МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ
ОДЕСЬКОГО НАЦІОНАЛЬНОГО ТЕХНОЛОГІЧНОГО УНІВЕРСИТЕТУ»

МАТЕРІАЛИ

студентської науково-практичної конференції «БАЗОВІ ПРАВИЛА БЕЗПЕКИ У ЦИФРОВОМУ СЕРЕДОВИЩІ»

17 травня 2023 р.

м. Одеса

ЗМІСТ

1 ІНТЕРНЕТ-ЗАЛЕЖНІСТЬ. ВПЛИВ ТЕХНОЛОГІЙ НА СУЧАСНЕ СУСПІЛЬСТВО

Доповідачі: Крістіна ДОРОШЕНКО
Олександра ІВАНИШИН
Анастасія ШУШМАН
Керівник: Олена СКОРНЯКОВА
ВСП «Одеський технічний фаховий коледж
Одеського національного технологічного університету»

В сучасному світі комп'ютер, смартфон та інші гаджети – це не просто пристрої для обробки інформації, а речі без яких ми не уявляємо своє теперішнє та майбутнє. Інтернет розширив можливості гаджетів, і тепер у віртуальному просторі можна прожити ціле життя: працювати, спілкуватися, закохуватися, грати, відвідувати музеї, наукові конференції, вчитися, домагатися популярності, робити покупки, розвиватися, та у декілька кліків знайти майже всю необхідну інформацію.

Сьогодні понад 4-х мільярдів людей є активними користувачами Інтернету (приблизно 56 % населення світу). Оскільки більшість наших щоденних заходів проводяться в мережі, люди все більше стурбовані тим, як технології впливають на наші думки, поведінку і, зрештою, як це формує нас як особистість.

Інтернет як велике досягнення технічного прогресу має величезне значення для людства, виконуючи безліч корисних і незамінних функцій. Але, як виявилося, всесвітня павутина володіє одним негативним наслідком, яке поширене по всьому світу – це інтернет-залежність, проблема сучасного суспільства. В чому її суть і в чому небезпека залежності від мережі?

На думку Эрин Хоффман, розробниці онлайн ігор, однією з причин Інтернет-залежності є прокрастинація. Прокрастинація – схильність людини до постійного відкладання важливих або неприємних справ. «Коли ми говоримо про залежність – ми говоримо не про те, що люди роблять, а про те, чого вони не роблять, заміщуючи не залежною поведінкою».

Інтернет-залежність є одним із різновидів залежної поведінки, поряд із алкогольною, наркотичною залежністю, залежністю від азартної гри тощо. На відміну від алкогольної та наркотичної залежності, інтернет-залежність цілком міститься у психічній сфері (фізіологічної залежності не формується). Проте, не слід вважати, що ця форма залежності менш серйозна. Вперше термін «інтернет-залежність» вжив Айвен Голдерг в 1994 році. Він мав на увазі не хворобу порівнянну з алкоголізмом або наркоманією, а скоріше проблему, пов'язану зі стресом і низьким самоконтролем людини. Тим не менш, цей термін прижився до сьогоднішніх днів і за роки придбав драматичний відтінок.

Хвороба ця ще не до кінця вивчена психологами, але причини залежності лежать на поверхні. Це може бути спроба компенсувати нереалізовані потреби (наприклад, завести «справжніх» друзів) або невмінням людини будувати стосунки в реальному житті, або проблеми з самооцінкою.

У цих випадках корені проблеми сягають набагато глибше: у виховання і атмосферу в сім'ї. Дуже часто діти і підлітки, які стикаються з брутальним ставленням до себе, знаходять віддушину на просторах всесвітньої павутини.

Інтернет-залежність у підлітків проявляється найбільш гостро. Це велика проблема сучасного суспільства. Люди втрачають зв'язок з навколишнім світом, тому що знаходять йому альтернативу на просторах мережі. Вони не бачать сенсу в зустрічах з друзями – можна поговорити в месенджерах або зробити відео-дзвінок.

Замість походу по магазинах люди також користуються послугами інтернету, а інші розваги їм замінюють онлайн-ігри, форуми, перегляд відео або просто серфінг.

З вищесказаного випливає, що є різні види інтернет-залежності: ігрова залежність (гемблінг); азартна залежність; залежність від інтернет-спілкування; інформаційна залежність; сексуальна залежність.

Чому люди стають залежними від Інтернету?

Доступність: більшість людей можуть легко та майже негайно вийти в Інтернет у будь-який час дня чи ночі.

Контроль: люди можуть виходити в Інтернет, коли хочуть і без відома інших людей, що створює відчуття контролю.

Хвилювання: вихід в Інтернет викликає у людей щось на кшталт «кайфу». Напруження ставок на онлайн-аукціонах, азартних іграх чи іграх може бути особливо захоплюючим, як «дофаміновий удар».

Поєднання доступності, контролю та хвилювання змушує залежну людину продовжувати працювати в Інтернеті.

Симптоми інтернет-залежності

Психологічні симптоми:

- Хороше самопочуття чи ейфорія за комп'ютером
- Неможливість зупинитися
- Збільшення кількості часу, проведеного за комп'ютером
- Нехтування сім'єю і друзями
- Відчуття порожнечі, депресії, роздратування не було за комп'ютером
- Брехня роботодавцям чи членів родини про діяльність
- Проблеми з роботою чи навчанням

Фізичні симптоми:

- Сухість у власних очах
- Головний біль чи навіть мігрені
- Біль в спині
- Нерегулярне харчування, пропуск прийомів їжі
- Нехтування особистою гігієною
- Розлади та зміна режиму сну
- Що допоможе побороти інтернет-залежності

Якщо ви виявили у себе декілька описаних вище симптомів, то краще відразу приступити до лікування своєї залежності. Для тих, у кого ці ознаки проявляються ще не надто яскраво, теж не варто зволікати. Тому, коли у вас безперервно рука тягнеться

до гаджета і ви боїтеся пропустити щось дуже важливе у віртуальному світі, краще провести профілактику, аніж запустити захворювання.

1. Розвантажувальні дні (або хоча б години). Відкладіть телефон, не вмикайте комп'ютер, вимкніть повідомлення на смарт-годиннику. Здається, що це дуже важко і ви не зможете провести так цілий день. Тому починайте з декількох годин. Зробіть, наприклад, свій вечір вільним від інтернету та присвятіть його сім'ї чи улюбленому заняттю. З часом ви зрозумієте, що нічого цікавого не пропускаєте в мережі, проте дещо варто надолужити у реальному житті.

2. Насичене дозвілля. Коли ви проводите свій вільний час на дивані, інтернет допомагає побороти нудьгу, але це не приносить вам ніякої користі. Намагайтеся зробити своє дозвілля насиченим, щоб, по-перше, у вас не вистачало часу на зазирання у соцмережі, а, по-друге, ви отримали яскраві враження та заряд енергії. Якщо у вас не вистачає сили чи фантазії на активний відпочинок, то краще візьміть до рук книгу.

