антивірусні програми, де забезпечувалося завдання виявлення загроз на окремих комп’ютерах без обміну даними через мережу.

*Рис. 2.1* **Класифікація методів захисту інформації**

*Джерело:* складено автором

Другий тип систем захисту застосовується для мереж типу «клієнт-сервер». Вони складаються із «клієнтів», що є учасниками мережі, яка підлягає захисту, і централізованого сервера, який виконує алгоритми виявлення загроз. Цей підхід характерний для сучасних антивірусних програм, коли, наприклад, необхідна перевірка доменів, що відвідуються «клієнтами», на предмет зловмисності. «Клієнт» надсилає запит на сервер, а сервер відповідає, чи безпечний домен, на основі наявного «чорного списку». Останній тип мереж (однорангові мережі) застосовується як розподілена мережа, у якій в основі лежать рівноправні клієнти. Системи захисту таких мережах представлені, наприклад, системою сенсорів, які розташовані на різних вузлах (клієнтах) і спільно, комунікуючи між собою, використовують алгоритми для виявлення аномалій чи атак у мережі, яка підлягає захисту.

Методи захисту діють на тих же трьох рівнях, що й потенційні загрози – на рівні апаратного забезпечення, на програмного забезпечення та на рівні мережі. На усіх цих рівнях є два основних підходи до виявлення загроз (види методів захисту за способом виявлення): виявлення аномалій, аналіз протоколів та сигнатур. Спосіб виявлення аномалій полягає у вивченні типових дій користувачів та програмного забезпечення і виявлення на основі цих знань нетипових дій, які можуть виявитися загрозливими. Аналіз протоколів та сигнатур застосовується для попередження вторгнень шляхом виявлення у вхідних пакетах даних сигнатур, що вказують на шкідливий трафік, або виявлення відхилення від очікуваних чи нормальних значень у полях протоколів. Цей метод може бути автоматизованим, коли програмне забезпечення самостійно обирає небезпечні сигнатури на основі типових операцій, або ручним, коли це робить фахівець із безпеки, прописуючи сигнатури, які вказують на шкідливі дії.

Системи та методи захисту також можна класифікувати на основі типу даних, які опрацьовує їхній алгоритм виявлення. Наприклад, мережеві системи виявлення вторгнень аналізують вхідні пакети даних на різних рівнях мережевих протоколів, а хостові системи виявлення вторгнень аналізують, які програми звертаються до яких ресурсів і чи відповідає це моделі нормальної безпечної діяльності [74, c. 36:5]. Ми пропонуємо розділяти дані, які аналізують системи захисту інформації, на так категорії: дані програм, дані файлів та мережеві дані. Перша група включає як системні операції програм, так і дії програм у мережі. При системних запитах деякі програми захисту аналізують лише сам запит (його зміст), а інші досліджують специфічні параметри запиту; аналогічним чином у HTTP протоколах одними системами захисту аналізуються лише заголовки (яка дія має бути виконана: GET, POST тощо), тоді як інші аналізують зміст запиту (які дані мають бути отримані чи записані). Наступна група даних (дані файлів) включає файли, які досліджуються, щоб переконатися, що вони не несуть загроз інформаційній безпеці. Найчастіше це документи Microsoft Office, документи формату PDF, медіа-файли (відео, зображення), файли, що потребують розпакування (EXE). До третьої групи даних (мережеві дані) відносимо інформацію, що міститься у низькорівневих пакетах даних. Технічно ці пакети звертаються до даних на рівнях, що нижчі від рівня програмного забезпечення. Різні механізми захисту перевіряють заголовок і вміст пакета або лише заголовок.

Ще один підхід, який ми можемо використати для класифікації методів захисту, пов'язаний із видом середовища, у якому система захисту може бути використана. Зокрема, системи захисту використовуються у таких основних середовищах: підприємство (організація), мобільні пристрої, «Інтернет речей». Середовище підприємства чи організації представлене типовою організаційною інфраструктурою, що складається із локально з’єднаних мережею комп’ютерів, серверів, мережевих приладів, але також може бути розширена шляхом надання доступу до зовнішніх ресурсів. Середовище мобільних пристроїв складається із особистих пристроїв, що, зазвичай, використовуються будь-де (смартфони, планшети тощо). Інтернет речей як середовище перебуває на стадії зародження, але вже створює суттєві загрози інформаційній безпеці. Сюди, наприклад, можна віднести IP-камери та інформацію, яку вони передають, сенсорні мережі, що синхронізовані із IP-хабами [55].

Окрім цієї доволі суттєвої за змістами класифікації, хочемо звернути увагу також на інші підходи, що дають змогу зрозуміти усі рівні, на яких можливо і необхідно вживати заходів інформаційної безпеки.

Дослідник А. Карачка у своїх роботах згадує класифікацію заходів протидії комп’ютерним злочинам. Серед них є правові, організаційно-адміністративні та інженерно-технічні (рис. 2.2 [18, с. 34-36]).

На нашу думку, в Україні реально застосовуваними методами захисту інформації нарівні організації можна вважати дві останні групи. Це пов’язано із тим, що правове регулювання на сьогодні дає скоріше етично-соціальний, а не прикладний захист.

*Рис 2.2.* **Заходи протидії комп’ютерним злочинам**

*Джерело:* Складено автором на основі наукових публікацій [18, с. 34-36].

Згідно із класифікацією організаційно-адміністративні заходи включають організаційні (налагодження та функціонування пропускного режиму, чіткий регламент зберігання документів, визначений порядок обліку та знищення документів організації, чітке технічне завдання при розробці та створенні мережі, навчання працівників правилам роботи із таємною інформацією) та адміністративні заходи (підтримка правильної конфігурації операційної системи, контроль журналів роботи, контроль частоти зміни паролів, виявлення загроз у системі захисту, проведення регулярних тестувань методів та засобів захисту інформації).

Інша група заходів включає відповідно інженерні та технічні заходи. До інженерних заходів відносять організацію охорони приміщень із комп’ютерами та серверами, наявність сигналізації, захист акустичних каналів, екранізацію приміщень. Технічні заходи передбачають використання фізичних, апаратних, програмних та криптографічних засобів захисту.

Така класифікація, як бачимо, більше дає розуміння того, які саме дії, прилади, заходи дозволяють забезпечити захист та збереження інформації, тоді як перший підхід меншою мірою прив’язаний до прикладних дій та засобів, а більшою мірою до природи та суті конкретних методів. В обох цих підходах чітко зрозуміло, що належний рівень безпеки досягається лише одночасним застосуванням багатьох засобів, тобто при функціонуванні налагодженої системи інформаційної безпеки. В той же час окреме рішення в галузі інформаційної безпеки на сьогодні навряд чи може бути ефективним, якщо не об’єднує у собі різні методи захисту інформації.

Отже, в органах ДПС України активно використовуються різні методи захисту залежно від вимог до збереження конкретного виду інформації. Слід зауважити, що більшість вимог визначаються на загальнодержавному рівні, а не на рівні окремої організації.

## 2.2. Практика застосування методів отримання акустичної інформації

Акустична розвідка реалізується шляхом перехоплення виробничих шумів об'єкту і перехопленням аудіальної інформації. У цілях акустичної розвідки поширеним є використання таких методів:

* пасивні;
* контактні;
* активні.

Також можна групувати технічні засоби збирання акустичної інформації за способом застосування. За цією ознакою виділяють наступні групи засобів [22, с, 112; 43; 17, с. 44-59]:

1. Засоби, які що потребують таємного фізичного проникнення на об'єкт:
* радіозакладки;
* закладки, що здійснюють передачу акустичної інформації в інфрачервоному діапазоні;
* закладки, що здійснюють передавання інформації по мережі 220 В;
* закладки, що здійснюють передавання акустичної інформації по телефонній лінії;
* диктофони;
* провідні мікрофони;
* так зване “телефонне вухо”.
1. Засоби, що встановлюються без проникнення на об’єкт:
* Прилади, що використовують для прослуховування мікрофонний ефект;
* високочастотне нав'язування;
* новітні стетоскопи;
* лазерні стетоскопи;
* направлені мікрофони.

Розглянемо ці методи детальніше, щоб зрозуміти їх механізм дії і можливі засоби захисту.

Перехоплення акустичної інформації за допомогою радіоперетворювальних засобів.До них належить велика кількість радіозакладок (радіомікрофонів, “жучків”), що створені для збирання і передавання акустичної інформації, що звучить на об'єкті.

Застосування радіоперетворювальних засобів, зазвичай, здійснюється в парі із приймачем, за допомогою якого приймається інформація, зібрана радіозакладкою. Залежно від потреб можуть використовуватися побутові приймачі (діапазон 88–108 Мгц) або спеціальні [22, с. 118]. Особливої уваги заслуговують автоматичні станції. Вони здійснюють автоматичний запис інформації, коли вона виникає на об’єкті розвідки.

Перехоплення акустичної інформації за допомогою інфрачервоних передавачів здійснюється, логічно, по інфрачервоному каналу. Для акустичних закладок цього виду властива крайня складність їх виявлення. Такі закладки можуть працювати до кількох діб, що зручно, але водночас, негативною стороною є необхідність використовувати спеціальні приймачі для передавання і прослуховування інформації. При цьому це можливо лише в прямому візуальному контакті із закладкою, тобто потрібно перебувати у безпосередній близькості, що може бути проблематично для збирача інформації. У зв’язку із цим такі закладки, зазвичай, встановлюються біля вікон або біля вентиляційних отворів, що полегшує прослуховування.

Закладки, що здійснюють передавання акустичної інформації мережу 220В і телефонні лінії, працюють на основі технології низькочастотного ущільнення каналу передачі інформації. Оскільки в електропровідних лініях (220В) і телефонних лініях частота сигналів 50 Гц і 300–3500 Гц відповідно, то ця група закладок здійснює передавання інформації, транслюючи її на частотах 100–250 кГц. При цьому не виникає ніяких перешкод у роботі цих мереж. Підключення до ліній з використанням спеціальних приймачів, дозволяє отримувати із закладки інформацію знаходячись на відстані до 500м від об’єкта [22, с. 119].

Принцип роботи наступного виду закладок – диктофонів – добре відомий. Такі пристрої, що записують авдіальну інформацію на магнітний носій (стрічку, внутрішню пам’ять). Час запису залежить від часу автономної роботи пристрою і обсягу внутрішньої пам’яті і, зазвичай, становить до 8 годин.

Сучасні цифрові диктофони не використовують магнітні стрічки, що робить їх практично безшумними, оскільки нема механічного стрічкопротяжного механізму. Окрім того, після вилучення диктофона, таку інформацію легко копіювати на інші носії і опрацьовувати. Зокрема, може знадобитися додаткове підвищення розбірливості мови, усунення фонових шумів тощо.

Ще один дуже зрозумілий засіб – це проводові мікрофони. Вони встановлюються в приміщенні, де здійснюватиметься прослуховування, і з'єднуються проводом із приймальним пристроєм. Встановлені мікрофони приховуються або маскуються під декорації, офісну техніку тощо. Такі системи здійснюють передавання звукового сигналу на дистанції до 20 м. У разі встановлення активних мікрофонів ця відстань може збільшуватися до 150 м. Декілька мікрофонів можуть бути з’єднані із спільним приймальним пристроєм, що дозволяє одночасно стежити за різними приміщеннями. Окрім того приймальні пристрої, зазвичай, також записують усі перехоплені розмови на диктофон.

