пояснювати дітям основні правила користування джерелами інформації, навчити основам інформаційної культури.

**Список використаних джерел:**

1. Волошин Н. За даними досліджень, щомісячна аудиторія соцмереж зросла до 4 млрд користувачів. URL: https://armyinform.com.ua/2020/10/za-danymy-doslidzhen-shhomisyachna-audytoriya-soczmerezh-zrosla-do-4-mlrd-korystuvachiv/

2. Панченко О.А., Кабанцева А.В. Людська психіка в інформаційній небезпеці. URL: http://www.pubadm.vernadskyjournals.in.ua/journals/2020/3_2020/41.pdf

3. Шутенко А. URL: https://www.ar25.org/article/informaciynperenavantazhennya.html

4. Пілат М. Інформаційні впливи та інформаційні війни: сутність понять та їх взаємозв'язок в інформаційну епоху. URL: https://intrel.lnu.edu.ua/wp-content/uploads/2015/10/VLNU_Mv_2013_32_25.pdf

**Карпей Д.О.**
*студентка,*
*Національна академія Служби безпеки України*

## МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ В КОНКУРЕНТНІЙ РОЗВІДЦІ

Малі та середні підприємства станом на 2019 рік досягли 64% валової доданої вартості. Вони займають велику частку в таких галузях, як «будівництво», «адміністративне та допоміжне обслуговування», «професійна, наукова та технічна діяльність», в кожній з яких на них припадає понад 90% зайнятості [1].

З огляду на це, економіка України складається більш ніж на 50% з малих та середніх підприємств та є складовою національної безпеки країни. Тому дослідження методів та способів захисту інформації в конкурентній розвідці підприємств є актуальним. Якщо звернутися до статті Мужанової Т.М., у якій автор зазначає, що в Україні, на відміну від розвинутих країн світу, більшість компаній взагалі не використовують методи конкурентної розвідки, або використовують непрофесійно. Серед причин такої ситуації поряд із нерозумінням підприємцями сутності і значення КР як засобу інформаційно-

аналітичного супроводу забезпечення інформаційної безпеки і в кінцевому рахунку успішного управління бізнесом недостатнє висвітлення цих аспектів у науковій літературі [2].

Тому мета цієї статті – зрозумілий виклад методів та способів захисту інформації в конкурентній розвідці підприємств. Одним із напрямів діяльності конкурентної розвідки є виявлення спроб конкурентів незаконно отримати доступ до конфіденційної інформації компанії (у співпраці зі службою безпеки) [2].

В час інформаційного суспільства стають найбільш актуальними методи захисту інформації в інформаційних системах (ІС) та інформаційних технологіях (ІТ) та ґрунтуються на таких принципах: системний підхід до побудови системи захисту, обґрунтуванні та реалізації найраціональніших методів, способів і шляхів удосконалення СІБ; безперервному контролі; виявленні її вузьких і слабких місць; встановленні потенційних каналів просочування інформації; визначенні нових способів несанкціонованого доступу.

Програмно-технічні методи – це сукупність засобів: запобігання витоку інформації; усунення можливості несанкціонованого доступу до інформації; запобігання впливам, які призводять до знищення, руйнування, переключення інформації або до збоїв чи відмов у функціонуванні засобів інформатизації; виявлення вмонтованих пристроїв; запобігання перехопленню інформації технічними засобами; використання криптографічних засобів захисту інформації під час передавання каналами зв'язку.

Організаційно-економічні методи передбачають: формування і забезпечення функціонування систем захисту секретної та конфіденційної інформації; сертифікацію цих систем відповідно до вимог інформаційної безпеки; ліцензування діяльності у сфері інформаційної безпеки; стандартизацію способів і засобів захисту інформації; контроль за діями персоналу в захищених інформаційних системах. Важливими для запобігання інформаційним загрозам є мотивація, економічне стимулювання і психологічна підтримка діяльності персоналу, який забезпечує інформаційну безпеку. Управління доступом – методи захисту інформації регулюванням всіх ресурсів ІС і ІТ. Ці методи протистоять можливим способам несанкціонованого доступу до інформації. Управління доступом виконує такі функції захисту: ідентифікацію користувачів, персоналу та ресурсів системи (закріплення за кожним об'єктом персонального ідентифікатора); розпізнання (визначення достовірності)

об'єкта або суб'єкта за пред'явленим ним ідентифікатором; Для захисту інформації можна встановити спеціальне обладнання, зокрема: 1. Для захисту телефонних ліній використовуються: аналізатори телефонних ліній; прилади активного захисту; фільтри; випалювачі засобів зняття. 2. Для захисту від радіозакладок використовують джерела радіошуму. 3. Для захисту від диктофонів: детектори диктофонів; прилади, що дистанційно стирають запис із касетних диктофонів. 4. Для захисту від лазерного перехоплення інформації з віконного скла використовують вібратор скла. 5. Для захисту від передавання інформації через лінію застосовують: фільтри; джерела шуму з діапазоном частот 50–300 кГц. До додаткових заходів належать: демонтаж усіх недіючих електричних кабелів; монтаж у мережі водо- та теплопостачання діелектричних муфт; контроль оперативної обстановки біля офісу: охорона, встановлення камер [3].

З метою раціонального використання ресурсів, сировини, компанії вимушені ефективніше використовувати та контролювати інформаційні процеси, що відбуваються на підприємстві. Особливо це стосується інформації з обмеженим доступом, що є на підприємстві. В умовах конкурентної розвідки захист власної інформації є одним з основних пріоритетів діяльності компанії. Методів захисту інформації в конкурентній розвідці підприємств багато, на підприємстві цим займається служба безпеки, на основі оцінки ризиків, керівництвом компанії приймаються рішення про застосування відповідного методу захисту інформації. Враховуючи, що зараз інформація циркулює здебільшого в інформаційних системах підприємства, методи захисту інформації в цій системі є найбільш актуальними.

**Список використаних джерел:**

1. Дмитро Горюнов, Олена Кравченко. URL: https://sme.gov.ua/analytics/
2. Мужанова Т.М. URL: http://economyandsociety.in.ua/journals/16_ukr/65.pdf
3. Керницький І.С., Живко З. Б. URL: https://cutt.ly/ulO6Vmu