3. Замініть віртуальне реальним. Якщо ви хочете поспілкуватися з подругою, то запросіть її на прогулянку чи в кафе, а не переписуйтеся цілий день у месенджері. Якщо хочете з кимось познайомитися – згадайте про романтичні дідівські методи, а якщо бажаєте подивитися фільм – запросіть чоловіка/дружину у кіно. Вийдіть за двері будинку та зрозумійте, що реальне життя набагато цікавіше.

4. Позбувайтеся поганих звичок. Так і хочеться сфотографувати свіжоприготовлений борщ та викласти в мережу, а стрічка ваших Stories з однакових селфі перетворилася у штрих-пунктирну лінію? Подумайте, чи справді людям настільки цікаве ваше повсякденне життя. Позбудьтеся від звички знімати кожен свій крок та жити заради лайків і переглядів у соцмережах. Навіть, коли ви в захваті від приготовленої вами яєчні, залиште фото для власного архіву.

Представимо результати дослідження на тему «Вплив технологій на сучасне суспільство». Ми провели опитування, у якому прийняли участь 156 респондентів, вікова категорія яких варіювалася від 10 років до приблизно 70 років. Більша кількість опитуваних була вікової категорії 16-20 років - 67%, 35-70 років - 16%, 10-15 років – 10,9%, 21-35 років – 5,8%. 77 % учасників не уявляє своє життя без цифрових технологій, при цьому опитуваних у віці 10-20 років – 78%, можемо зробити припущення, що це саме молодь. Та проте 89% респондентів використовують Інтернет, щоб відволіктись від проблем та поганого настрою. Більшість учасників опитування не приховують від батьків реальний час проведення за гаджетами, і приховують тільки 5,1%. Більше половини людей використовують гаджети більше 7 годин на день (54,5%), 5-7 годин на день – 25%, 3-4 години – 17,9%, 1-2 години – 2,6%. На соціальні мережі респонденти витрачають – більше 7 годин – 9%, 5-7 годин – 10,9%, 3-4 години – 35,9 %, 1-2 години – 39,1%, не сидять в соціальних мережах – 5,1% опитуваних.

Загалом на думку опитуваних, соцмережі, ігри та мобільні додатки є єдиним способом зняття стресу, тому що це доступно, легко, відволікає від реальних проблем.

В соціальних мережах, опитувану аудиторію найбільше цікавить інформаційний контент - 85,9%; вірусний – 50,6 %; той, шо залучає – 28,8%, торгівельний – 23,7% ,та хочемо відмітити що більшість учасників обирає 2 типи контенту. Думаємо, тут можна провести паралель з найпопулярнішими соц мережами Telegram, Instagram, Youtube, Tik

Tok, Viber, що пояснюється тим, що зараз українці слідкують за новинами, спілкуються та намагаються підтримувати зв'язок один з одним, відволікаються від тяжких обставин, шукають мотивацію та підтримку, продовжують працювати.

У приблизно 50% опитуваних спостерігаються такі симптоми інтернет-залежності: непереборне бажання вийти в інтернет; нездатність контролювати час, проведений в мережі; розумове або фізичне виснаження; порушення сну або концентрації уваги.

Згідно даних ВООЗ 66 % людей страждають депресією через соціальні мережі, що підтвердила думка опитуваних. Також опитувані вважають, що найчастіше страждають інтернет-хворобами люди у підлітковому (59% відповідей) та юнацькому віці (33% відповідей).

На питання «Чи почуваєте Ви себе втомленим, пригніченим чи роздратованим, коли намагаєтес, обмежити або припинити користування інтернетом?» так почували себе - 18,6%, при цьому контролювати, обмежити чи припинити використання інтернету намагалися 30,8%. 82,7% людей з даного дослідження підтверджують, що замість робочих завдань сиділи в мережі, але здається більша половина змогла впоратися з цією проблемою, тому що тільки 28,2 % згодні з тим, що ризикували одержати проблеми на роботі, в навчанні чи особистому житті через захоплення інтернетом.

Основними плюсами використання гаджетів, соц мереж опитувані вважають:

- спілкування;
- корисна інформація;
- можливість розвиватися;
- дозвілля;
- перегляд фільмів;
- прослуховування музики;
- можливість заробітку.

Основними мінусами використання гаджетів, соц мереж опитувані вважають:

- великий обсяг інформації;
- інформація нецензурного, аморального, злочинного характеру;
- хейт, цькування;
- ймовірність виникнення залежності

Як Ви ставитеся до закритих груп та пабліків? За результатами опитування, на дане питання більшість людей відповіло, що ставляться до закритих груп/пабліків нейтрально (28,2%) та нормально (17,3%). Трохи менша кількість опитуваних ставляться до таких груп позитивно (19,2%), вважаючи, що деякий контент необхідно приховувати від зайвих або неповнолітніх осіб:

1. «Я вважаю, що закриті групи та пабліки це цілком нормально, бо у всіх є така інформація або розмови, які б не хотіли оприлюднювати серед усіх користувачів інтернету.»

2. «Нормально бо є групи та пабліки сторго 18+ в яких краще неповнолітнім не бути.»

3. «Цілком позитивно: не все повинно бути доступним для всіх.»

Майже така ж кількість користувачів відповіли, що ставляться до приватності груп/пабліків негативно (18,6%), вважаючи, що контент в них переважно пов'язаний з насиллям, булінгом, аферистами і подібним.

1. «Ставлюся до цього негативно, тому що більшість пабліків в інтернеті є обманливими.»

2. «У деяких групах або каналах можуть пропагандувати насилля, вбивства або ідеологій які можуть нашкодити суспільству/людині.»

3. «Я не дуже довіряю таким групам або чомусь іншому що є закритим,за такими закритими групами можуть приховуватися аферисти і тому подібне.»

Певна частина опитуваних відповіли, що їх ставлення до подібних груп чи пабліків залежить від змісту та тематики даних груп/пабліків (9,6%):

1. «Дивлячись якого характеру, якщо це інформаційні - нейтрально, якщо мають злочинний характер – негативно.»

2. «Дивлячись які теми обговорюються в цих групах і пабліках.»

Ще невелика група відноситься до закритих груп/пабликів з підозрою або обережністю – 3,2%, не користуються такими групами – 3,8%.

Отож, ми розглянули вплив комп'ютеру та гаджетів на наше життя та емоційний (внутрішній) стан людини. Отримані дані показали, що більшість людей залежні від сучасної техніки, а кіберпсихологія поки є не до кінця розвиненою практикою.