Для ефективного прослуховування розмов застосовується спеціальний пристрій “телефонне вухо”. Цей прилад таємно встановлюється в телефон, або монтується в телефонну розетку. Механізм дії наступний. Людина, яка здійснює прослуховування за допомогою пристрою (оператор), телефонує на номер телефону, на якому воно встановлене. «Телефонне вухо» спрацьовуючи заглушує перші два дзвінки, тобто в приміщенні, яке прослуховується, ці телефонні дзвінки не лунають. Оператор кладе трубку і ще раз телефонує на цей номер. У трубці звучатимуть короткі гудки (сигнал “зайнято”), далі оператор очікує 30-60 с (часовий пароль) і після припинення сигналу “зайнято” набирає через генератор DTMF-посилок на перед задану числову комбінацію (пароль). Після цього включається мікрофон “телефонного вуха” і оператор чує всі розмови та шуми, що звучать в контрольованому приміщенні. Суттєвою перевагою є відсутність обмежень у відстані, з якої здійснюється прослуховування. Це можливо практично з будь-якої точки світу через лінії телефонного зв’язку. Втім у засобу є й слабкі місця. Зокрема, відбувається розрив зв’язку, якщо хтось у контрольованому приміщенні підніме телефонну трубку. Окрім того, для решти всіх абонентів, які намагатимуться телефонувати по цьому номеру, під час прослуховування завжди лунатиме сигнал “зайнято”, що може викликати підозри. Цей механізм роботи є стандартним, але залежно від потреб може змінюватися. Окрім цього, ще один суттєвий недолік методу полягає в тому, що “мікрофонним ефектом”, необхідним для прослуховування, володіють старі моделі телефонів, які з часом застосовуються все рідше [22, с. 121-122].

Апаратура високочастотного нав'язування працює завдякивисокочастотним коливанням, що проходять через мікрофон або інші елементи телефону, що мають “мікрофонний ефект”. Ці коливання модулюються в акустичний сигнал, що йде із приміщення, яке прослуховується. Змодульованний сигнал демодулюється спеціальним приладом - амплітудним детектором. Після демодульований сигнал фіксується реєструючим пристроєм [22, с. 120]. Цей метод ефективний тим, що у якості мікрофона може слугувати навіть вся будівля. На будівлю направляється випромінювання відповідної частоти, змодельоване спеціальними приладами, які здатні згодом вловлювати та фіксувати, як змінилися звукові коливання через виникнення розмови у будівлі. Тобто прилад аналізує відбите від прослуховуваної будівлі випромінювання, виявляє зміни у ньому, що несуть у собі інформацію про розмови всередині будівлі.

Розглянемо детальніше фізичні процеси та властивості матеріалів, які дозволяють реалізувати такий спосіб акустичної розвідки. Прикладом може слугувати резонанс звичайної телефонної трубки. Звичайний мікрофон має суттєво нижчий опір, ніж телефонний капсуль. Тому можна уявити просту схему, що складається із коротко замкнутої лінії з проводами довжиною Lі прослуховувальною ємністю С (рис. 2.3)[22, c. 120].



*Рис. 2.3.* **Схематичне зображення телефонної трубки**

*Джерело:* складено автором на основі наукових публікацій [22, c.120]

Необхідний резонанс виникає при виконанні умови рівності нулю суми опорів ємності Сі вхідного опору лінії. Основний резонанс має місце при частоті . Розрахувати цю резонансну частоту можна за умови, що відома довжина дроту між мікрофоном і телефоном в телефонній трубці.

Струм на мікрофоні зростає і стає найвищий тоді, коли напруга зменшується і прямує до нуля, що видно на рис. 2.4. Струм проходить через мікрофон і модулюється за законом низької частоти. Зважаючи на те, що лінія в трубці може мати природні дефекти, основна частина енергії трансформується в електромагнітні коливання і випромінюється.



*Рис. 2.4.* **Взаємна залежність струму і напруги на мікрофоні**

*Джерело:* складено автором на основі наукових публікацій [22, c.120]

Звернемо увагу також на процес збудження коливань, що виникає в резонансній системі (в нашому випадку це та ж телефонна трубка) на частоті Процес збудження починається при опромінюванні цієї резонансної системи на частоті зовнішнім джерелом високочастотного сигналу (рис. 2.5). Виходячи з цього, можна зробити висновок про те, що найбільша потужність наведеного сигналу досягається у разі паралельного розташування телефонної трубки і передаючої антени. І навпаки - якщо вони розташовані під кутом відносно один до одного ЕРС зменшується [22, c.121].



*Рис.2.5.* **Випромінювання модульованого сигналу**

*Джерело:* складено автором на основі наукових публікацій [22, c.121]

Як ми вже зазначали, наведений сигнал модулюється по амплітуді і випромінюється в ефір на тій же резонансній частоті, але оскільки цей сигнал, що значно слабше опромінюється ВЧ сигналом на резонансній частоті, то і коефіцієнт модуляції по відношенню до частоти модуляції стає дуже малим.

Для нормального прийому необхідно, щоб коефіцієнт модуляції був рівний 30%. При потужності генератора на частоті 370 МГц рівною 40 мкВт вдається добитися впевненого прийому на відстані близько 100м. Виявилось, що на дальність прийому дуже сильно впливає відстань телефонного апарату від землі. Чим ближче він розташований до землі, тим більше поглинання електромагнітного поля. У розглянутому прикладі процес модуляції відбувається за рахунок зміни опору мікрофону телефонного апарату [17, с. 40-41].

При опромінюванні проводів, ліній зв'язку і т.п., що несуть аналогову або цифрову інформацію при значенні, що описане формулою 2.1, модуляція з опромінюючим сигналом відбувається легше, ніж у випадку з мікрофоном телефонного апарату.

 (2.1)

Таким чином, знімання вербальної інформації при опромінюванні, наприклад, персонального комп'ютера на великій відстані стає реальністю.

У всіх технічних засобах встановлені певні фізичні перетворювачі, що виконують свої функції, на основі певних фізичних законів і принципів дії. Наявність знань про різні типи перетворювачів дає можливість зрозуміти, які саме неконтрольовані прояви фізичних полів цих приладів створюють канали витоку інформації і дозволяють проводити акустичну розвідку.

Перетворювач – це будь-який прилад, який трансформує зміну однієї фізичної величини в зміну іншої. Мовою електроніки перетворювачем називають як прилад, що перетворює неелектричну величину на електричний сигнал, так і прилад, що діє у зворотному напрямку.

Функції приладів і електронних пристроїв можна розділити на два основні види – обробка електричних сигналів і перетворення якої-небудь зовнішньої фізичної дії в електричні сигнали. Нас більше цікавлять прилади другого типу, оскільки саме у цьому випадку основну роль виконують датчики і перетворювачі.

Великий обсяг проявів навколишнього світу включає чимало різних фізичних явищ, окрім електричних сигналів. Сюди можна віднести звук, світло, температуру, тиск, магнітні поля, рух тощо. Перетворення інформації про ці та інші фізичні явища на електричний сигнал в електронних приладах забезпечують чутливі елементи – датчики. Вони є вхідною точкою для інформації у будь-яких електронних приладах і відіграючи роль генератора електричного сигналу.

За походженням можна виділити два види датчиків:

* ті, які були спеціально розроблені для вловлення певного явища та створення необхідного електричного сигналу, що фіксуватиме його;
* випадкові, які стали результатом недосконалості схеми або пристрою.

Інша класифікаційна ознака - за формою перетворення – поділяє датчики таким чином:

* перетворювачі сигналу;
* перетворювачі енергії.

На перетворювач впливають певні сили, що провокують його реакцію (перетворення). Будь-який перетворювач характеризується певними параметрами. Найбільш важливими з них є:

* чутливість до появи, зміни, зникнення сигналу на його вході;
* роздільна здатність, що характеризує те, із якою точністю, з якою точністю здійснюється перетворення;
* лінійність визначає ступінь рівномірності зміни вихідного сигналу в залежно від того, як змінюється вхідний;
* інертність, або час відклику, визначає, як швидко генерується зміна вихідного сигналу в результаті зміни вхідного.
* смуга частот показує, на яких частотах перетворювач здатен розпізнати вхідний сигнал, створивши при цьому на виході допустимий для приладу рівень сигналу [19].

Отже, перетворювачі класифікують по фізичній природі на такі групи, як фотоелектричні, термоелектричні, п'єзоелектричні, електромагнітні і акусто-електричні перетворювачі. Різні види з них поширені сучасних системах управління і обробки інформації.

Таким чином лише засобів перехоплення акустичної інформації є чимало. Усі вони потенційно можуть бути використані зловмисниками для викрадення інформації. Система захисту інформації повинна усі їх передбачати і вживати заходів для попередження та уникнення потенційних витоків.

## 2.3. Програмний захист інформації як невід’ємна складова збереження цілісності інформації в органах ДПС України

У попередніх підрозділах ми акцентували увагу на тому, що ефективна система захисту інформації включає в себе різні види методів захисту інформації, які використовуються в різних поєднаннях залежно від загроз і потреб організації. Серед них дуже вагому роль відіграють програмні методи, оскільки їх роль є провідною у майже всіх сферах людської діяльності, коли йде мова про захист інформації.

З метою розуміння важливості збереження цілісності інформації та методів, що слід застосовувати, важливо проаналізувати саме поняття цілісності даних. Цілісність – це дуже широке поняття, яке має різний контекст залежно від галузі комп’ютерних наук. Коли мова йде про безпеку даних під цілісністю, зазвичай, розуміють збереження даних у тому вигляді, у якому вони були створені (відсутність перекручень, випадкових змін, змін, що викликані шахрайськими діями) [78, c 35-36]. У теорії баз даних під достовірністю прийнято вважати забезпечення точності і повноти даних протягом усього життєвого циклу бази [59, с. 60]. Тобто усі дії спрямовані на захист інформації від несанкціонованого доступу та змін можна вважати захистом цілісності інформації.

Під час передавання чи отримання даних у мережі Інтернет основним засобом захисту інформації є міжмережеві екрани, або фаєрволи (англ. «firewalls»). Для організацій, які надають своїм працівникам доступ до глобальної мережі – це ключовий елемент захисту від загроз, що надходять із мережі. Фаєрволи здійснюють управління як вхідним, так і вихідним мережевим трафіком. Міжмережевий екран дає можливість створити профіль кожного користувача і налаштувати у ному рівень доступу користувача до мережі Інтернет. Водночас в цьому ж профілі можна налаштувати доступність користувача для будь-яких засобів, що намагатимуться взаємодіяти із ним через мережу, обмеживши підозрілі алгоритми або повністю заборонивши взаємодію із певними видами файлів, сайтів тощо. З точки зору збереження конфіденційної інформації міжмережевий екран також дозволяє заблокувати передавання певного визначеного виду трафіку та виконати перевірку трафіку перед його передачею. Належне налаштування параметрів міжмережевого екрану дає можливість уникнути значної частини сучасних загроз інформаційній безпеці, що походять із мережі [7, с. 56].

