система штучного інтелекту, яка не має 100 % якості. Їй завжди властиві помилки першого та другого роду: тобто вона може розпізнати «неправильний» об'єкт як правильний чи не пропустити правильний об'єкт. Тобто завжди залишається ймовірність, що система вас не розпізнає чи розпізнає вас як когось іншого, на кого ви схожі.

Сфера біометричної автентифікації перспективна та швидко розвивається, з кожним роком зростає кількість досліджень та розробок у цій сфері. Однак ці методи недосконалі, і завжди є ймовірність помилок. Варто уважно зважити всі «за і проти», перш ніж ухвалити рішення використати біометрію для захисту своїх конфіденційних даних та коштів. Якщо вкрадений пароль або банківську картку можна замінити, то як замінити вкрадене «обличчя» чи «палець»? Втрачений чи вкрадений біометричний ідентифікатор стає скомпрометованим уже назавжди. Про це слід пам'ятати, погоджуючись використовувати метод біометричної автентифікації. У людей має бути вибір – здавати чи не здавати свої біометричні дані, адже ризики їхнього несанкціонованого використання, як і раніше, залишаються високими.

Бібліографічні посилання

1. Биометрическая идентификация: удобство и риски. URL: https://plus-one.rbc.ru/society/biometricheskaya-identifikaciya-udobstvo-i-riski

2. Биометрия и информационная безопасность. URL: https://safe-surf.ru/users-of/article/659637/

3. Суомалайнен А. Биометрическая защита: обзор технологии. Изд-во ДМК-Пресс, 2019. 99 с.

Касич Є. Ю.,
здобувач 2-го курсу вищої освіти
факультету підготовки фахівців
для органів досудового розслідування
Науковий керівник – Прокопов С. О.,
старший викладач кафедри
економічної та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

ПОШИРЕННЯ КІБЕРЗЛОЧИННОСТІ В СУЧАСНІЙ УКРАЇНІ, ПРОБЛЕМАТИКА ТА ШЛЯХИ ВИРІШЕННЯ

На сьогодні глобальною проблемою не тільки України, але й усього світу є поширення кіберзлочинів, спроби подолання та звісно статистика даних правопорушень, що значно зросла з періодом усесвітньої пандемії. Кіберзлочини мають різні напрями, що реалізуються у зовсім не схожих

сферах життя: від шахрайських схем за допомогою смартфону до розповсюдження дитячої порнографії, але ж структура з кожним роком стає все ширше та посягає на значні соціальні блага та цінності.

Як ми вже сказали, що через введення карантину статистика кіберзлочинів зросла. Це пов'язано з тим, що суспільство почало віддавати перевагу глобальній мережі «Інтернет» та ставити на задній план спілкування в соціальних мережах, згідно з цим шахраям простіше розповсюджувати павутиння шахрайства, адже закриті магазини, банки, кінотеатри тощо штовхають користуватися онлайн-послугами, які не завжди у сучасному світі є легалізовані та законні. Якщо порівняти статистику 2021 року з іншими роками, ми бачимо значну різницю. Про це розповів глава Департаменту кіберполіції Олександр Гринчак в інтерв'ю в РБК-Україна: «На сьогодні в нас дійсно зросла статистика по кіберзлочинах. За чотири місяці цього року, порівняно з минулим, ми бачимо приріст на 25 %. На цей час ми зафіксували 1157 таких інцидентів. По них ми вже оголосили 263 підозри» [1]. Статистика інших років вказує: «Стрибок кількості всіх кіберзлочинів відбувся в 2017 році. Після цього кількість злочинів має тенденцію зростати. Так в 2017 було зафіксовано 1795 справ, в 2018 році – 1023, за останні півроку – 1005» [2].

Найбільш актуальною проблемою є кримінальні правопорушення з участю неповнолітніх. На нашу думку, саме цей вид є найбільш поширеним, адже діти або неповнолітні – особи, які мають великий рівень довіри, вважають, що сварки з друзями, погані оцінки, матеріальне неблагополуччя – це дилема, яка немає виходу, саме тому звертаються до Інтернету або поглиблюються до онлайн-життя за порадою та розумінням, потрапляючи на челенджі, летальні ігри та депресивний контент, що штовхає дитину до вчинення суїциду та інших наслідків. Щодо цього під час інтерв'ю Олександру Гринчаку поставили таке запитання, на яке він дав обґрунтовану відповідь: «Через соцмережі вже кілька років відбуваються злочини за участю неповнолітніх. Це і «групи смерті» так звані «сині кити», зараз це ще й челенджі в Tik-Tok на кшталт «напийся таблеток». У нас вже є жертви і постраждалі від цього. Як цьому можна протидіяти?