Спочатку нам здавалося це нормальним – гаджети нам багато в чому допомагають, але в той же час взяв якийсь смуток, бо віддаючи настільки себе віртуальному, ми зовсім забули про реальне – я чесно кажучи останнім часом помітила, що мені набридає дуже багато часу сидіти перед монітором – я хочу більше часу проводити на вулиці, з друзями, я хочу читати живі книжки, іноді мені хочеться весь день тільки читати.

Тож, технології – це чудово, це дуже круто, що ми все більш розвиваємося в цій сфері, але все ж таки хоча б іноді відпочивайте від наших кіберпомічників.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Інтернет-залежність. Одеський обласний центр громадського здоров'я. URL: https://healthcenter.od.ua/psyhichne-zdorovya/internet-zalezhnist/ (дата звернення: 05.04.2023).
2. Кібербулінг: як протистояти. SupportME. URL: http://supportme.org.ua /needle-and-bullying/cyberbullying (дата звернення: 20.02.2023).
3. Манасова А. Кіберхондрія: наскільки небезпечно шукати симптоми в інтернеті?. Одеський обласний центр громадського здоров'я. URL: https://healthcenter.od.ua/2020/10/29/kiberhondriya-naskilky-nebezpechno-shukaty-symptomy-v-interneti/ (дата звернення: 05.04.2023).
4. Мащенко С. Номофобія - хвороба 21 століття, про яку ви можете не знати. РБК-Украина. URL: https://www.rbc.ua/ukr/styler/nomofobiya-bolezn-21-veka-kotoroy-mozhete-1663046878.html (дата звернення: 16.02.2023).
5. Як позбутися від інтернет-залежності: розбираємося в темі. ALEXUS - Чоловічий журнал: спорт, здоров'я. URL: https://alexus.com.ua/internet-zalezhnist-problema-suchasnogo-suspilstva/ (дата звернення: 05.03.2023).

6. Ancis J. R. The Age of Cyberpsychology: An Overview. Technology, Mind, and Behavior. URL: https://tmb.apaopen.org/pub/2yn6jhyv/release/1.
7. Basic Group – ЕФЕКТ GOOGLE. ЯК ТЕХНОЛОГІЇ ЗМІНЮЮТЬ НАШУ ПАМ'ЯТЬ. Basic Group. URL: https://basicgroup.ua/ефект-google-як-технології-змінюють-нашу-па/ (дата звернення: 16.02.2023).
8. Cyber Therapy. JupiterOne: Cyber Asset Attack Surface Management. URL: https://www.jupiterone.com/cyber-therapy (date of access: 05.04.2023).
9. Internet Addiction | Personal Assistance Service. Personal Assistance Service. URL: https://pas.duke.edu/concerns/addictions/internet/ (date of access: 05.04.2023).
10. Maike Neuhaus Ph.D. Artificial Intelligence in Psychology: 9 Examples & Apps. PositivePsychology.com. URL: https://positivepsychology.com/artificial-intelligence-in-psychology/ (date of access: 05.04.2023).
11. Peony Rose. Киберпсихология: краткий экскурс. https://author.today /post/214801. URL: http://librarychl.kr.ua/kn_in/informatoria/inf-ge.php (дата звернення: 16.02.2023).

2 ІНТЕРНЕТ-БЕЗПЕКА В СОЦІАЛЬНИХ МЕРЕЖАХ

Доповідач: Денис ХЛЬОУПЕК
Керівник: Богдан БРИНЗЕЙ
Івано-Франківський фаховий коледж технологій та бізнесу

На сьогодні існує велика кількість соціальних мереж. Деякі з найбільш відомих соціальних мереж включають: Facebook, Twitter, Instagram, LinkedIn, Tik Tok, Snapchat, Pinterest, YouTube та інші. Кожна з цієї соціальної мережі має свої унікальні функції та спеціалізацію, тому користувачі можуть вибрати ту, яка найбільше відповідає їхнім потребам та інтересам.

Сьогодні соціальні мережі є складовою майже всіх сфер людського життя і хоча вони мають багато переваг, існують проблеми і серйозні загрози, про які не завжди згадують. Багато людей вважають соціальні мережі розвагою, але мала кількість людей звертає увагу на важливість дотримання правил безпеки в цьому середовищі. Існує низка небезпек, пов'язаних з використанням соціальних мереж:

Розповсюдження небезпечної інформації: спільноти та групи в соціальних мережах можуть бути використані для розповсюдження небезпечної інформації, такої як фейкові новини, пропаганди насильства та екстремізму.

Кібербулінг та кіберсталкінг: соціальні мережі можуть бути майданчиком для кібербулінгу та кіберсталкінгу, що може призвести до психологічних проблем та негативного впливу на здоров'я людини.

Крадіжка особистих даних: зловмисники можуть використовувати соціальні мережі для отримання доступу до особистої інформації та для крадіжки облікових даних, таких як паролі та номери кредитних карток.

Негативний вплив на психічне здоров'я: залежність від соціальних мереж може мати негативний вплив на психічне здоров'я та продуктивність людини, зокрема, сприяти розвитку депресії та тривоги.

Шахрайство та використання особистих даних для злочинних цілей: соціальні мережі можуть бути використані для поширення шахрайських схем, крадіжки грошей тощо.

Неправдиві новини та інформація, яка розповсюджується в соціальних мережах, можуть призвести до зростання паніки та негативного впливу на суспільство.

Реклама в соціальних мережах може бути небезпечною для фінансової безпеки користувача.

Віруси можуть поширюватися через соціальні мережі, що може призвести до втрати особистих даних.

Публікація зображення та відео може призвести до порушення особистої приватності та використання матеріалу для шахрайства чи шантажу.

Зловмисники використовують всі види обману для отримання доступу до особистої інформації користувача мережі та її використання [2, с.204]. Такими є фішинг та фармінг.

Фішинг – це метод шахрайства, коли зловмисники вибирають підроблені електронні повідомлення або веб-сторінки, щоб отримувати від користувачів конфіденційну інформацію, таку як паролі, номери кредитних карток, інформацію про банківські рахунки тощо.

Фармінг – це метод збору інформації, коли зловмисники створюють підроблені веб-сторінки, щоб отримати доступ до особистої інформації користувачів. Зазвичай зловмисники використовують соціальні мережі, електронні листи або підроблені веб-сторінки, щоб залучити користувачів до введення своїх особистих даних.

Захист від фішингу та фармінгу включає в себе використання складних паролів, відмову від відповіді на сумнівні електронні повідомлення та веб-сторінки, а також інсталяційне програмне забезпечення для захисту від шкідливих програм та вірусів. Також важливо регулярно оновлювати програмне забезпечення та оновлення системи на комп’ютері та мобільному пристрої.