Фаєрволи розроблені для захисту протоколів і програмних засобів. Вони контролюють доступ Інтернету до внутрішньої мережі організації, робочих місць окремих користувачів тощо на основі аналізу змісту та походження даних, що циркулюють між двома мережами.

Фаєрволи за своєю суттю є програмними маршрутизаторами, тобто здійснюють фільтрацію вхідних та вихідних мережевих пакетів, оцінюючи за визначеними критеріями, чи можна передавати пакет даних. Якщо між мережевий екран визначив, що пакет можна передавати, то надалі він також відстежує аби пакет був переданий за визначеним маршрутом. Щоб робота Фаєрвола була ефективною, важливо правильно налаштувати та підібрати правила фільтрації. Тобто, Фаєрвол є умовним віртуальним кордоном, котрий здійснює контроль над передаванням пакетів даних, визначає відповідність заданим вимогам.

Комп’ютерні мережі великих організацій зазвичай функціонують на великій відстані, зв'язуючи велику кількість об’єктів, що розміщенні в різних частинах міста, області, країни та по всьому світі. Тому ще одним актуальним засобом захисту інформації є захист мережевого рівня ІР-мереж (тобто захист мереж, з яких складається Інтернет). Світові розробники Фаєрволів і маршрутизаторів захисту інформації створили технологію Structured Wireless Aware Network. Її суть полягає у запровадженні тестування протоколів, які використовуються у мережі, як засоби захисту трафіку даних. Дані протоколи здійснюють автентифікацію та криптографічне шифрування пакетів даних. Новітні протоколи зможуть дати можливість комплексно використовувати маршрутизаторами та брандмауерами різних компаній. Це в свою чергу забезпечить можливість територіальним управлінням однієї організації розміщеним в різних містах країни, а також організаціям, що з ними співпрацюють в межах спільного інформаційного поля безпечно обмінюватися даними в мережі. Тобто, організації мають можливість створювати власні віртуальні приватні мережі (virtual private networks, VPN) та використовувати глобальну мережу, як ще один засіб зв’язку [7, с.89]. Віртуальні приватні мережі (virtual private networks, VPN) – розділенні організаційні, корпоративні, приватні мережі, котрі здійснюють зв'язку між собою за допомогою глобальної мережі. Але Фаєрволи не дають можливість усунути всі загрози інформаційній безпеці, що походять глобальної мережі Інтернет. Зокрема, вони не можуть захистити від комп’ютерних вірусів, а також не мають інструментів для забезпечення цілісності даних [13, c.66].

Віртуальні приватні мережі VPN – це вбудовані віртуальні мережі, що забезпечують захист інформації у мережі, в цілому, її частин та кожного користувача зокрема. Це реалізується завдяки застосуванню захищеного TCP/IP трафіку, захисту окремих станцій, використання серверів глобальної мережі, баз даних, автоматичного опрацювання транзакцій, що пов’язані із проведенням фінансових та банківських операцій за допомогою платіжних систем. Основним апаратно-програмним рішенням для забезпечення функціонування приватних віртуальних мереж є VPN-шлюзи. Найважливішими функціями VPN-шлюзів є наступні: автентифікація користувачів, шифрування даних, передавання пакетів даних через закриті захищені з’єднання [13, c.66; 56, с. 59-60]. Часто VPN-шлюзи мають також вбудований механізм Фаєрвол.

Ще одним важливим елементом систем захисту інформації при роботі за комп’ютерами з підключенням до глобальної мережі є використання антивірусних засобів. Це дає можливість суттєво знизити ймовірність інфікування комп’ютерів та пошкодження або втрати інформації внаслідок цього.

Антивірусне програмне забезпечення здійснює перевірку вхідного трафіку, виявляючи та нейтралізуючи комп’ютерні віруси [7, с,122]. Вірус – це програмне забезпечення, котре пошкоджує, змінює або знищує інші програми, дані тощо. В аспекті захисту інформації під вірусами зазвичай розуміють умисно створені програми з наміром завдати шкоди чи викрасти інформацію. Зазвичай віруси автоматично копіюються під час здійснення з’єднання чи запуску завантаженої програми. Окрім того, деякі види вірусів можуть себе проявляти не автоматично, а лише за настання певної події у системі.

Спеціальні види антивірусів розроблені для попередження загроз, що надходять з глобальної мережі. Це так звані мережеві антивіруси. Вони забезпечують захист протоколів, локальних комп’ютерних мереж, а також є ефективними при роботі з електронною поштою [29, с. 110]. Мережеві антивіруси здійснюють регулярну перевірку мережі на предмет можливих загроз, а також сканують корпоративні сервери з метою виявлення потенційних загроз. Це суттєво знижує ймовірність вдалих кібератак на мережу загалом.

В органах ДПС України використовується програмні продукти антивірусного захисту інформації виключно згідно з чинним експертними висновками Державної служби спеціального зв’язку та захисту інформації України. Оновлення даних програмних продуктів антивірусного захисту інформації здійснюється щоденно, з використанням веб-ресурсів Центру антивірусного захисту інформації.

Для побудови віртуальних з’єднань в органах ДПС України використовується система технічних та програмних рішень для захисту з’єднань «ІІТ Захист з’єднань». Це дає змогу без втрати даних та стороннього втручання пересилати та обробляти великі об’єми даних. Він був розроблений акціонерним товариством «Інститутом інформаційних технологій» для досягнення цілісності, захищеності та повноти інформації, яка надсилається мережею між користувачами. До зазначеного технічного рішення належать шлюзи для забезпечення захищених з’єднань (апаратні або програмні засоби) з можливістю дистанційного управління, робочі станції адміністраторів, програмні засоби агентів моніторингу, програмні засоби для оперативного моніторингу, власне програмне забезпечення «ІІТ Захист з’єднань. Клієнт», проксі-клієнти, програмні засоби моніторингу проксі для адміністраторів та комплекси віртуальних мереж типу шлюз-клієнт.

Детально розглянемо кожен компонент, що входить до цього пакету рішень. Шлюз захисту розроблений для забезпечення цілісності та захисту сервера, а також забезпечує передавання даних як захищеними, так і відкритими з’єднаннями, здійснює шифрування та розшифрування пакетів даних, що надсилаються від сервера до клієнта і навпаки. Шлюз включає в себе програмну частину, яка інсталюється лише на сервер мережі, яка потребує захисту. Робоча станція адміністратора з віддаленим доступом забезпечує керування шлюзами, налагодження конфігурації шлюзу, отримування технічної інформації про стан шлюзу, завантаження основних даних у шлюз. Агент моніторингу розроблений тільки для збирання та збереження статистичних даних від шлюзу, а монітор шлюзів створений для відправки цих даних до відповідальної особи та сповіщає при виявленні збоїв чи при виявленні несанкціонованого доступу до шлюзу. Програмне забезпечення «ІІТ Захист з’єднань. Клієнт» призначене для автентифікації користувача на робочій станції, побудови захищеного з’єднання з шлюзом захисту, зашифрування/розшифрування ключових даних при обробці з сервера. Проксі-клієнти захисту – це програмні продукти, які встановлюються на робочі станції організації з метою перенаправлення даних через відповідні проксі та у захищеному вигляді повертає їх до сервера. Відповідно програмні засоби агентів моніторингу проксі розроблені для збирання та збереження результатів роботи проксі захисту.

З’єднання між територіальними управліннями та центральним органом ДПС України здійснюється наступним чином:

1) працівник організації здійснює автентифікацію у певному необхідному шлюзі захисту органів ДПС;

2) шлюз органів ДПС перевіряє правильність даних для автентифікації та в разі підтвердження логування користувача створює захищене з’єднання між робочою станцією та відповідним сервером;

3) працівник організації за допомогою захищеного шлюзу ініціює шифрування даних залежно від потреб та звернень користувачів для їх захищеного надсилання між робочою станцією та сервером;

4) програмне забезпечення «ІІТ Захист з’єднань. Клієнт» проводить шифрування даних згідно ініційованих завдань від користувачів та розшифровує дані, які необхідно надіслати від сервера до шлюзу.

5) коли робоча сесія закінчується, сервер синхронізує усі дані отриманні від всіх працівників організацій протягом сесії.

Слід зазначити, що зазначені віртуальні з’єднання також можуть працювати з електронними ключами «Кристал-1» та «Алмаз-1К» розробленими АТ «Інститут інформаційних технологій». Дані електронні ключі розроблені у вигляді знімного USB-пристрою з програмним інтерфейсом. Швидкість створення електронних цифрових підписів у даних пристроях 100мс. Апаратна частина розроблена таким чином, що усі криптографічні перетворення захищені та не доступні для шкідливих програмних чи апаратних засобів. Ключі працівників організації створюються, зберігаються, використовуються та знищуються лише у середині апаратного пристрою та жодним чином не потравляють за його межі. У разі втрати апаратного персонального ключа або заволодінням ним іншими особами при введені не вірного паролю, персональний електронний цифровий підпис знищується без можливості його відновлення. В Головному управлінні ДПС у Тернопільській області та у інших територіальних управліннях всі з’єднання відбуваються виключно з використанням електронних ключів.

В органах ДПС України використовуються системи обмеження доступу працівників до глобальної мережі, новітні маршрутизатори CISCO та послуги надання Internet здійснюють виключено компанії, котрі забезпечують захист інформації під час передачі даних.

Для захисту інформації між територіальними органами та центральним органом використовується шифрування. В майбутньому в Головному управлінні ДПС у Тернопільській області та у всіх інших територіальних управліннях планується використання мережних криптомодулів на зразок «Гряда-301». Цей засіб дозволяє генерувати особисті та відкриті ключі для алгоритму електронного цифрового підпису, зберігати їх у своїй пам’яті та захищати від несанкціонованого доступу. Даний мережний криптомодуль має два мережевих інтерфейси для підключення до глобальної мережі з роздільною здатністю 10/100/1000. Генерація ключових даних здійснюється згідно правил генерації даних, які погодженні з Адміністрацією державної служби спеціального зв'язку та захисту інформації України. Також слід відзначити швидкодію даного криптомодуля, яка досягає формування одного електронного цифрового підпису протягом 0,32мс, а при навантажені може сформувати до 3100 електронних цифрових підписів за одну секунду. В даному криптомодулю використовується алгоритм криптографічного шифрування та ключ до нього.

Алгоритм криптографічного шифрування – це математична функція, яка перетворює за визначеними алгоритмом (ключем) відкритий текст на ланцюжок цифр і букв так, щоб цю інформацію не могли зрозуміти сторонні користувачі чи злочинці без використання ключа. Основними перевагами криптографічного шифрування з використанням ключа є:

а) розробка алгоритму криптографічного шифрування займає витрату величезних ресурсів та часу, тому один і той самий алгоритм можна використовувати для всіх територіальних управлінь та центрального органу ДПС України. Обов’язковою умовою є створення для кожного працівника організації нового ключа.

б) навіть, якщо перехопити зашифровану інформацію, то для відновлення та продовження роботи системи, можна лише створити нові ключі. Створювати новий алгоритм криптографічного шифрування не потрібно. [18, с. 47].

