***Лобанчикова Н. М., канд., техн. наук, доцент,***
***доцент кафедри КІ та КБ,***
***Ющенко О. О., старший викладач кафедри КІ та КБ***
*Державний університет «Житомирська політехніка»,*
***Лобанчикова В. С., магістрантка***
*ІІНО Київський національний університет будівництва і архітектури*

# АНАЛІЗ СФЕР ЛЮДСЬКОЇ ДІЯЛЬНОСТІ ЩОДО ВРАЗЛИВОСТЕЙ В РЕАЛІЯХ ПАНДЕМІЇ COVID-19

Розвиток цифрових інновацій та технологій спричинив активний вплив на усі сфери життя сучасного людства. Технології IoT являє собою мережу об'єктів зв'язаних через інтернет і здатних збирати дані і обмінюватися даними, які надходять із вбудованих сервісів. За прогнозами аналітиків у найближчі роки очікується справжній бум інтернету речей. Застосування технологій IoT успішно проявили себе у всі аспектах сучасного людського життя, таких як освіта, охорона здоров'я та бізнес, виробництво, інфраструктура, логістика, транспорт, військово-оборонний комплекс, нафто-газова промисловість і видобуток корисних копалин, напрямки Smarthome і Smartcity, агро-сектор і багато інших.

Слід враховувати, якщо приймається рішення про запровадження і використання технології Інтернет речей, в першу чергу необхідно забезпечити систему безпеки. Кібербезпека, зазнала нових умов розвитку за останній рік в нових реаліях пандемії COVID-19. Кібератаки не тільки спричиняють фінансові збитки, але й значно впливають на репутацію компаній. У зв'язку з переходом багатьох організацій на умови дистанційної роботи, який спровокувала пандемія COVID-19, виникли нові можливості для кібератак. Їхня кількість зросла з менше 5000 за тиждень у лютому 2020 року до понад 200 000 за тиждень у кінці квітня 2021-го.

Згідно статистичних даних наразі в Україні фіксуються 60 тисяч кібератак на тиждень. Перше місце посідають атаки на державний сектор. Сьогодні Україна має високі показники за індикаторами цифровізації, тому що введено в дію застосунок "Дія", є понад 15 сервісів, які дос-тупні на платформі. Що стосується бізнесу, то, безумовно, це атаки на фінансовий сектор, банківський сектор, тут бізнес теж вибудовує свої системи. І все це вимагає координації, обміну інформацією.

Однією з вразливих індустрій другий рік поспіль є сфера охорони здоров'я та медичних наук. Було зареєстровано 240 інцидентів, з них 1,2 млрд. скомпрометованих записів. Це викликає серйозні побоювання, зважаючи на величезну кількість скомпрометованих записів і типів даних. Злами у сфері охорони здоров'я можуть призвести до розкриття медичної інформації, яка може вплинути на репутацію жертв. Виникають ризики використання даних про окрему людину і порушення конфіденційності. Тому виникає питання про надійність зберігання цих даних і правового забезпечення їх захисту від несанкціонованого використання.

Сфера технологій і медіа посідають друге місце в рейтингу найбільш вразливих: 158 інцидентів і 3,3 мільярда скомпрометованих записів. Кібератаки спричиняють збільшення витрат організацій і зменшують їх дохід, внаслідок чого вони зазнають банкрутства і змушені зменшувати масштаб своєї діяльності виходити з ринку.

Сфера освіти була однією з найбільш уразливих ще до COVID-19, 2020- 2021 роки стали просто продовженням зростаючого тренду, хоча він спостерігається у всіх секторах. Має 157 інцидентів і 884 мільйони записів. Як і у випадку з витоками в охороні здоров'я, інциденти безпеки в освітніх організаціях надзвичайно небезпечні, оскільки більшість записів містять інформацію про дітей.

Зазнають велику кількість кібератак і вітчизняні ІТ-компанії. На початку вересня 2020 р. зазнала злому велика українська ІТ-компанія, цей випадок став публічним, хоча зазвичай подробиці таких атак не розголошуються. Саме тому, в Україні досить важко знайти механізми аналізу і розробку рекомендацій щодо запобігання загроз. Навіть великі ІТ-компанії, які серед іншого позиціонують себе як провайдерів послуг в сфері забезпечення кібербезпеки, не завжди можуть з 100% надійністю протистояти кібератакам. Лише деякі великі компанії не з ІТ-сектору виділяють ресурси на забезпечення кібербезпеки. І, навіть, вони в більшості випадків розглядають кібербезпеку як додаткову функцію ІТ-підрозділу, хоча це неправильно.

Основі «тренди» кіберзахисту:

- аналітика безпеки і можливих загроз;
- endpoint-рішення;
- ідентифікації користувачів;
- безпека мережі і даних.

Отже питання безпеки та конфіденційності стають все більш актуальними для користувачів та постачальників у зв'язку з їх переходом на дистанційну форму роботи. Використання сучасних технологій віддаленої роботи вимагає нового підходу до безпеки, який передбачає не лише запобігання вторгненням, а й швидке виявлення атак, оцінку та компенсацію збитків