Щодня безпека даних у соціальних мережах піддається сумніву. Важливо пам’ятати, що особисті та корпоративні облікові записи, які більше не використовуються, можуть становити особливу загрозу. Кіберзлочинці можуть використовувати їх для поширення загрози та дезінформації. Тому дуже важливо контролювати, хто має доступ до облікових записів та видаляти їх, коли вони більше не потрібні. Хоча навмисних атак зловмисників стає все більше, практика показує, що випадкові помилки, неуважність до правил безпеки впливають на діяльність підприємства набагато більше, ніж атаки шахраїв [1, с.126].

У зв’язку з постійним вдосконаленням інструментів кіберзлочинців, користувачі можуть здійснювати ряд заходів безпеки:

Не розголошувати особисту інформацію: уникнення розголошення особистої інформації, такої як адреса, номер телефону, номер кредитної картки та інше.

Встановлення власних налаштувань приватності: налаштування профілю у соціальних мережах таким чином, щоб забезпечити максимальний рівень приватності.

Обережність з фейковими новинами: перевірка джерел новин та відмовлення від поширення сумнівних повідомлень.

Запам'ятовування паролю: заборона запам'ятовувати паролі в соціальній мережі та завжди використання складних комбінацій символів для їх створення.

Видалення неактивних облікових записів: при не використанні облікового запису у соціальній мережі, потрібно видалити такий запис, щоб запобігти його використанню зловмисниками.

Висновки. Інтенсивний інформаційний розвиток, що спричиняє проникнення інформаційно-комунікаційних технологій в усі сфери суспільного життя, крім значного потенціалу для самоорганізації та самореалізації, несе низку нових загроз глобального масштабу, серед яких − кіберзлочинність і кібертероризм, розмивання національної ідентичності, нехтування моральними засадами суспільства, маніпулювання свідомістю [3, с.155]. Загалом, використання соціальної мережі може бути безпечним, якщо користуватися правилами безпеки та пам'ятати про свої дані та приватність.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Коваленко Ю.О. Забезпечення інформаційної безпеки на підприємстві. Економіка промисловостісті. 2010. № 3. С. 123-129.
2. Скрута Г.В., Шкарупа І.В., Нікуліщев Г.І. Забезпечення інформаційної безпеки у соціальних мережах. Актуальні задачі та досягнення у галузі кібербезпеки: матеріали Всеукраїнської науково-практичної конференції. М.Кропивницький. С.204-205.
3. Тихомиров О.О. Забезпечення інформаційної безпеки як функція сучасної держави : моногр.; заг. ред. Р. А. Калюжний. К.: Центр навч.-наук. та наук.-практ. вид. НА СБ України, 2014. 196 с.

3 ПАСПОРТ ІДЕАЛЬНОГО ІТ-ФАХІВЦЯ

Доповідач: Ксенія ПАЮК
Керівник: Олена СКОРНЯКОВА
ВСП «Одеський технічний фаховий коледж Одеського національного технологічного університету»

ІТ-спеціаліст, інакшими словами «айтішник» - поняття, що об'єднує в собі багато професій, яке відноситься і до програміста, і до адміністратора мережі, і до технічного інженера.

Сучасний професіонал – це широко обізнана людина, яка здатна швидко адаптуватися, вміє ефективно комунікувати та постійно вдосконалюватися . Наразі в усьому світі спостерігається дефіцит кваліфікованих ІТ-фахівців, це пов'язано з стрімким розвитком цифрових технологій. Чим більш розвиненими стають технологічні галузі, тим гострішим стає дефіцит у якісних кадрах.

Що ж таке навички комп'ютерного інженера?

Навички комп'ютерного інженера є важливими атрибутами та здібностями, які потрібні їм для досягнення успіху у своїй галузі. Ці навички включають як м'які навички (софт скілс), такі як спілкування, так і здатність адаптуватися до жорстких навичок (хард скілс), таких як, наприклад, кодування та кібербезпека.

Незважаючи на стереотипи, навіть ІТ-фахівцям потрібні так звані м'які навички, щоб добре виконувати свою роботу.

Soft skills – це особисті якості, які напряму не пов'язані зі спеціальністю, але тісно переплітаються із професійними навичками, саме завдяки їм людина може ефективно взаємодіяти з іншими.

Soft skills об'єднують ряд психологічних характеристик, властивостей та вмінь, які можна згрупувати. Ці якості складно виміряти, а тому їх оцінка носить суб'єктивний характер. Більшість роботодавців вважають їх так само важливими, як і професійні знання та вміння. Професійні вміння мають властивість застарівати, а ось soft skills є актуальними завжди. Але які ж саме софт скіли потрібні? Насправді, їх список дуже варіюється, тож давайте передивимось різноманітні варіанти найактуальніших софт скілів на думку різноманітних компаній та лідерів думок.

У дослідженні Всесвітнього економічного форуму, заснованого на прогнозах керівників понад трьохсот світових компаній, а також на даних LinkedIn та FutureFit.AI, виділили топ-10 скіллів, які матимуть попит до 2025 року а саме:

- аналітичне мислення та іноваційність,
- активний і стратегічний підхід до навчання,
- комплексний підхід до розв'язання проблем
- критичне мислення та аналітичні навички
- креативність, оригінальність та ініціативність
- лідерство та соціальний вплив
- використання моніторинг та контроль технологій
- технологічний дизайн та програмування
- витривалість, стресостійкість та гнучкість
- навички логічної аргументації, розв'язання проблем та генерації ідей

Дивлячись на даний перелік ми бачимо, що хард скіли займають усього два пункти в рейтингу, а всі ж інші це софт скіли.

Forbes також опублікував п'ять найкращих soft skills, які потрібні кожному працівнику в 21 столітті. У даному переліку присутні такі якості, як гнучкість, відповідальність, командна робота, емпатія та критичне мислення.

А що ж думають про софт скіли лідери думок?

Ілон Маск висловився: "Загалом люди отримують задоволення від взаємодії з іншими людьми. Якщо ви працюєте над проєктом, до якого залучено команду, то вміння взаємодіяти — надважливе, а спілкування з іншими – найголовніший челендж". До цих навичок за версією високотехнологічного бізнесмена включено: комунікабельність, залученість до спільної справи, гнучкість, продуктивність, вміння спостерігати, слухати та аналізувати.

Майже десять років тому у статті BBC News із заголовком «Білл Гейтс: навички, необхідні для успіху» співзасновник Microsoft-мільярдер сказав: «Навички спілкування та вміння добре працювати з різними типами людей дуже важливі, інновація програмного забезпечення, як і майже будь-який інший вид інновації, вимагає здатності співпрацювати, ділитися ідеями з іншими людьми, а також розуміти потреби клієнтів». Із цікавих фактів, Білл Ґейтс двічі на рік присвячує цілий тиждень розвитку критичного мислення, усамітнюючись подалі від шуму великих міст, щоб зосередитись і подумати. Протягом цього часу, Ґейтс генерує інноваційні ідеї.