У сучасному світі криптографічні алгоритми шифрування можна подіти на симетричні та асиметричні. Симетричні методи використовуються організаціями, компаніями, де є великий об’єм даних. Даний метод забезпечує надзвичайне швидке шифрування/розшифрування даних. Секрет даного методу полягає у використанні одного і того самого ключа у робочій станції працівника та серверу. Органи ДПС України для передачі ключів між територіальними управліннями здійснюється за допомогою відділів та управлінь урядового фельд’єгерського зв’язку Держспецзв’язку. Асиметричні методи використовують організації, компанії, де об’єм даних для передачі є незначним.

На основі криптографічних алгоритмів шифрування створено чимало протоколів для забезпечення високого рівня захищеності операцій у глобальній мережі. Тобто насправді думка про те, що глобальна мережа несе чимало ризиків через його децентралізацію, не є цілком правильною, адже використання відповідних протоколів на усіх рівнях мережі дозволяє належним чином захистити, як окремі пакети даних, так і комплексні, об’ємні дані.

Створено новий засіб для здійснення електронних платежів. Він полягає в моментальній автентифікацію користувача та забезпечені захисту фінансової інформації в глобальній мережі. Протокол Seсure Sockets Layer дозволяє здійснити захист інформації на канальному рівні. А протокол Secure Electronic Transaction, який був розроблений основними компаніями платіжним систем, забезпечує збереження виключно фінансової інформації. Оскільки в глобальній мережі працюють одночасно мільйони користувачів, то дані протоколи розроблялися з метою забезпечення збереження даних для всіх учасників процесу [18, c. 70-71].

У програмних засобах, веб-сторінках чи додатках розроблених з використанням алгоритму Secure Electronic Transaction, користувач має дані про замовлення, а банк не знаючи замовлення, має всю іншу інформацію про транзакцію.

В органах ДПС України доступ до електронних документів здійснюється за допомогою перевірки персональних електронно-цифрових підписів. Система в автоматичному режимі перевіряє, чи при відправці ключа він не зазнав змін. Якщо перевірка пройшла успішно, то працівник організації отримує доступ до відповідної інформації. Також електронний цифрових підпис не тільки дає доступ до інформації, але і перевіряє її цілісність. Дана процедура надзвичайно схожа на процедуру шифрування в асиметричному шифруванні, єдиною відмінністю служить те, що закритий ключ здійснює шифрування, а відкритий розшифрування [32; 18, с, 71-72].

Процедура використання алгоритму електронного цифрового підпису виглядає таким чином:

1) створюються декілька ключів (відкритий та закритий);

2) відкритий ключ направляється (засобами глобальної мережі, поштою, при особистій зустрічі тощо) іншій стороні;

3) власник інформації шифрує дані за допомогою іншого (закритого) ключа та направляє їх засобами зв’язку;

4) одержувач даних розшифровує їх за допомогою відкритого ключа, який отримав раніше від власника інформації.

Програмне забезпечення може бути об’єктом атак зловмисників у зв’язку із наявністю в нього слабких місць. Зазвичай, вони пов’язані з особливостями проектування систем або з особливостями використання програмного забезпечення і його налаштувань (вразливості реалізації).

Вразливості реалізації, зазвичай, набагато більш поширені, оскільки розробники при проектуванні намагається зменшити кількість можливих слабких місць з метою досягнення високої успішної продукту. В той же час адміністратори та користувачі програмного забезпечення не завжди мають доступ до інформації про всі особливості продукту, щоб налаштувати і використовувати його найбільш безпечним та ефективним чином.

Втім вплив усіх цих загроз можна знизити або повністю нівелювати шляхом застосування відповідних засобів захисту. Для того щоб розуміти, які засоби будуть ефективними у різних ситуаціях потрібно розуміти, які елементи та рівні включає в себе інформаційна система. Зазвичай, дослідники виділяють чотири рівні інформаційних систем. Найнижчий рівень (перший) включає в себе операційну систему, яка в свою чергу обслуговує програмне забезпечення та бази даних. Другий рівень забезпечує ефективне функціонування мережі, тобто являє собою актуальну конфігурацію мережевого обладнання. Сюди, наприклад можна віднести застосування протоколу TCP/IP.

Забезпечення захисту інформації на цих рівнях реалізується шляхом ідентифікації та не допущення сторонніх осіб, а також мережевих атак типу DDoS (англ. «Distributed Denial-of-service»). Зокрема, для цього використовуються Фаєрволи та коректно налаштовані маршрутизатори. На рівні окремного робочого місця для не допущення сторонніх осіб обов’язковою має бути автентифікація користувачів операційної системи за паролем. Дана система реалізована в органах ДПС України.

Третій рівень включає в себе сертифіковане прикладне програмне забезпечення, що використовується для реалізації функцій організацій. Поширеними у практично всіх державних установах програмами цього рівня є:

* Microsoft Word;
* Microsoft Excel;
* Microsoft Outlook;
* браузери Google Chrome та Mozilla Firefox.

На цьому рівні важливо використовувати автентифікацію користувачів із визначеним обмеженим доступом до відповідних програм, а також обмеження можливості встановлення стороннього несертифікованого програмного забезпечення.

Четвертий рівень системи управління базами даних (СУБД) забезпечує внесення, зберігання, опрацювання та передачу даних в межах інформаційної системи. Найпоширенішими типами баз даних, які використовуються в органах державного управління, є Oracle, MS SQL Server, MS Access. Цей рівень потребує як програмного, так і організаційного компоненту захисту інформації, які в цьому випадку безпосередньо пов’язані. Ключовими засобами захисту СУБД є необхідність використання паролю (із вимогою про рівень його складності, регулярної заміни тощо); розподілення прав доступу до окремих елементів чи модулів бази даних відповідно до погоджених прав для конкретного користувача; застосування шифрування та криптографічного захисту інформації, що міститься у базі даних.

Таким чином комплексна система захисту повинна бути створена на усіх інформаційно-телекомунікаційних системах органів ДПС. В протилежному випадку злочинці зможуть знайти слабкі сторони системи та завдати збитків у вигляді пошкодження або втрати інформації держави. Це у свою чергу може бути загрозою навіть національній безпеці країни.

# Висновки до розділу 2.

У результаті дослідження сучасних методів захисту інформації в органах ДПС України ми дійшли до наступних висновків.

У підрозділі 2.1 на основі аналізу підходів інших дослідників розроблено власний підхід до класифікації засобів захисту, що максимально враховує багатогранність, комплексність і складність сучасних інформацій мереж. Також на основі дослідження підходів інших авторів зроблено висновок, що сьогодні теоретична база дослідження способів класифікації методів захисту інформації досить широка і може служити основою для формування стратегії захисту інформації. Але в межах ДПС як елементу уряду більшість методів захисту визначені на перед законодавчо і локально не можуть бути змінені.

У підрозділі 2.2 досліджено одні із найбільш ймовірних для органів ДПС на сьогодні каналів витоку інформації – акустичний та віброакустичний. В цій частині роботи детально проаналізовано основні методи отримання акустичної інформації, засоби, які для цього використовуються, умови, коли вони можуть бути застосовані, а також їхні слабкі сторони. У секторі державного управління саме така інформація має особливу цінність, оскільки вона може бути на пряму пов’язана із людиною, яка її сказала, а також емоційним ставленням до цієї інформації. Таке потенційне джерело витоку інформації потребує особливої уваги, тому засоби захисту аудіальної інформації мають бути важливим елементом системи захисту інформації.

У підрозділі 2.3 розкрито результати дослідження особливостей програмного захисту інформації, яка зберігається, опрацьовується та передається у цифровому вигляді органами ДПС. Нами проаналізовано засоби забезпечення збереження інформації як в локальних мережах, так і в мережах із доступом до глобальної мережі. Також охарактеризовано протоколи, які реалізовують ефективний захист інформації при користуванні електронною поштою, здійсненні оплат в мережі, погодженні документів (електронний цифоровий підпис). Окрім того визначено, які засоби програмного захисту ефективні на різних рівнях інформаційної системи і наскільки вони здатні захистити систему від зовнішніх загроз.

# РОЗДІЛ 3

# Перспективні напрями вдосконалення методів захисту інформації в органах ДПС України

**3.1. Напрями підвищення ефективності використання систем зашумлення**

Дія інформативного акустичного сигналу на різні будівельні несучі конструкції, що підлягають захисту, приводить до появи в них вібраційних механічних коливань. Прийом інформативних вібраційних сигналів відбувається на фоні шумів, що мають природне або штучне походження, або сумарних. Якщо природні шумові сигнали не унеможливлюють прийом інформативного сигналу, то подібний небезпечний інформативний сигнал може бути пригнічений за рахунок створення на несучих конструкціях, спеціальних шумоподібних і мовоподібних сигналів [1, с. 24].

При придушенні інформативного вібраційного сигналу можуть бути досягнуті різні ступені захисту:

* мінімальний ступінь захисту, коли навіть при багатократному прослуховуванні фонограми неможливо відновити сенс повідомлення;
* максимальний ступінь захисту, коли неможливо встановити сам факт проведення бесіди або наявності мови в сигналі.

Мінімальний ступінь захисту досягається при перевищенні рівня інтенсивності шуму над рівнем сигналу у всьому частотному діапазоні при дотриманні співвідношення сигнал/шум мінус 10 дБ.

Максимальний ступінь захисту досягається, коли в кожній третьооктавній смузі мовного сигналу співвідношення сигнал/шум складає мінус 20 дБ [1, c.25].

Подібні вимоги по придушенню інформативного сигналу можуть бути забезпечені при оптимальній побудові електроакустичних перетворювачів систем зашумлення, вибору виду переважаючого шумового сигналу і його потужності.

Електроакустичні перетворювачі перетворюють електричну енергію шумового сигналу в енергію пружних коливань, що діють на несучу конструкцію. Подібні перетворювачі повинні мати широку смугу частот (відповідно смузі мовного сигналу) і тому питання узгодження параметрів таких перетворювачів з середовищем несучої конструкції, має велике значення.

У пропонованих на сучасному ринку системах зашумлення використовуються електромагнітні і п'єзоелектричні випромінювачі.

При виборі типу випромінювача необхідно враховувати вид конструкції, що захищається. Так, наприклад, при збудженні конструкцій, що мають високий акустичний опір (цегляні стіни, бетонні перекриття) узгодження в широкому частотному діапазоні, краще здійснюється з пристроями, що мають високий механічний імпеданс рухомої системи (п'єзоелектричнs перетворювачі).

Аналізуючи можливі варіанти використання як п'єзоелектричних, так і електромеханічних випромінювачів, приходимо до висновку:

а) по п'єзоелектричних датчиках:

- п’єзоелектрики володіють яскраво вираженими резонансними властивостями, отже необхідне достатньо складне коректування амплітудно-частотної характеристики (АЧХ) підсилювачів;

- маса рухомої системи, при використанні п’єзоелектриків , відносно мала, що знижує ефективність датчиків в області низьких частот (менше 200 Гц):

* п'єзоелектричні пластини мають великий технологічний розкид параметрів АЧХ (особливо на частотах основних резонансів), що ще більш ускладнює корекцію підсилювачів, що працюють на них;
* неможливо створити п'єзоелектричний давач з потрібними параметрами за прийнятну ціну на основі однієї пластини.