– Щодо дітей, то ми щодня відстежуємо статистику незалежно від того, стався суїцид або вдалося врятувати дитину. Ми виїжджаємо на кожен такий випадок і оглядаємо девайси, щоб зрозуміти, в чому причина. Стосовно нещодавніх інцидентів, то ми не фіксували їх зв'язок із суїцидальними групами. Як правило, причина – це любов, непорозуміння з друзями в школі, проблеми з навчанням або батьками або просто неблагополучна сім'я. Звісно, коли є проблеми, дитина замикається. Вона заходить в Інтернет, а там маса деструктивних каналів, інформаційних джерел і підозрілих людей, які можуть «підкинути» депресивну музику або скинути в особисті пост із закликом, що «нічого робити в цьому світі» і краще просто померти…» [1]. Отже, кіберполіція запроваджує нові кроки подолання саме цього летального

виду злочинності у онлайн-існуванні підлітків.

Також нині «В Україні кожна четверта дитина за останній рік стикалася з проявами сексуального насильства в Інтернеті» [3]. Ми звернулись до офіційних джерел щодо інцидентів проявів сексизму над дитиною «Кожних 5 хвилин Internet Watch Foundation знаходить у мережі фото чи відео сексуального насильства над дитиною. 46 000 000 зображень із дитячою порнографією зберігається у базі Європолу. Третина цих матеріалів припадає на селфі, тобто дітей змушують робити інтимні фото чи відео самостійно. Щоб досягти своєї мети, злочинці вдаються до особливих практик: секстингу, онлайн-грумінгу та сексторшену» [4] .

Крім того, правоохоронці вже розробили шляхи припинення вчинення правопорушень. По-перше, для того щоб мати більш розвинуту систему, ми звертаємось до європейських або американських партнерів для обміну інформацією та досвідом. По-друге, «Кіберполіція весь час вказує на необхідність ратифікації парламентом додаткових положень Конвенції про кіберзлочинність від 23 листопада 2001 року. Йдеться про удосконалення збору цифрових доказів, що дасть правоохоронцям якісно документувати та оперативно розслідувати кримінальні кіберпорушення. Ми повинні узгодити кримінальне законодавство у сфері інфотехнологій до європейських стандартів та підвищити кримінальну відповідальність за вчинення кіберзлочинів» [5].

Зважаючи на вищенаведене, можна зробити висновок, що ця проблема посягає глобального масштабу та для її подолання треба звертатись до європейських партнерів. Також впровадження програм роботи із неповнолітніми та малолітніми особами щодо небезпеки інтернету та кіберзлочинів. Створювати відповідні гуртки у школах, проводити тренінги для поширення необхідної інформації, спрямованої на захист та певною мірою на протидію проявів кіберзлочинів.

Бібліографічні посилання

1. Глава Департаменту кіберполіції Олександр Гринчак про злочинні схеми через месенджери, шахрайство по телефону і з банківськими картами, «групи смерті» в соцмережах, легалізацію криптовалют і «піратство» – в інтерв'ю РБК-Україна. URL: https://www.cyberpolice.gov.ua/news/glava-kiberpolicziyi-oleksandr-grynchak-cherez-kryptovalyutu-proxodyt-bilshist-zlochynnyx-operaczij-395/ (дата звернення: 19.10.2021).
2. За п'ять років кіберзлочинність в Україні зросла вдвічі. URL: https://www.epravda.com.ua/rus/news/2019/10/21/652782/ (дата звернення: 19.10.2021).
3. Кількість кіберзлочинів в Україні в 2021 році зросла на 25 %. URL: https://www.rbc.ua/ukr/news/kolichestvo-kiberprestupleniy-ukraine-2021-1622012394.html (дата звернення: 18.10.2021).
4. Сексуальне насильство онлайн: як захистити дитину в інтернеті. URL: https://kyivstar.ua/uk/cybersecurity/seksualne-nasylstvo-onlayn-yak-zahystyty-dytynu-v-interneti (дата звернення: 19.10.2021).
5. Міжнародні хакерські угруповання: як працюють і що робить Кіберполіція. URL: https://biz.nv.ua/ukr/experts/hakeri-ta-kiberpoliciya-chi-vdastsya-zahistiti-ukrajinciv-novini-ukrajini-50165630.html (дата звернення: 19.10.2021).