А Стів Джобс казав, що працювати потрібно не 12 годин, а головою. Відомо, що Джобс не мав технічних скілів, як у нинішнього генерального директора Apple Тіма Кука. Але він був саме тим ключовим лідером і генератором ідей, який зробив Apple Company такою, якою світ знає її сьогодні.

Давайте, поговоримо про деякі софт скіли, їх особливості.

1. Комунікабельність:

Маст хев для ІТ спеціаліста — комунікація: вміння слухати та чути, підтримувати відносини, доносити думки, при цьому не обов'язково бути красномовним оратором.

Комунікаційні навички важливі й для обміну досвідом. Вміння ділитися знаннями — одна із рис професіонала. Якщо ви бажаєте розвиватися, вчитися у колег, потрібно комунікувати. І коли необхідно вести переговори чи знаходити компроміси, без комунікації ніяк.

2. Тайм-менеджемент

Кожен день в ІТ-спеціалістів є певні таски. Однак поряд з основними задачами постійно виникають нові. До них додаються незаплановані мітинги, дзвінки, форс-мажори. Усе горить. За що хапатися? Якщо неправильно спланувати роботу, вона стає малопродуктивною та виснажливою. Не розрахував сили — не виконав завдання.

Людина не здатна керувати часом, але в її силах ставити пріоритети, розподіляти завдання, знаходити вірний робочий баланс. Допомагає в цьому скіл тайм-менеджменту

3. Гнучкість

Пристосовуваність породжує самостійність. У світі технологій щодня розробляються та застосовуються нові інструменти. ІТ-спеціаліст повинен бути в курсі останніх тенденцій, які потенційно можуть оптимізувати ваш кінцевий продукт. Для цього вони використовують модель постійного навчання у своїй повсякденній роботі. Здатність йти в ногу з часом і працювати над підвищенням кваліфікації, щоб адаптуватися до поточного сценарію, є однією з найкращих навичок, які може мати ІТ-спеціаліст.

4. Емоційний інтелект

Емоційний інтелект — це цінна навичка, яка користується великим попитом, і не лише серед генеральних директорів і менеджерів. Під емоційним інтелектом розуміють емпатію, здатність бачити й розпізнавати приховані емоції людини, навичку керувати власними емоціями при прийнятті практичних рішень. Опитування Careerbuilder в якому приймали участь понад двох тисяч шести сот менеджерів з найму в США показало, що 71% роботодавців цінують емоційний інтелект у своїх співробітниках більше ніж коефіцієнт інтелекту.

5. Відповідальність

Відповідальність — це надійність, і з таким фахівцем захочуть працювати, бо на нього завжди можна покластися. Щодня у IT спеціалістів виникають зобов'язання — перед командою та клієнтом. І немає значення, чи ви trainee, чи обіймаєте керівну посаду - почуття відповідальності повинно бути у кожного.

6. Самонавчання

Володіння навичками самонавчання може принести велику користь IT спеціалісту на робочому місці. Самонавчання протягом усього життя може надати здатність виявляти проблеми та швидко самостійно шукати ефективні рішення. Є тисячі IT фахівців, які приходять у світ технологій, не маючи офіційної комп'ютерної освіти, але все ще мають навички комп'ютерної інженерії. Незалежно від того, чи йдеться про вивчення нової мови чи заняття з новими технологіями, безперервне навчання є хорошою навичкою.

7. Командна робота

Ще один важливий soft skills IT фахівця - вміння працювати у команді. Навіть коли ви «дистанційник», і єдина людина, з якою ви комунікуєте - це менеджер, ви теж команда. Незалежно від того, чи це команда розробників, дизайнерів чи проектна команда, потрібно добре співпрацювати, щоб досягти успіху. Успіхи Facebook чи Google - це виключно результат командної роботи. Один у світі діджитал не воїн.

8. Абстрактне мислення

Це мислення без присутності фізичного об'єкта. Абстрактне мислення також можна описати, як здатність думати про предмет, об'єкт або проект на багатьох рівнях одночасно.

9. Творчість

Сфера IT приваблює людей креативних, які вміють мислити поза шаблонами, знаходити нові нестандартні рішення. Тут важко буде тим, хто може працювати тільки за інструкцією. Принаймні, в умовах високої конкуренції.

Найкращі ідеї та рішення часто приходять до нас, коли ми підходимо до речей з іншої точки зору. Незважаючи на поширену думку, творчості можна навчитися, але вона приходить з практикою. Читання художньої літератури, письмо, мистецтво, рукоділля, навіть кулінарія – це способи виявити творчі здібності. Чим більше способів творчості ви досліджуєте, тим легше вам знайти різні способи підходу до однієї проблеми.

10. Лідерство

Лідерство в галузі науки, технології, інженерії та математики – це використання емоційного інтелекту, щоб отримати найкраще від себе та тих, з ким ви працюєте.

Аналітики World Economic Forum зазначають, що жодному комп'ютеру поки що не під силу взяти на себе завдання лідера - надихати та вести команду. Лідер - це база будь-якої команди. Від нього залежить культура команди, загальний настрій та атмосфера. Основне завдання лідера - згуртувати людей. Причому успішні лідери витрачають вдвічі більше часу на формування команди, ніж рядові керівники, але підсумковий результат того вартий.

Перейдемо до хард скілів

Хард скіли – це навички, які необхідні для того, щоб бути затребуваними на ринку праці. Оскільки глобальна економіка зазнає змін, то і професійні навички

потребують удосконалення чи перекваліфікації. Уже недостатньо просто здобути професію раз і на все життя. Варто отримувати додаткові скіли.

Прикладами хард скілів для ІТ фахівців є вміння писати код, знання математики, бібліотек та фреймворків, UX та UI (для дизайнера), володіння англійською мовою. Давайте поближче познайомимось з хард скілами.

Знання англійської мови

Незалежно від сфери чи спеціалізації, яку ви оберете, варто також паралельно вивчати англійську мову – в сфері ІТ це не лише мова спілкування з клієнтами, а й мова "за замовчуванням" для самоосвіти, роботи з найновішими технічними інструментами та управління проектами. Чим вищий ваш рівень, тим більше «плюшок» ви відкриєте для себе. Майже всі інструменти, бібліотеки, фреймворки розроблені закордоном, а отже вони на англійській мові. Та й взагалі, на практиці ІТ-фахівцям доводиться дуже багато читати технічної документації на англійській. Окрім того, від рівня володіння іноземною мовою напряму залежить і зарплата ІТ-фахівця.