б) по електромеханічних датчиках:

* електромагнітні датчики володіють достатньо великою масою для ефективної роботи з великими поверхнями;
* число власних резонансів у електромагнітного датчика менше, ніж у п'єзоелектричного, а їх АЧХ має більш гладкий вигляд, що спрощує корекцію АЧХ підсилювача;
* необхідні параметри електромагнітного датчика підібрати простіше через його конструктивні і технологічні особливості;
* надійність електромеханічних датчиків дещо нижча.

В результаті подібних порівняльних досліджень в роботі з побудови комплексної системи захисту акустичної інформації застосовуються електромеханічні випромінювачі, в яких використання рідкоземельних магнітів, дозволило зробити пристрої компактними і за прийнятною ціною.

При вирішенні задач активного захисту приміщень необхідно враховувати, що при роботі давачів створюється певний дискомфорт в приміщенні, через "паразитні" випромінювання давача, які викликаються:

а) випромінювачем шумових сигналів;

б) перевипромінюються вібруючою конструкцією в повітря у вигляді акустичних коливань.

Таким чином встановлення ряду зашумлювальних систем, без урахування особливостей "паразитних" акустичних випромінювань може істотно збільшити шумовий фон в приміщенні, що захищається і створювати дискомфортні умови для персоналу, що працює в цих умовах.

Це пов’язано із наступними факторами:

а) чим більше амплітуда власних коливань вібратора, тим вище рівень створюваних ним паразитних шумів

б) п'єзокерамічні випромінювач має менший рівень паразитних акустичних шумів (при рівній величині вібраційних коливань).

З можливих способів усунення впливу "паразитних" шумів можна відзначити наступне:

а) розташовувати вібровипромінювачі не на поверхні стін, а в спеціальних нішах в стінах;

б) розташовувати датчики на вікнах із зовнішнього боку рами, що дозволить зменшити рівень акустичних паразитних коливань в приміщенні за рахунок акустичного захисту внутрішньої рами (скла);

в) при використанні підвісної стелі розміщувати випромінювач вище підвісної стелі (наприклад, в нішах основної стелі); [3]

Для забезпечення якісного кріплення вібродатчика до поверхні, що гарантує необхідне зашумлення останньою, використовуються різні види кріплень.

Для забезпечення оперативної установки можуть бути використані системи із забезпеченням щільного притиску вібродатчиків до зашумляючої конструкцій. Прикладом є мобільні системи віброакустичного зашумления ANG-2000. У цих системах використовується генератор ANG-2000, кріплення вібродатчиків якого (TRN-2000 і TRN-2000m) здійснюється за допомогою спеціальних металоконструкцій, що входять до складу системи. Система ANG-2000 забезпечує захист приміщенню площею до 25м2 і висотою від 2 до 3,75м.

Системи призначені для оперативного встановлення в тимчасово використовуваних приміщеннях і подальшого демонтажу без пошкодження будівельних конструкцій і елементів обробки приміщення [14].

Дійсний рівень шуму, потрібний для гарантованого захисту можливого структурного каналу витоку інформації залежить від розміру площі конструкції що зашумляється, її структури, зовнішнього шуму і максимальної гучності маскованої розмови.

На конструкціях, що захищаються (стіни, двері, вікна), величина наведеного вібраційного інформативного сигналу при однаковій потужності повітряного сигналу виходить різною і тому для виконання вимог гарантованого придушення інформативного сигналу потрібна різна потужність шумового сигналу. У реальних схемах цього досягають шляхом:

1. Установки розроблених спеціально для конкретних поверхонь вібровипромінювачів – для стін, вікон, для інженерних конструкцій. Наприклад, для кріплення на стіни, стелю і систему опалювання - вібраційний випромінювач "Базальт-4ДВМ" або OMS-2000 для кріплення на раму [11], на скло - вібраційний випромінювач "Копійка" або КВП-7.
2. Встановлення необхідних поділок на шкалі напруги вхідного генератора, з урахуванням схем з'єднання датчиків. Залежно від схеми підключення вібродатчиків, вони поділяються на повнорівневі, 1/2-рівневі, 1/3-рівневі. Наприклад, в інструкції на систему ANG-2000 даються рекомендації по установці для повнорівневих датчиків, встановлених на дерев'яній поверхні або стіні сухої кладки, 2/3 рівневих датчиків, встановлених на склі [14].

Задача вирівнювання рівня зашумляючого сигналу у всій смузі частот може бути вирішена при включенні в генератор еквалайзера, що дозволяє проводити підстроювання системи зашумлення по певних ділянках частот і отримувати зашумляючий сигнал близький до потрібного, що не приводить до створення паразитних сигналів в приміщенні.

Послідовне з'єднання рекомендується для скла. Не рекомендується підключати більш 3-х випромінювачів, оскільки рівень сигналу буде низьким.

Паралельне з'єднання рекомендується для стін, підлоги і стель. Не рекомендується підключати більше 4-х випромінювачів паралельно, оскільки опір буде дуже малий, що може привести до виходу генератора з ладу.

Як один з нових напрямів в створенні систем віброакустичного захисту слід зазначити створення акустичних випромінювачів з вбудованим некорельованим цифровим генератором синтезованого мовоподібного шуму [45, c.238]. Такі пристрої добре підходять для організації віброакустичного захисту невеликих приміщень, а також при оперативному усуненні локальних зон витоку мовної інформації. Випромінювач для роботи вимагає тільки живлення постійного струму 12В. Електромагнітній перетворювач виробу забезпечує нерівномірність АЧХ (не більш +10 дБ) в діапазоні робочих частот 150-6000 Гц.

Таким чином можна зробити висновок про ефективність різних засобів зашумлення в окремих ситуаціях. Детальне розуміння особливостей їх роботи дає можливість комплексно їх застосовувати для досягнення максимального ступеню захисту аудіальної інформації, коли це необхідно.

**3.2. Пріоритети вибору елементів системи захисту інформації у контексті новітніх тенденцій**

У сучасний період часу організація, компанія, будь-яка країна, організація може стати жертвою кіберзлочинності та втратити цінну інформацію. Повідомлення про нові інформаційні загрози та кібератаки надходять від державних організацій, освітніх і медичних установ, банків, юридичних фірм, некомерційних та багатьох інших організацій. Так, нещодавній гучний скандал «Pandora Papers» може служити прикладом того, як жертвами кіберзлочинності стають будь-які особи, країни тощо. Хакери, інсайдерські погрози, програми-вимагачі зазнали великого поширення серед загроз в останні роки.

Передові країни та великі транснаціональні компанії більше інвестують у засоби захисту інформації, щоб усунути ризики та захистити свої конфіденційні дані. І це вже принесло перші результати. Нижче подано інфографіку, що підтверджує ефективність сучасних систем захисту і цим самим демонструє останні тенденції в галузі кібербезпеки. Організації у всьому світі постійно нарощують витрати у галузі забезпечення інформаційної безпеки, що відображається у відповідному рості цього сегменту світового ринку (рис. 3.1). В той же час кількість атак у світі суттєво знизилася з 2016 року (рис. 3.2), що говорить про ефективність коштів, витрачених на реалізацію інформаційної безпеки.

*Рис. 3.1.* **Динаміка інвестицій у продукти інформаційної безпеки у світі, 2017-2021 рр.**

*Джерело:* складено автором на основі статистичних даних [74]

*Рис 3.2.* **Динаміка кількості атак із використанням програм-вимагачів у світі, 2015-2020 рр.**

*Джерело:* складено автором на основі статистичних даних [52]

Проте в результаті глобалізаційних процесів та у зв’язку з інтенсивним переходом усього можливого документообігу, банківської системи, медичної системи тощо у електронний формат зловмисникам за один злам вдається щоразу викрадати все більше даних під час одного зламу (рис. 3.3).

*Рис. 3.3.* **Динаміка щорічних зламів даних та викрадених записів у США, 2005-2020 рр**.

*Джерело:* складено автором на основі статистичних даних [51]

Сучасний світ дає кіберзлочинцям можливість отримати велику кількість даних. Хоч злами і стали складнішими, в контексті діджиталізації, вони потенційно стали більш прибутковими. Тож ключове запитання у галузі інформаційної безпеки залишається тим же: що може зробити кожен керівник організації, щоб захистити дані? Сучасні технології пропонують ряд заходів для того, щоб урядові організації та бізнес могли вдосконалити свої системи інформаційної безпеки.

Одним із сучасних трендів у галзі інформаційної безпеки є використання біометричних технологій. На сьогодні вони інтегровані навіть у кожен смартфон (сканер відбитка пальця чи Face-ID). Застосування біометрики забезпечує швидку автентифікацію, високий рівень безпеки в управлінні доступом, а також точний моніторинг дій працівника (час логування, роботи, реєстрація внесених змін).

Перевірка особистості користувача перед наданням доступу до цінних активів чи засекречених документів є критично важливою в державному управлінні. Розпізнання голосу, сканер відбитка пальця чи всієї долоні, розпізнавання облич, поведінкова біометрика та аналіз ходи – це ідеальні варіанти, щоб визначити, чи є користувачі тими, за кого себе видають.

Використання біометричних даних як одного з найкращих методів захисту даних забезпечує більш безпечну аутентифікацію, ніж паролі та підтвердження за допомогою SMS. Ось чому біометричні дані вже стали невід’ємною частиною багатофакторної автентифікації.

Однак автентифікація – це не єдиний елемент системи захисту інформації, що використовує біометричні дані. Співробітники служби безпеки за допомогою біометричних даних можуть виявляти зламані облікові записи в режимі реального часу. Це дає можливість попередити викрадення чи втрату даних, коли злам вже відбувся. Окрім того, при миттєвому виявленні зламу, є шанс відстежити та ідентифікувати, хто чинить злам. Це можливо завдяки поведінковій біометрії, яка аналізує спосіб взаємодії користувачів із пристроями та їх поведінку в мережі. Якщо виявлено ненормальну поведінку, програма надсилає попередження співробітникам служби безпеки, щоб вони могли негайно відреагувати.

Нижче наведено кілька типів поведінкової біометрії, які можуть використовуватися системами аналітики поведінки користувачів [69, c. 95].

1. Динаміка натискання клавіш – враховує швидкість введення тексту та тенденцію робити типові помилки в певних словах для створення профілів поведінки користувачів
2. Динаміка миші – відстежує час між клацаннями та швидкість, ритм і стиль руху курсору
3. Біометрія руху очей - використовує пристрої відстеження очей і погляду для запису відео рухів очей і виявлення унікальних моделей.

Існує ряд біометричних параметрів, за якими здійснюється ідентифікація та аутентифікація особи. До них належать:

* райдужна оболонка ока;
* сітківка ока;
* вени на руках;
* відбиток пальця;
* відбиток руки;
* геометрія руки;
* геометрія обличчя;
* 2-D / 3D модель обличчя;
* підпис;
* голос;
* хода;
* форма вух.

З кожним роком з’являється все більше біометричних параметрів, за якими можна ідентифікувати та підтвердити особу. Але щоб їх вивчити і знайти способи обробки алгоритмів, потрібно багато часу і грошей. Тому ступінь перевірки біометричного параметра безпосередньо впливає на ступінь його використання.

