

заходів з ТЗІ за наявності відомостей щодо порушень виконання вимог нормативно-правових актів з питань ТЗІ.

Перевірки здійснюються комісіями Підприємства на які покладено виконання завдань щодо здійснення контролю за функціонуванням системи ТЗІ.

При проведенні перевірки стану ТЗІ контролю підлягають організаційні, організаційно-технічні, технічні заходи з ТЗІ в виділених приміщеннях, інформаційних системах і об'єктах, повнота та достатність робіт з атестації виділених приміщень.

Необхідно провести аналіз функціонування системи захисту інформації, перевірку виконання заходів ТЗІ, контроль ефективності захисту, підготувати та видати дані для керування системою захисту інформації. Керування системою захисту інформації полягає у адаптації заходів ТЗІ до поточного завдання захисту інформації. За фактами зміни умов здійснення або виявлення нових загроз заходи ТЗІ реалізуються у найкоротший строк.

### **Список використаних джерел:**

1. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення системи захисту інформації в автоматизованій системі, затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28.04.99 р. № 22.

2. Михайлюк В.А. Безпека інформаційної сфери – основа стійкого розвитку соціуму // Безпека життєдіяльності. – 2007. – № 6. – С. 15-16.

3. Цимбалюк В. Інформаційна безпека підприємницької діяльності: визначення сутності та змісту поняття за умов входження України до інформаційного суспільства (глобальні кіберцивілізації) // Підприємництво, господарство і право. – 2004. – № 3. – С. 88-91.

**Харицька О.М.**

*студент,*

*Навчально-науковий інститут інформаційної безпеки*

*Національної академії Служби безпеки України*

## **ФЕЙКОВА ІНФОРМАЦІЯ ЯК ІНСТРУМЕНТ ДЕСТАБІЛІЗАЦІЇ СУСПІЛЬСТВА**

Сучасний світ сильно ускладнюється завдяки технологізації та інформатизації практично всіх сфер життя суспільства. Не має сумніву, що названі процеси можуть як полегшувати працю та життєдіяльність людей, так і обтяжувати, оскільки збільшується інформаційне й технологічне (техногенне) навантаження на людину, особливо в технополісах і великих промислових регіонах, відволікаючи її від соціального та природного середовища, в якому вона живе й працює. Під впливом інформатизації змінюється спосіб і характер життя, обмежуються «живі» міжособистісні комунікації, натомість формується штучно створений віртуальний світ, який набуває здебільшого надуманих, нерідко мімікрійних (маскувальних, імітаційних) форм, за якими приховується, а подекуди й пригнічується «жива» та динамічна людська природа [3].

Нова інформація та знання, які щоденно продукуються в сучасному світі, зокрема в комп'ютерних мережах, суттєво впливають на світогляд людини, на її зв'язки з навколишнім світом. Як зазначає професор Б. А. Головка, інформація є «базовим ресурсом усіх суб'єктів соціальної дії, проте вона не безпосередньо детермінує соціальну дію, а лише створює інформаційне підґрунтя для формотворного вияву логіки мережі в усьому розмаїтті суспільних практик» [1].

Оскільки інформація продукується ким завгодно і де завгодно, вона не завжди буває правдивою й нерідко несе в собі псевдомеседжі, фейки, які спотворюють реальну дійсність.

Для початку, визначимо значення терміну «фейк». Це слово прийшло з англійського середовища, де мало сленгове підґрунтя і перекладається, як фальшивка, підробка, несправжній, неістинний, фальшивий, обманювати, прикидатися.

Фейками називають фотографії, які зроблені у фотошопі, спеціально створені відеоролики, написані або вигадані неправдиві новини, які важко відрізнити від правдивих. Також фейками називають створені акаунти вигаданих людей у соціальних мережах, через які розповсюджується неправдива інформація.

Така інформація поширюється дуже швидко та з часом поповнюється новими подробицями. Фейкова інформація може використовуватися як для поширення інформації про товари з метою збільшення обсягів їх продажу, так і для поширення інформації від вигаданих людей, яких із часом можуть почати вважати реальними та використовувати їх думку, бачення ситуації.

На фейки взагалі можна було б не звертати увагу, сприймати їх як байки чи гуморески, якби такі повідомлення не були б інформаційною зброєю масового ураження, яка може використовуватись однією соціальною групою проти іншої.

Основна мета фейкових повідомлень як інструменту інформаційної війни – це посіяти сумніви і переконати аудиторію у правдивості поданої інформації. А завдання: дезінформувати аудиторію; пропагувати власне бачення, політику чи позицію; викликати агресію; похитнути позицію індивідуума і змусити його засумніватися; посіяти паніку; змінити уставлену думку в аудиторії; спонукати до певної дії; активувати увагу і зацікавити аудиторію; переконати аудиторію за допомогою вигаданих фактів; залякування аудиторії тощо [5].

Вагомою проблемою є те, що люди звикли довіряти засобам масової інформації, тому практично завжди сприймають «на віру» все те, що «подається» ЗМІ. Тому виникає ризик довірливого (бездумного) сприйняття значною кількістю людей псевдоінформації як правдивої й такої, що відповідає дійсності. Тобто йдеться про деформацію суспільної свідомості окремих груп людей під впливом маніпулятивних технологій, які реалізуються окремими ЗМІ й політичними акторами, що переслідують особистісні чи групові політичні інтереси.

Під впливом подібної неначебто правдивої інформації в особистісній структурі багатьох людей відбуваються зміни, оскільки формування й укорінення в їх свідомості рухливих інформаційно-віртуальних образів і форм взаємодії з агентами соціальних мереж розмиває ціннісно-нормативні патерни,

які були сформовані під впливом соціального середовища, в якому людина розвивалася та виховувалася.