Нами було проведено дослідження на предмет визначенні переліку найбільш значущих soft skills та hard skills у формування паспорта ідеального ІТ- фахівця, для майбутнього працевлаштування, а також порівняння очікувань та уподобань роботодавців та майбутніх ІТ-фахівців. У дослідження взяли участь 50 студентів нашого коледжу та 5 українських ІТ-компаній. 71% опитуваних – чоловічої статі, і 29% жіночої. 51% опитуваних студентів перебувають у віці від 14 до 17 років, 45% у віці від 17 до 20, і лише 4% старші за 20.

Як зазначалося раніше, софт скіли складно виміряти, і їх оцінка носить досить суб’єктивний характер. Більшість роботодавців вважають їх так само важливими, як і професійні знання та вміння. Та чи це є правдою? Задавши питання ІТ- компаніям, що ж для них є більш пріоритетним, отримані такі відповіді:

«Це комбінація. Завжди важливо і перше і друге. Іноді стається так, що якщо хард скіли ще не на вищому рівні, але бачимо що людина завзята, старанна і відповідальна - будемо пробувати співпрацювати з людиною, бо хард скіли можна підтягнути, а софт скіли дуже рідко можна змінити.» - MYDIGICODE

«І софт-, і хадр-скіли є важливими, на них звертають увагу на етапі відбору, технічних співбесідах..» - ELEKS SOFT

«Ми звертаємо увагу на певний симбіоз та поєднання технічних знань з софт скілами.» - INFOPULSE

«В загалі на обидві категорії, адже робота в команді завжди потребує гарних софт та хард скілів» - VISEVEN GROUP

Отже, ІТ компаніям однаково важливі, як софт скіли, так і хард скіли – і слід вміти балансувати. Якщо ж у Вас виникають проблеми з софт або хард скілами, то у деяких ІТ компаніях надають тренінги, аби Ви мали можливість удосконалити їх.

Наступним питанням, вже студентам постало **«Чи важливо удосконалювати свої софт скіли?»**. 96 % відповіли «так», і лише 4% - «ні». Отже, більшість мають рацію, софт скіли необхідно вдосконалювати – розвиток soft skills посилює професійні навички. Наприклад, можна бути професіоналом у роботі з базами даних, але не вміти презентувати свої рішення колегам чи клієнтам – і це буде великим мінусом для вас,

також з добре розвиненими софт скілами у вас з'явиться більше шансів на співбесіді, а потім ці скіли допоможуть вам підійматися по кар'єрних сходах.

Ще одним питанням стало **«Чи важливо ІТ-спеціалісту бути комунікабельною людиною?»**. 86 % відповіли «так» - і ця думка не є хибною. Навички переговорів, презентації, уміння знаходити компроміси та працювати у команді – це все є невід'ємною частиною життя ІТ-спеціалістів.

Але, що ж робити, якщо Ви некомунікабельна людина, чи взагалі інтроверт, але вам ну дуже сильно хочеться в ІТ сферу. Саме таке питання я поставила до ІТ-компаніям.

Чи візьмуть вони на роботу некомунікабельну людину чи інтроверта Ось, які відповіді я отримала:

«Все залежить від позиції, якщо це позиція менеджера - то навряд, якщо позиція розробника, тестувальника, дизайнера то - то чого ні?», «На деяких позиціях це допустимо» «Комунікабельність не є основним критерієм вибору спеціаліста. Якщо людина інтроверт - це не є причиною відмови.» - пишуть вони

Аналізуючи відповіді, можна впевнено казати, що комунікабельність не є основною причиною прийому Вас, як ІТ-фахівця на роботу, але не всі позиції ви зможете обіймати, так як для деяких з них (наприклад, для позиції project менеджера) вкрай необхідні вміння комунікації. Отже, комунікабельність є скоріш скілом, який допоможе Вам у подальшому, наприклад, для роботи у команді, або якщо ви працюєте на фрілансі, то навички комунікації допоможуть вам для спілкування з клієнтом.

Чи присутні у студентів лідерські якості? Цілих 55% студентів вважають, що так, а отже у них автоматично з'являється перспектива стати менеджерами або очолити команду над проектом.

Важливість англійської мови для ІТ-спеціалістів:

ІТ компанії, серед яких я проводила опитування відповіли, що знання англійської є важливими і мінімальний рівень повинен бути B1, тобто intermediate. Вони пишуть:

«Так як ми надаємо послуги міжнародним компаніям, для нас є критично важливим знання англійської мови від рівня intermediate»

«Як для ІТ, для всіх співробітників важливо знати англ. мову на рівні читання і розуміння технічної документації. Все інше - відповідно до позиції специфіки проєкту.»

«Залежить від посади, іноді, достатньо розмовного англійського, а взагалі, нам важливі знання технічної англійської і вміння працювати з документацією на англійській мові»

А чи відповідають знання англійської мови наших студентів з вимогами ІТ-компаній?

Я вже зазначила раніше, що мінімальний рівень англійської у ІТ-спеціаліста повинен бути Intermediate (B1), але все ж таки більшість компаній хочуть, щоб ви розуміли технічну документацію і мали рівень B2. Нажаль, лише 14% відповідають цій вимозі, але рівень сімдесяти шести% студентів досягає рівню A1-B1 та вони знають розмовну англійську, отож я щиро вірю, що вони зможуть трішечки підтягнути свою англійську (деякі ІТ-компанії навіть надають курси для підвищення англійської мови) і зможуть відкрити більше можливостей для себе. Отож вчить англійську, вона обов'язково знадобиться.

Питання самоосвіти. Самоосвіта є однією з ключових якостей, якою повинні володіти IT-фахівці. На діаграмі ми бачимо, що цілих 75% студентів займаються самоосвітою і це не можна не відмітити. Яким ж методам студенти віддають перевагу? 70% віддають перевагу відеороликам, 14% - професійній літературі і 16% - інакшим засобам. Тож, можна зробити висновок, що молодому поколінню легше засвоювати інформацію завдяки відеороликам і це не перевантажує їх організм і такий формат отримання знань не набридає.

Вища освіта. Чи є вона обов'язковою складовою для IT-спеціаліста? Більшість студентів, а саме 67% все ж таки вважають, що так, і лише 33% мають інакшу думку.

Що ж про це думають IT-компанії? Чи візьмуть вони на роботу людину без вищої технічної освіти?

«Так, звісно! Тільки в 10 відсотках буває, що для клієнтів необхідна наявність вищої освіти. Але це завжди буде великим плюсом :)» - MYDIGICODE

«Для нас не критично чи має людина вищу освіту, головне що вона вміє і знає як розвивається.» - QUARTSOFT

«Так. З популярністю IT-сфери дедалі більше людей стають "світчерами", міняють свою професію» - ELEKS SOFT

«Для нас є важливим знання та вміння спеціаліста, який хоче обіймати позицію, а не підтвердження його рівня освіти, тому ми звертаємо увагу саме на технічні та софт скіли кандидата. Кожен спеціаліст, який пройшов курси чи навчався спеціальності самостійно має рівні шанси отримати позицію.» - INFOPULSE

Абсолютно всі IT-компанії, які приймали участь в опитуванні не вважають необхідністю мати вищу технічну освіту, але часто її наявність буде для вас плюсом.