Найбільш часто використовуваним варіантом сьогодні є відбиток пальця. Це пов’язано з тим, що дактилоскопія набула поширення в кінці XIX – початку XX століття. Вартість сканерів відбитків пальців з кожним днем зменшується, а кількість додаткових параметрів, таких як температура, сила натискання пальцем тощо, збільшується. Можна припускати, що зараз виробники сканерів відбитків пальців досягли межі можливостей у цій сфері.

Попри дешевизну і доступність сканерів відбитків пальців, найбільш статистично надійними і стійкими до підробок параметрами доступу є райдужка ока та скан вен на руках. Але процес збору та обробки таких параметрів займає трохи більше часу, ніж обробка відбитків пальців або форми обличчя.

В контексті біометричних методів ідентифікації важливо розглянути індекси надійності. Сюди відносять такі показники, як ймовірність помилкового ненадання доступу та ймовірність помилкового надання доступу. Для більшості сучасних біометричних методів ідентифікації ймовірність помилкової відмови у доступі прямує до 0%, а ймовірність помилкового надання доступу не перевищує 1-2% [8, c. 138]. Очевидно, що чим менші обидва ці показники, тим надійніший захист надає той чи інший метод. Також ці фактори допомагають вирішити, чи використовувати той чи інший метод ідентифікації та аутентифікації, залежно від ситуації. У таблиці 3.1 наведено ці індекси для найпопулярніших методів біометричної ідентифікації.

*Таблиця 3.1*

**Ймовірності хибного спрацювання найпопулярніших методів біометричної ідентифікації**

|  |  |  |  |
| --- | --- | --- | --- |
| Індекс | Відбиток пальця | Геометрія обличчя | Райдужка ока |
| Ймовірність помилкового ненадання доступу | 0,001% | 0,1% | 0,00001% |
| Ймовірність помилкового надання доступу | 0,8% | 7% | 0,1% |

*Джерело:* складено автором на основі наукових публікацій [69, c. 96]

Сьогодні вважається оптимальним і доречним для середніх і великих об’єктів, а також об’єктів з максимальною вимогою безпеки використовувати біометричний доступ до райдужної оболонки і, можливо, розпізнавати вени рук. Для об'єктів з чисельністю персоналу до кількох сотень чоловік оптимальним буде застосування доступу за сканом відбитків пальців. Система розпізнавання двовимірного зображення обличчя дуже специфічна. Вона може бути доречною в тих випадках, коли не допустимий фізичний контакт з системою розпізнавання, а встановити систему розпізнавання за райдужною оболонкою неможливо. Наприклад, це може бути актуально, коли ідентифікація здійснюється прихованою камерою, але це можливо лише при невеликій кількості осіб у базі даних і невеликому потоці людей.

Прогноз Markets&Markets на 2025 рік передбачає зростання ринку біометричних даних із 36,6 мільярдів доларів у 2020 році до 68,6 мільярда доларів у 2025 році [55]. Тому вкрай важливо стежити за технологіями біометричної безпеки та обирати найкращі новинки для конкретного випадку і нових загроз, які виникатимуть у майбутньому.

Ще одним важливим і обов’язковим заходом при виборі заходів інформаційної безпеки є формування письмової політики інформаційної безпеки.

Наявність письмового документу настільки важлива, по-перше, тому, що він служить офіційним керівництвом до всіх заходів забезпечення інформаційної безпеки, які використовуються у державі та державних органах. Це дозволяє фахівцям з інформаційної безпеки та співробітникам чітко розуміти усі вимоги у цій сфері та дає вам можливість виконувати правила, які захищають державні таємниці, а також особисті дані працівників і громадян. Однак робочий процес кожного відділу може бути унікальним, а наявність недоречних чи зайвих методів та заходів кібербезпеки може бути не лише неефективним витрачанням державних коштів, а й причиною порушення нормальної роботи відділу. Тому важливо, щоб у політиці були прописані особливості інформаційної безпеки для окремих відділів. Водночас, централізована політика безпеки може бути корисною як основний орієнтир для всієї компанії, вона не повинна охоплювати кожен процес у кожному відділі. Тобто заходи в межах відділу повинні створюватися індивідуально на основі центральної політики [18, с. 31-32].

Розбивка політик безпеки в такий ієрархічний спосіб має багато переваг. Роблячи це, служба інформаційної безпеки враховуєте потреби кожного відділу та гарантуєте, що їхні робочі процеси та загальний результат не будуть скомпрометовані в ім’я безпеки.

Наступним пріоритетним напрямком є специфікація інформаційної безпеки. Кожна галузь має свої специфічні та приховані ризики, тому зосередитися на дотриманні та виконанні всіх стандартних правил недостатньо для захисту конфіденційних даних. Раніше у роботі ми звертали особливу увагу на способи викрадення аудіальної інформації та шляхи попередження таких зламів. Це обумовлено тим, що в органах ДПС цьому приділена особлива увага, оскільки чимало важливої інформації обговорюється на нарадах або у телефонному режимі.

Слід звертати увагу на ризики, з якими стикається окрема організація чи компанія, і на те, як вони впливають на ефективність і результативність її діяльності. Найкращий інструмент у цьому питанні – ретельна оцінка ризику.

Деякі з найважливіших речей, які дозволяє виявити оцінка ризику, наведено нижче [76, с. 36:6-36:8]:

* визначити всі цінні активи організації,
* оцінити поточний стан системи захисту інформації в організації,
* розумно керувати стратегією інформаційної безпеки.

Правильна оцінка ризиків дозволяє уникнути багатьох неприємних речей, таких як штрафи та догани за недотримання правил, витрати на усунення потенційних витоків і порушень, а також збитки від відсутніх або неефективних процесів забезпечення інформаційної безпеки. В контексті цього доцільно рекомендувати проводити оцінку ризиків на регулярній основі для виявлення нових ризиків та дослідження стану виявлених раніше (чи були усунуті).

Щоб виявити нові ризики, необхідно слідкувати за новими методами злому, особливо з використанням баз даних і фреймворків, таких як MITRE ATT&CK.

Ретельна оцінка ризиків допоможе визначити пріоритети заходів безпеки та постійно вдосконалюватиме стратегію так, аби вона якнайкраще реалізовувала необхідний рівень безпеки.

Зазвичай, оцінка ризиків включає окремо оцінку ризиків природного походження та спричинених людиною, оцінку очікуваних необхідних заходів захисту, оцінку можливостей створення власного програмного забезпечення. В процесі аналізу коригуються найсуттєвіші виявлені ризики, а також проводиться оцінка ризиків після проведення коригувальних заходів.

Резервне копіювання даних є одним досить давніх засобів захисту інформації, але станом на сьогодні він набуває більш високої пріоритетності в світлі значного поширення використання програм-вимагачів. В ситуації із проникненням такої програми у систему, повна та поточна резервна копія всіх даних може стати порятунком.

Втім при роботі із резервними копіями важливо переконатися, що вони ретельно захищені, зашифровані та часто оновлюються. Також важливо розподілити обов’язки резервного копіювання між кількома людьми, щоб пом’якшити внутрішні загрози.

З року в рік набуває набуває все більшої популярності тренд 2018 року – Internet Of Things (Інтернет Речей). Bain & Company, Inc. прогнозує, що ринок Інтернету речей зросте приблизно до 520 мільярдів доларів у 2021 році [55]. Проте, як би сильно ми не хотіли бачити нові технології, безпека завжди стоїть на першому місці.

Найскладнішим у пристроях «Інтернету Речей» є їх доступ до конфіденційної інформації.

Камери безпеки, дверні дзвінки, розумні дверні замки, системи опалення, офісне обладнання – усі ці невеликі частини інформаційної мережі організації є потенційними точками доступу. Наприклад, зламаний принтер може дозволити зловмисникам переглядати всі документи, які друкуються або скануються. Раніше ми також описували механізм прослуховування шляхом зламу телефона.

Таким чином, до найефективніших методів захисту корпоративної мережі для забезпечення безпеки даних можна віднести:

1. проведення регулярних тестувань на проникнення, щоб зрозуміти реальні ризики та відповідно спланувати свою стратегію безпеки;
2. забезпечення шифрування даних як у стані спокою, так і в процесі передачі (наскрізне шифрування);
3. забезпечення належної автентифікацію, коли дозволені лише надійні з’єднання з кінцевими точками;
4. слід не допускати використання облікових даних, встановлених на приладах за замовчуванням, адже часто використовувані паролі легко знайти в Інтернеті;
5. стратегія системи інформаційної безпеки повинна включати заходи захисту для усіх пристроїв «Інтернету Речей».

Отже, можемо виділити такі основні напрямки подальшого вдосконалення системи захисту інформації як підвищення захищеності доступу шляхом впровадження біометричної автентифікації та підвищення рівня захищеності пристроїв, які є елементами «Інтернету речей». Окрім того, вважаємо аргументованою позицію, що політика інформаційної безпеки заслуговує підвищеної уваги і постійного оновлення, ефективним інструментом у чому має слугувати проведення регулярної оцінки ризиків.

**Висновки до розділу 3.**

У результаті аналізу перспективних напрямів вдосконалення методів захисту інформації ми дійшли до наступних висновків.

У підрозділі 3.1 досліджено питання щодо ефективного звукозашумлення з метою уникнення витоків аудіальної інформаціії, зокрема визначено критерії для оцінювання рівня акустичної безпеки, охарактеризовано основні види перетворювачів для забезпечення зашумлення, проаналізовано їхні основні властивості та ситуації, коли кожен із них доцільно застосовувати. Також виявлено можливі негативні наслідки від застосування зашумлювачів та шляхи вирішення цих негативних наслідків. Водночас, розкрито методи та особливості встановлення зашумлювачів для досягнення найкращого ефекту їхньої роботи. Окремим пунктом у висновках слід візначити пріоритетність створення сучасних акустичних випромінювачів з вбудованим некорельованим цифровим генератором синтезованого мовоподібного шуму.

Підбиваючи підсумки підрозділу 3.2 щодо дослідження пріоритетів вибору елементів системи захисту варто наголосити на доцільності постійного розвитку та вдосконалення системи інформаційної безпеки. У зв’язку із постійною еволюцією наявних загроз та виникненням нових, методи захисту інформації також потребують регулярного вдосконалення. Відповідно на постійній основі повинна оновлюватися стратегія організацій щодо інформаційної безпеки. З цією метою рекомендуємо на регулярній основі проведення оцінювання ризиків у галузі інформаційної безпеки. Окремої уваги у сучасній кібербезпеці заслуговує застосування біометричних методів ідентифікації та автентифікації. На сьогодні це золотий стандарт у наданні доступу. Кількість методів біометричної ідентифікації постійно зростає, а наявні методи вдосконалюються, що дозволяє кожній організації обирати певний метод відповідно до своїх вимог, можливостей та особливостей функціонування.

**ВИСНОВКИ**

Відповідно до сформульованої мети роботи та поставлених завдань у результаті дослідження теоретичних та практичних засад методів захисту інформації ми дійшли наступних висновків.