А відтак, віртуальні образи-норми негативно впливають на особистісне «Я», порушуючи звичне ставлення людини й до оточення, і до природи, і до предметно-речового світу.

Особистісні зміни можуть бути і конструктивними, і деструктивними, вони можуть сприяти розвитку людини, посилюючи її гуманістичну природу, і, навпаки, можуть призводити до проявів її агресивних та руйнівних властивостей [2].

Український філософ Б. А. Головка, розмірковуючи над тематичною диспозицією проблем та напрямів інформаційної соціології, вказує на те, що відкритість глобальної інформаційної мережі й відсутність санкціонованого контролю за рухом інформації в ній «має для суспільства певні негативні наслідки: поширення комп'ютерних вірусів, різні види інформаційного «засмічення» – «чорна», «сіра», «біла» дезінформація, «патогенні» тексти, порносайти, комп'ютерне хакерство, несанкціонований доступ, або «злам» сайтів державних установ та комерційних організацій з метою отримання конфіденційних інформаційних ресурсів та переказування на інші рахунки фінансових ресурсів» [1]

Перелічені негативні наслідки свідчать, що в діяльнісній діаді «людина – інформація» сформувався також ризик деморалізації певних груп людей під впливом комп'ютерної інформації, особливо підлітків і молоді, у яких досить нестійкою є нервова система й недостатньо сформовані особистісні ціннісно-нормативні системи. Існує немало прикладів того, коли молоді люди під впливом неперевіреної інформації втрачають обережність, довіряючись різним шахраям, аферистам, залучаються до різних релігійних, екстремістських, радикальних груп, сатанинських культур, мережевих «оргій», метою яких є політичний, релігійний або екстремістський фанатизм, який виявляється в асоціальній, делінквентній, а іноді й у суїцидальній поведінці. Інтернет, як павук, затягує людину у свою павутину. І як тільки вона починає жити в ілюзорному світі, вона втрачає зв'язок зі світом реальним і потрапляє в залежність від всесвітньої мережі» [4].

Отже, існує реальний ризик масової психологічної залежності окремих груп населення, зокрема підлітків і молоді, від інтернет інформації, наслідком якого є поширення психічних розладів і захворювань, не випадково у «психіатрів збільшується кількість пацієнтів, основні скарги яких пов'язані з впливом Інтернету»

З фейками не потрібно боротися, їх варто спростовувати і висміювати, але у жодному разі не поширювати. Між тим універсальна сутність людини уможливорює кореляцію цього впливу відповідно до її потреб і бажань, запобігаючи руйнації особистісної структури. Однак для цього потрібна оперативна (миттєва) і потужна інформаційно-освітня протидія, яка б відслідковувала й спростовувала фейкову інформацію в соціальних мережах. Звісно, що її суб'єктом-носієм мусить бути фахівець (індивід, група, організація тощо), який є експертом у відповідній сфері діяльності й переконливий у своїх контраргументах і доказах.

З іншого боку, дуже важливо, щоб кожен член суспільства, навіть якщо він не є експертом у певній сфері, був підкріплений такими знаннями, які допоможуть виявити фейкову інформацію та протидіяти її впливу на свідомість.

### Список використаних джерел:

1. Головка Б. Інформаційна соціологія: тематична диспозиція / Борис Головка // Соціологія: теорія, методи, маркетинг. – 2004. – № 2.
2. Вплив ЗМІ на свідомість людини [Електронний ресурс] / Володарська державна районна рада – 2015. – 18 лютого. – Режим доступу: [http://volodarka-rda.gov.ua/index.php?option=com\\_content&view](http://volodarka-rda.gov.ua/index.php?option=com_content&view)
3. Малюк А. Глобалізація як процес виникнення інформаційного суспільства / Андрій Малюк // Соціологія: теорія, методи, маркетинг. – 2015. – № 4. – С. 20–39.
4. Мінченко О. Страх і ненависть в мережі: огляд сайтів, що поширюють фейки та чутки [Електронний ресурс] / Ольга Мінченко // watcher: – Режим доступу: <http://watcher.com.ua/2014/09/26/strah-i-nenavyst-v-merezhi-ohlyad-saytiv-scho-poshyruyut-feyky-ta-chutki>
4. Прокопенко М. Фейк як інструмент війни [Електронний ресурс] / Марія Прокопенко // День. – Режим доступу: <http://m.day.kiev.ua/uk/article/media/feyk-yak-instrument-viyni>

**Харламов Б.С.**

*студент,*

*Навчально-науковий інститут інформаційної безпеки  
Національної академії Служби безпеки України*

## ПОНЯТТЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Роботи із захисту інформації у нас в країні ведуться досить інтенсивно і вже тривалий час. Накопичено значний досвід. Зараз вже ніхто не думає, що достатньо провести на підприємстві ряд організаційних заходів, включити до складу автоматизованих систем деякі технічні і програмні засоби – і цього буде достатньо для забезпечення безпеки.

Головний напрямок пошуку нових шляхів захисту інформації полягає не просто в створенні відповідних механізмів, а являє собою реалізацію регулярного процесу, здійснюваного на всіх етапах життєвого циклу систем обробки інформації при комплексному використанні всіх наявних засобів захисту. При цьому всі засоби, методи і заходи, що використовуються для ЗІ, найбільш раціональним чином об'єднуються в єдиний цілісний механізм – причому не тільки від зловмисників, але і від некомпетентних або недостатньо підготовлених користувачів і персоналу, а також позаштатних ситуацій технічного характеру.

Основною проблемою реалізації систем захисту є:

– З одного боку, забезпечення надійного захисту, що знаходиться в системі інформації: виключення випадкового і навмисного отримання інформації