А чи вважають IT-компанії, що знань, які фахівці отримують у ВНЗ повністю достатньо для того, щоб відповідати вимогам роботодавців?

Не всі компанії захотіли відповісти на це запитання, деякі ж просто висловились, що їм важко відповісти, але все ж деякі дали свою відповідь:

«Без самовдосконалення та навчання додаткового – ні» - VISEVEN GROUP

«Кожна позиція є індивідуальною і потребує своїм знань, вмінь та навичок, здебільшого ми розпочинаємо співпрацю з молодими спеціалістами, які окрім університетської освіти отримують додаткові знання, будь то вивчено самостійно чи за допомогою додаткових курсів.» - INFOPULSE

Що ж думають про це студенти, чи вистачає знань, які фахівці отримують у ВНЗ для того, щоб відповідати вимогам роботодавців?

Нажаль, 80% студентів вважають, що знань повністю достатньо, а ось IT-компанії вважають інакше - їм важливий саморозвиток майбутнього робітника. Отже, ми знов прийшли до актуальності та важливості такого скіла, як самонавчання – без цього ніяк.

Якщо Ви вважаєте, що ваші професійні чи особисті якості недостатньо прокачані, то є гарна новина – це наявність різноманітних курсів та тренінгів, які надають IT-компанії, головне показати компанії, що у Вас є потенціал і Ви маєте жагу розвиватися, і вдосконалитись вам допоможуть. У чотирьох з п'яти IT-компаній, серед яких я проводила опитування є курси, де співробітник може розширити свої знання.

Підбиваючи підсумки, хочемо порадити вам самовдосконалюватись, вивчати нові технології, тенденції та англійську мову, не забувайте балансувати і розвивати, як хард

скіли, так і софт скіли. Будьте амбіціозними, комунікабельними, відповідальними, щирими та проявляйте лідерські якості. Ідеальних не буває, але ви повинні прагнути бути професіоналом у своїй справі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. https://careers.easternpeak.com/blog/top-soft-skills-for-programmers/
2. https://www.forbes.com/sites/carolinecastrillon/2022/09/18/why-soft-skills-are-more-in-demand-than-ever/?sh=58c6d02c5c6f
3. https://www.forbes.com/advisor/education/soft-skills-for-tech/
4. https://itexpert.work/uk/ne-lyshe-kodyng-top-8-soft-skills-dlya-programista/

4 КІБЕРЗЛОЧИННІСТЬ. ЕКОНОМІЧНЕ ШАХРАЙСТВО В ІНТЕРНЕТІ

Доповідачі: Микола ЦЮСЬМАК,
Артем ВАСИЛЬЄВ, Олександр ЯНАКІ
Керівник: Олена СКОРНЯКОВА
ВСП «Одеський технічний фаховий коледж
Одеського національного технологічного університету»

Вступ. Кіберзлочинність стала серйозною проблемою сучасного цифрового світу. З розвитком технологій та Інтернету кіберзлочинці знаходять нові способи здійснення незаконної діяльності в Інтернеті.

Кіберзлочинність - це широке поняття, що описує кримінальну діяльність, яка здійснюється в інтернет-просторі, з метою отримання неправомірної вигоди або доступу до особистої інформації. Дослідження показують, що кожні три секунди на когось скоюється кіберзлочин.

Кіберзлочин - це злочинні дії, які здійснюються віртуально або за допомогою комп'ютерних технологій. Це можуть бути різні види злочинів, включаючи крадіжку особистих даних, шахрайство, шпигунство, атаки на комп'ютерні системи та мережі, віруси та інші шкідливі програми.

Згідно зі статистикою, кіберзлочинність постійно зростає, оскільки залежність людей від комп'ютерів і Інтернету стає все більшою. Зокрема, розповсюдження кіберзлочинів зросло під час пандемії COVID-19, коли багато людей стали працювати з дому та проводити більше часу в Інтернеті.

Кіберзлочинні дії можуть призвести до крадіжки конфіденційної інформації, фінансових втрат, шкоди репутації, порушення приватності та інших негативних наслідків для жертв. Типовими прикладами кіберзлочинства є фішинг, хакінг, віруси, крадіжка даних, електронні афери та інші злочинні дії, які вчиняються в електронному середовищі.

Кіберзлочинство є серйозною загрозою для суспільства, оскільки залежність від інформаційних технологій росте, а злочинці постійно розвивають нові методи здійснення злочинних дій. Для боротьби з кіберзлочинством необхідно вдосконалювати технічні засоби захисту, залучати кваліфікованих фахівців та забезпечувати підвищення кібербезпеки як на рівні окремих користувачів, так і на державному рівні.

Однією з найпоширеніших форм кіберзлочинності є Фішинг. Ми розглянемо концепцію кіберзлочинності, на прикладі саме фішингу, адже цей метод є одним з найпростіших для реалізації зі сторони кіберзлочинця, але може мати великі матеріальні та моральні втрати для жертви фішингу.

Фішинг - це метод атак на користувачів Інтернету, за допомогою якого зловмисники намагаються отримати конфіденційну інформацію (наприклад, логіни, паролі, номери банківських карток тощо) від своїх жертв. Це зазвичай відбувається через надсилання електронних листів, які містять підроблені повідомлення від відомих компаній, банків, соціальних мереж, прохання про допомогу, лотерейні виграші або інші подібні запрошення. Жертвам надсилають посилання на підроблені сайти, які дуже схожі на оригінальні, з метою злому їх облікових записів або отримання конфіденційної інформації, яку необережний користувач самостійно вводить.

Фішинг є загальним поняттям для низки способів та метдів інтернет- шахрайства. Їх можна класифікувати за підходом та цільовою аудиторією.

Методи фішингу:

Фішингові сайти - шахрайські веб-ресурси, які виманюють реквізити платіжних карток, під виглядом надання послуг, яких насправді не існує. Наприклад, шахраї можуть пропонувати поповнення мобільного рахунку або перекази з картки на картку, але насправді метою їх є збір реквізитів платіжних карток для подальшої крадіжки грошових коштів з рахунків власників карток. Більше 90% фішингових сайтів надають відсутні послуги з поповнення мобільного рахунку та переказу коштів з картки на картку.

Шахраї використовують різні методи, щоб залучити людей до своїх сайтів, такі як запит на перевірку, чи не була картка в складі бази даних хакерів, акції з безкоштовними переказами та поповненнями, або просто рекламу в соціальних мережах. Шахраї також використовують інструменти веб-маркетингу, такі як SEO-оптимізацію та контекстну рекламу, щоб залучити більше людей на свої сайти.