1. У процесі комплексного дослідження сутності та ролі безпеки інформаційних технологій на сонові праць вітчизняних та зарубіжних вчених сформульовано принципові відмінності між поняттями інформаційної та функціональної безпеки, а також визначено основні властивості інформації як об’єкта захисту. Результати аналізу властивостей інформації дали змогу визначити вимоги, які повинні виконуватися для забезпечення збереження інформації та її якості. Окрім того, визначено відмінності між поняттями загрози інформаційні безпеці та загрози безпеці інформації. Також виокремлено актуальні загрози інформаційній безпеці та окреслено можливі методи їх усунення.
2. У роботі розкрито історичний процес розвитку інформаційних загроз у галузі захисту інформації та впливу цих змін на появу нових технологічних та програмних засобів захисту. Встановлено, що зазвичай, засоби захисту розроблялися і впроваджувалися у відповідь на нові загрози, а не шляхом їх прогнозування і попередження. Виявлено, що в минулому поява та розвиток законодавчого регулювання галузі захисту інформації у світі більшою чи меншою мірою відставали від потреб галузі і намагалися наздогнати її. Втім сучасний стан організаційно-нормативного забезпечення галузі в провідних країнах світу та в Україні аргументовано як достатній.
3. Проаналізовано підходи вітчизняних та зарубіжних вчених до класифікації методів захисту інформації та запропоновано на їх основі власну класифікацію, що відображає багатогранність та складність галузі інформаційних технологій та захисту інформації. Втім на сьогодні більшість вимог щодо інформаційної безпеки в органах державного управління визначаються на загальнодержавному рівні, а не на рівні окремої організації. Це з однієї сторони робить рівень вимог до системи захисту інформації достатньо високим, а з іншої – знижує гнучкість окремих організацій і забирає в них можливість обирати методи залежно від особливостей функціонування та потреб. Окрім того, це може сповільнювати впровадження подальших інновацій в галузі.
4. У роботі приділено значну увагу особливостям практичного застосування методів отримання акустичної інформації. Цей потенційний канал витоку інформації є особливо важливим в органах державного управління, оскільки аудіальна інформація може бути на пряму пов’язана із конкретною людиною, яка її сказала, репутацією цієї людини або навіть країни загалом. Окрім того, важливою інформацією може бути не сам зміст даних, а емоційне ставлення посадової особи до цієї інформації. Велика кількість можливих способів отримання аудіальної інформації вимагає комплексних рішень у захисті такої інформації та врахування таких особливостей як розмір будівлі, будівельні матеріали, площа приміщення, кількість та перелік осіб, які мають до приміщення доступ, техніка, яка використовується у приміщенні, її технічні характеристики та вразливість тощо. Втім кожен із засобів отримання аудіальної інформації має певні слабкі місця, які охарактеризовано у роботі. Наприклад, для інфрачервоних передавачів – це необхідність знаходитися у безпосередній близькості до «жучка» для отримання інформації, для «телефонного вуха» - можливість виявлення через постійну зайнятість лінії абонента, для передавачів на основі технологій Wi-Fi, Bluetooth, GSM – можливість виявлення спеціальними приладами тощо. Ці слабкі місця повинні бути враховані при формуванні системи захисту інформації.
5. На основі моніторингу виокремлено найпоширеніші програмні методи збереження інформації як в локальних мережах, так і в мережах із доступом до глобальної мережі. Зокрема це використання firewall, антивірусів, програм для шифрування трафіку між зовнішньою та внутрішньою мережами, застосування захищених з’єднань на основі методів криптографії. Також здійснено розподіл методів програмного захисту відповідно до їх ефективності на різних рівнях інформаційної системи. Зокрема визначено такі рівні, як рівень окремого робочого місця, мережі, рівень взаємодії з користувачем та рівень системи управління базами даних. В даний час ефективно використовувати на рівні мережі маршрутизатори і міжмережеві екрани, а на рівні операційної системи – вбудовані засоби розмежування доступу. На рівні взаємодії із користувачем важливими заходами є аутетифікація, обмеження доступу та обмеження можливості самостійного встановлення програмного забезпечення користувачем. На рівні СУБД найнеобхіднішими на сьогодні визнано такі заходи як управління рівнями доступу, використання паролів, встановлення вимог до паролів, криптографічний захист інформації, що міститься у СУДБ.
6. У процесі дослідження виявлено особливості ефективного застосування систем зашумлення. Для цього сформульовано критерії для оцінювання рівня акустичної безпеки, зокрема мінімальний (при багатократному прослуховуванні запису неможливо відновити сенс повідомлення) та максимальний (неможливо встановити сам факт проведення бесіди). Виявлено, що для більшості сучасних будівель державних органів (цегляні стіни, бетонні перекриття) технічно більш ефективно застосовувати п'єзоелектричні перетворювачі як засоби зашумлення, але зважаючи на високу ціну та масу таких зашумлювачів (для досягнення необхідної ефективності) оптимальним рішенням є використання електромеханічних випромінювачів. Для уникнення негативних ефектів від застосування таких зашумлювачів рекомендовано встановлювати їх у нішах стін, вище підвісної стелі (якщо вона є), а також із зовнішньої сторони рами вікна. Окрім того, аргументовано необхідність коригування роботи випромінювача залежно від того, на які поверхні він встановлений. Це реалізується шляхом встановлення різних випромінювачів на різні поверхні, коригуванням налаштувань залежно від методу підключення, а також включенням в генератор еквалайзера.
7. Шляхом дослідження сучасного стану ринку продуктів інформаційної безпеки аргументовано необхідність постійного оновлення та вдосконалення елементів системи захисту інформації, а також визначено пріоритети вибору нових елементів системи захисту інформації. Доведено ефективність збільшення витрачання на засоби інформаційного захисту з метою зниження ризиків у галузі інформаційної безпеки, адже в світових масштабах загалом ця тенденція корелює із трендом зниження кількості окремих видів кібератак. У роботі доведено ефективність методів біометричної ідентифікації як перспективного напрямку вдосконалення систем захисту інформації. Вони характеризуються високим рівнем надійності та можуть використовувати різні біометричні характеристики залежно від потреб. Окрім того, біометричні методи можуть ефективно застосовуватися для виявлення нетипової поведінки і попередження викрадення чи втрати інформації, коли злам вже відбувся. Іншим пріоритетним елементом системи захисту інформації визначено необхідність її регулярного вдосконалення. Загрози інформаційній безпеці постійно розвиваються та змінюються, тож методи захисту інформації також потребують регулярного вдосконалення. Тому рекомендуємо оцінювання ризиків у галузі інформаційної безпеки як регулярний захід.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Абрамов Ю., Калиниченко М., Каргашин В. Опыт практических работ по виброакустической защите выделенных помещений от утечки речевой информации. *Ключевые проблемы банковской безопасности* : сбор. докл. Третьего московского междунар. форума "Технология безопасности – 98", Москва, 4 – 7 февраля 1998 г. Москва, 1998. С. 21-33.
2. Антонов В. В., Конахович Г. Ф., Козлюк І. О. Особливості передавання захищеного мовного трафіка через стандартний радіоканал авіаційних систем зв’язку. *Захист інформації.* 2011. №3. DOI: https://doi.org/10.18372/2410-7840.13.2036
3. Аппаратура защиты конфиденциальных переговоров TF-012N. URL: http://detektor.ru/prod/self/protect/tf-012n/ (дата звернення 20.07.2021).
4. Барсуков В. С. Интегральная защита информации. *Электроника. Наука, технология, бизнес.* 1998. №3-4. С 39-44. URL: https://www.electronics.ru/files/article\_pdf/1/article\_1933\_338.pdf
5. Барсуков В. С. Интегрированная защита специальных экранированных помещений. *Специальная техника.* 2000. № 1. C 36-46.
6. Басан А. С., Басан Е. С., Макаревич О. Б. Анализ средств моделирования для построения модели беспроводной сенсорной сети. *Модели мышления и интеграция информационно-управляющих систем :* сбор. труд. второй Международной научной конференции, посвящённой 25-летнему юбилею Кабардино-Балкарского научного центра Российской академии наук. Нальчик, 04–09 декабря 2018 года . Нальчик : КБНЦ РАН, 2018. С 148-153.
7. Береза А. М., Козак І. А., Шевченко Ф. А. Електронна комерція: навч. посіб. Київ. 2004. 326 с.
8. Біднюк П., Бондарчук В. Сучасні методи біометричної ідентифікації. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.* 2009. №1. С. 137-146.
9. Вавринчук М. П., Когут О. В. Інформаційна безпека держави. *Правові засади організації та здійснення публічної влади* : зб. тез II Всеукр. наук.-практ. інтернет-конф., м. Хмельницький, 2-8 трав. 2019 р. Хмельницький : ХУУП, 2019. - С. 37-40.
10. Василюк В. Об’єкти захисту інформації. Методи та засоби захисту інформації. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.* 2006. №2 (13). С. 88-102.
11. Випромінювач віброакустичний «Базальт-4ДВМ». URL: https://usts.kiev.ua/vyprominiuvach-vibroakustychnyj-bazalt-4dvm/ (дата звернення: 07.07.2021).
12. Галанский В., Ващенко Н., Королев Т., Лаврентьев А. Сравнительный анализ характеристик систем виброакустического зашумления. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.* 2003. №7. С. 217-221.
13. Галкін В. В., Пархоменко І. І. Використання VPN-технологій для захисту інформації в каналах корпоративних мереж. *Проблема кібербезпеки інформаційно-телекомунікаційних систем*: матер. наук.-техніч. конф., Київ, 10 – 11 березня 2016. Київ : КНУ, 2016. – С. 66.
14. Генератор виброакустического шума "ANG-2000”. URL: http://www.bnti.ru/des.asp?itm=751&tbl=04.03.01.01.02. (дата звернення: 07.07.2021)
15. Гладун А., Хала К. Таксономія стандартів інформаційної безпеки. *Наука, технології, інновації.* 2017. №2. С. 53-64.
16. Голев Д. В., Русляченко О. Ю., Бєлова Ю. В. Гончарук Д. С. Інформаційна безпека комунікаційних систем. Лабораторний практикум. Частина 2 – Комплекси техничного захисту інформації : навч. посіб. Одеса. 2010. 184 с.
17. Іванченко С. О., Гавриленко О. В., Липський О. А.Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації: навч. посіб. Київ : ІСЗЗІ НТУУ «КПІ», 2016. 104 с.
18. Карачка А. Технології захисту інформації: конспект лекцій. Тернопіль : ТНЕУ, 2017. 86 с.
19. Каргашин В. Л. Проблемы активной защиты виброакустических каналов*. Специальная техника.* 1999, № 6. URL: http://detektor.ru/files/publikaci/spectehnika\_6-1999.pdf (дата звернення 07.08.2021).
20. Коваленко Ю. О. Забезпечення інформаційної безпеки на підприємстві. *Економіка промисловості.* 2010. №3. С. 123-129
21. Козюра В., Хорошко В., Шелест М. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. Ніжин. 2019. 144 с.
22. Ластівка Г. І., Шпатар П. М. Технічний захист інформації і інформаційних та телекомунікаційних системах : навч. посіб. Чернівці : ЧНУ ім. Ю. Федьковича, 2018. 206 с.
23. Лізунов С. І., Філобок Є. В. Захист мовної інформації з використанням систем активного звукопридушення. *Захист інформації.* 2011. №1. С. 20-25.
24. Ліпкан В., Максименко Ю., Желіховський В. Інформаційна безпека України в умовах євроінтеграції: навч. посіб. Київ : КНТ, 2006. 280 с.
25. Ноздріна Л. В. Безпека проектів у контексті сталого розвитку. *Вісник Університету банківської справи.* 2017. №3 (30). С. 112-117.
26. Палагнюк, Д. М., Тищук Д. С., Березюк О. В. Принципи забезпечення інформаційної безпеки. *Якість і безпека. Сучасні реалії:* матер. наук.-техніч. конф., 14-15 березня 2018. Вінниця : ВНТУ, 2018. – С. 19-22.
27. Пархоменко І. І., Галкін В. В. Способи захисту каналів корпоративних мереж на базі VPN-рішень. *Сучасний захист інформації.* 2016. №4. С 35-40.
28. Перчевська Л. В, Дрозденко О. І, Дрозденко К. С., Лейко О. Г. Забезпечення теплового режиму роботи стержневих конструкцій п’єзокерамічних електроакустичних перетворювачів. *Мікросистеми, Електроніка та Акустика*. 2019. № 24. С. 56–63.
29. Плескач В. Л. Технології електронного бізнесу. Київ : КНТЕУ, 2004. 222 с.
30. Порошин И., Прокофьев М., Дворский В. Техника активной виброакустической защиты речевой информации в Украине: состояние и перспективы. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.* 2013. №1. С. 98-106.
31. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23.02.2006 р. № 3475-IV. Дата оновлення: 23.04.2021. URL: https://zakon.rada.gov.ua/laws/show/3475-15.#Text (дата звернення: 11.09.2021)
32. Про електронні довірчі послуги : Закон України від 05.10.2017 р. № 2155-VIII. Дата оновлення: 13.02.2020. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 08.06.2021)
33. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 р. № 851-IV. Дата оновлення: 07.11.2008. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення: 08.06.2021)
34. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки : Закон України від 09.01.2007 р. № 537-V. Дата оновлення: 09.01.2007. URL: https://zakon.rada.gov.ua/laws/show/537-16#Text (дата звернення: 08.06.2021)
35. Про Положення про технічний захист інформації в Україні : Указ Президента України від 27.09.1999 р. № 1229/99. Дата оновлення: 04.05.2008. URL: https://zakon.rada.gov.ua/laws/show/1229/99#Text (дата звернення: 08.06.2021)
36. Про Стратегію кібербезпеки України : Указ Президента України від 15.03.2016 р. № 96/2016. Дата оновлення: 18.03.2016. URL: <https://zakon.rada.gov.ua/laws/show/96/2016#n11> (дата звернення: 08.06.2021)
37. Про Доктрину інформаційної безпеки України : Указ Президента України від 25.02.2017 р. № 47/2017. Дата оновлення: 28.02.2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text (дата звернення: 08.06.2021)
38. Рибальський О. В., Хахановський В. Г., Кудінов В. А. Основи інформаційної безпеки та технічного захисту інформації : навч. посіб. Київ : НАВС, 2012. 104 с.
39. Рудий Є. М. Технології передачі дискретних технологій: навч. посіб. Одеса : ОНАЗ ім. О.С. Попова, 2013. 102 с.
40. Семенова О. О., Семенов А. О., Бєлов В. С. Системи рухомого зв’язку : навч. посіб. Вінниця : ВНТУ, 2017. 186 с.
41. Смирнова Е. В. Использование технологии VPN для защиты распределенной сети авиапредприятия от целенаправленных атак. *Современные тенденции в науке, технике, образовании* : сбор. науч. труд. V Междунар. науч.-практ. конф., г. Смоленск, 15 июля 2019 г. Смоленск, 2019. С. 64-67.
42. Хорев А. А., Быков А. И., Соколов А. Н. Проектирование и исследование характеристик аналогового генератора акустических помех. *Вестник УРФО. Безопасность в информационной сфере.* 2016. № 2(20). С. 4-10.
43. Хорев А. А. Классификация и характеристика технических каналов утечки информации, обрабатываемой ТСПИ и передаваемой по каналам связи. *Специальная техника*. 1998. №2. URL: http://st.ess.ru/publications/articles/tspi/tspi.htm (дата звернення: 18.09.2021)
44. Хорев А. А., Лукманова О.Р. Математическое моделирование пассивного акустоэлектрического канала утечки акустической речевой информации в телефонном аппарате. *Специальная техника*. 2016. № 6. С. 56 – 63.
45. Хорев А. А.Техническая защита информации. Т. 1. Технические каналы утечки информации: учеб. пособ. Москва: НПЦ «Аналитика», 2008. 436 с.
46. Шаповал З. В., Заболотний В. І. Аналіз ефективності існуючих засобів захисту від лазерних засобів акустичної розвідки. *Проблеми інформатизації:* тези доп. восьмої міжнар. наук.-тех. конф., 26-27 листопада 2020 року, Т. 1. Черкаси, Харків, Баку, Бельсько-Бяла, 2020. С. 100.
47. Шепель І. В. Порядок видачі та застосування кваліфікованого електронного підпису. *Актуальні проблеми та перспективи розвитку обліку, аналізу та контролю в соціально-орієнтованій системі управління підприємством* : матеріали ІІІ Всеукр. наук.практ. конф., м. Полтава, 31 березня 2020 року. Полтава, 2020. С. 177-180.
48. A Brief History of Cybersecurity. URL: <https://www.cybersecurity-insiders.com/a-brief-history-of-cybersecurity/>. (дата звернення 09.06.2021)
49. A history of information security. URL: https://www.ifsecgloba­­­l.com/cyber-security/a-history-of-information-security/ (дата звернення: 07.06.2021)
50. Aizuddin A. The Common criteria ISO/IEC 15408 – The Isights, Some Thought, Questions and Issues. Фредеріксбург: SANS Institute, 2021. 12с.
51. Annual number of data breaches and exposed records in the United States from 2005 to 2020. URL: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/ (дата звернення 31.09.2021).
52. Annual number of ransomware attacks worldwide from 2016 to 2020. URL: https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/ (дата звернення 31.09.2021).
53. Basin D., Cremers C. Meier S. Provably Repairing the ISO/IEC 9798 Standard for Entity Authentication. *Principles of Security and Trust.:* proceedings of First International Conference, Tallin, 24th of March – 1st of April 1, 2012. Berlin : Springer, 2012. P. 129-148.
54. Bischoff P. Which countries have the worst (and best) cybersecurity? *Comparitech.* 2021. URL: https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/# (дата звернення 10.10.2021).
55. Bosche A., Crawford D., Jackson D. Unlocking Opportunities in the Internet of Things. URL: https://www.bain.com/insights/unlocking-opportunities-in-the-internet-of-things/ (дата звернення 15.10.2021).
56. Danda J. M. R., Hota C. Attack identification framework for IoT devices. Information Systems Design and Intelligent Applications : proceedings of Third International Conference India 2016, Vol. 2. New-Deli, 2016. P. 505–513.
57. DOD 5200.28-STD. Department of Defense Trusted Computer System Evaluation Criteria. [Чинний від 26.12.1985]. – Вид. офіц. Вашингтон, 1985. 116 с.
58. Global biometric system market revenue in 2020 and 2025. URL: https://www.statista.com/statistics/1048705/worldwide-biometrics-market-revenue/ (дата звернення 31.09.2021)
59. Iqubal M., Riadi I. Analysis of security virtual private network (VPN) using open VPN. *International Journal of Cyber-Security and Digital Forensics.* 2019. №8 (1). P. 58-65.
60. ISO/IEC 10164-7:1992. Information technology – Open Systems Interconnection – Systems Management: Security alarm reporting function. [Чинний від 1992 року]. – Вид. офіц. Женева, 1992. 14 с.
61. ISO/IEC 10745:1995. Information technology – Open Systems Interconnection – Upper layers security model. [Чинний від 1995 року]. – Вид. офіц. Женева, 1995. 19 с.
62. ISO/IEC 11577:1995. Information technology – Open Systems Interconnection – Network layer security protocol. [Чинний від 1995 року]. – Вид. офіц. Женева, 1995. 116 с.
63. ISO/IEC 11586-1:1996. Information technology – Open Systems Interconnection – Generic upper layers security: Overview, models and notation. [Чинний від 1996 року]. – Вид. офіц. Женева, 1996. 54 с.
64. ISO/IEC 15408-1. Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model. [Чинний від 2009 року]. – Вид. офіц. Женева, 2014. 64 с.
65. ISO/IEC 15408-2. Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components. [Чинний від 2009 року]. – Вид. офіц. Женева, 2014. 218 с.
66. ISO/IEC 15408-3. Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components. [Чинний від 2009 року]. – Вид. офіц. Женева, 2014. 174 с.
67. ISO/IEC 18045. Information technology – Security techniques – Methodology for IT security evaluation. [Чинний від 2008 року]. – Вид. офіц. Женева, 2014. 290 с.
68. ISO/IEC 9798-1:2010. Information technology – Security techniques – Entity authentication – Part 1: General. [Чинний від 2010 року]. – Вид. офіц. Женева, 2010. 11 с.
69. Jain A., Hong L., Pankanti Sh. Biometric identification. *Comunication of the AMC.* 2019. Vol. 43. P. 90-98.
70. Lezzi M., Lazoi M., Corallo A. Cybersecurity for Industry 4.0 in the current literature: A reference framework. *Computers in Industry.* 2018. Vol. 103. P. 97-110.
71. Longworth J. VPN: from an obscure network to a widespread solution. *Computer Frau&Security.* 2018. №4. P. 14-15.
72. Research electronics international catalog 2021. URL: https://reiusa.net/wp-content/uploads/2021/02/2021\_REI\_Catalogue.pdf
73. Soomro, Z. A., Shah, M. H., & Ahmed, J. Information security management needs more holistic approach: A literature review. *International Journal of Information Management*. 2016. Vol. 36(2). P. 215-225.
74. Spending on cybersecurity worldwide from 2017 to 2021 (COVID-19 adjusted). URL: https://www.statista.com/statistics/991304/worldwide-cybersecurity-spending/ (дата звернення 20.09.2021).
75. The History of Cybersecurity. URL: https://www.futureoftech.org/cybersecurity/2-history-of-cybersecurity/. (дата звернення 09.06.2021)
76. Toch E., Bettini C., Shmueli E., Radaelli L., Lanzi A., Riboni D., Lepri B. The Privacy Implications of Cyber Security Systems: A Technological Survey. *ACM Computing Surveys.* 2018. Vol. 51. P. 36-1–36-27.
77. Tran T., Al-Shaer E., Boutaba R. PolicyVis: Firewall Security Policy Visualization and Inspection : proceedings of the 21st Large Installation System Administration Conference, Dallas, November 11-16. Dallas, TX: USENIX Association, 2007. P. 1-16.
78. Yeboah-Boateng E. O. Cyber-Security Challenges with SMEs in Developing Economies: Issues of Confidentiality, Integrity & Availability (CIA). Copenhagen: Aalborg University, 2013. 218 p.
79. Yin L., Fang B., Guo Y., Sun Z., Tian Z. Hierarchically defining Internet of Things security: From CIA to CACA. *International Journal of Distributed Sensor Networks.* 2020. Vol. 16 (1). P. 1-13.