Останнім часом все більше фішингових сайтів налаштовуються на використання протоколу захищеної передачі даних HTTPS, який для користувача виглядає як абсолютно безпечний сайт.

Фішингові дзвінки, також відомі як "вішинг", є однією з форм фішингу, при яких зловмисники намагаються викрасти конфіденційну інформацію у потенційної жертви. Це робиться шляхом підроблення своєї особи і вигляду на телефоні як працівника банку, представника компанії або іншої організації.

Наприклад, зловмисник може зателефонувати жертві та заявити, що на її банківській карті виникли певні проблеми, і негайно потрібно їх вирішити. Він може запросити жертву на авторизацію на підробленому сайті, що нагадує офіційний сайт банку, та надати особисті дані, які ні в якому разі не можна розголошувати.

Такі дзвінки можуть бути дуже переконливими та виглядати дійсно автентичними, що збільшує ймовірність успіху атаки. Жертви часто не підозрюють, що вони стали жертвами шахраїв, і надають їм конфіденційну інформацію.

Смішинг - це форма фішингу, яка здійснюється за допомогою СМС-повідомлень. Зловмисник відправляє текстові повідомлення від імені відомої компанії або банку, в яких просить отримати доступ до фішингового сайту або надати особисту інформацію.

Діпфейк фішинг - це новий тип фішингової атаки, який використовує засоби відео та аудіо комунікації. Цей вид атак став особливо популярним під час коронавірусного локдауну.

Діпфейк фішинг включає в себе використання діпфейк технології для переконання співрозмовника у тому, що він спілкується з іншою людиною. Зловмисник може використовувати цей метод для викрадення особистих даних або вірусів, відправляючи посилання на шкідливий сайт через відео- або аудіодзвінок. У такому випадку жертва може навіть не здогадуватись про те, що її комп'ютер чи мобільний пристрій став жертвою кібератаки.

Соціальна інженерія є методом несанкціонованого доступу до інформації або систем зберігання даних без використання технічних засобів. Дослідження показують, що люди мають певні поведінкові схильності, які можуть бути використані для маніпулювання. Більшість зломів систем безпеки стаються саме завдяки використанню соціальної інженерії, а не через електронний злам. Це відбувається через те, що дії людини можна передбачити, маніпулювати ними, та як результат отримати з цього вигоду, яку жерта сама й надає через навіювання вибору. На основі людської довірливості і будуються усі методи фішингу, а через те що таких людей у середовищі Інтернету велика кількість- методи фішингу і є найпоширинішими серед кіберзлочинів

Фішинг може бути дуже небезпечним, оскільки зловмисники можуть використовувати отриману конфіденційну інформацію для здійснення шахрайства або крадіжки особистих даних, коштів.

Ми використаємо результати опитування 44 осіб, щоб зрозуміти, наскільки поширені випадки кіберзлочинств, їх основні методи, групи ризику та як люди можуть захистити себе від таких нападів.

Опитування та результати дослідження.

Наше опитування охоплює 44 особи, з яких 15 студенти групи 2КС-58, опитування яких проводиося через форму опитування у соціальній мережі, інші учасники це друзі, знайомі та родичі, опитування яких проводилося індивідуально до кожного. Результати опитування показали, що 19 учасників ніколи не стикалися з кіберзлочинністю, або мали настільки незначний контакт, який можна скоріш віднести до незначних перешкод як наприклад спам, чи набридлива реклама. 16 учасників стикалися, але не зазнали збитків через те, що вчасно усвідомили ситуацію та перешкоджали діям злочинців не даючи скоїти злочин по відношенню до себе. Інші 9

учасників опитування стикалися з кіберзлочинністю та зазнали матеріальних, а деякі й моральних збитків. 8 з них зазнали збитків саме в результаті фішингу.

Згідно з результатами опитування можна зрозуміти, що літні люди, яки є основною кількістю учасників 3 групи опитування, найбільш піддатні до впливу кіберзлочинності через, зазвичай, низький рівень комп'ютерної грамотності по відношенню до членів інших груп.

Группа, що була опитана	Кількість	Форма опитування	Не стикалися з кіберзлочинністю	Стикалися, не понесли збитків	Стикалися, понесли збитків
Студенти групи 2КС-58	15	Опитування у соц мережі	5 (33%)*	8 (53%)	2 (13%)
Друзі учасників 2 групи дослідницького проекту	17	Індивідуальне опитування	7 (41%)	7 (41%)	3 (18%)
Родичі учасників 2 групи дослідницького проекту	12	Індивідуальне опитування	7 (58%)	1 (8%)	4 (33%)
Всього учасників:	44	Всього за випадками:	19 (43%)	16 (36%)	9 (20%)

*Вказано відсоток кількості голосів кожної групи за різні варіанти опитування

З результатів також видно що фішинг атаки є поширеною формою кіберзлочинності і що люди повинні вжити заходів, щоб захистити себе від таких атак.

Захист від фішинг атак:

Є кілька кроків, які люди можуть зробити, щоб захистити себе від фішинг атак.

Першим кроком є усвідомлення ризиків, пов’язаних з нападами. Особам слід остерігатися електронних листів або веб-сайтів, які просять надати особисту інформацію, зокрема облікові дані для входу або фінансову інформацію. Їм також слід бути обережними, натискаючи посилання або завантажуючи вкладення з невідомих джерел.

Другим кроком необхідно завжди перевіряти адресу сайту, який запитує в вас конфеденційні дані. Усі офіційні адреси сайтів зазвичай лаконічні, не мають помилок у написанні, зайвих символів. Якщо ви не впевнені у тому, справжній сайт це, чи підробка, є варіант скористатися сервісом пошуку інформації по домену сайту, який має мати дату регістрації відповідну до сервісу. Для цього треба скористатись одним за сайтів для пошуку інормації по домену, наприклад www.godaddy.com/en-uk/offers/whois-b , де треба ввести адресу сайту та знайти дату його регістрації. Якщо дата регістрації очевидно не співпадає з реальним віком ресурсу- скоріш за все цей сайт підробка.

Ще один спосіб захисту від фішинг атак — використання надійних паролів і двофакторної автентифікації. Кіберзлочинцям важко вгадати надійні паролі, а двофакторна автентифікація додає додатковий рівень безпеки процесу входу, тож без додаткових зусиль злому кіберзлочин по відношенню до вас не відбудеться. Крім того, люди повинні постійно оновлювати своє програмне забезпечення та системи безпеки, щоб захистити їх від відомих уразливостей. Для цього компанії- розробники програмного забезпечення регулярно збирають статистику від користувачів, аналізують проблеми та розробляють план їх вирішення та захисту. Саме тому варто повідомляти у

підтримку сервісу, банку, додатку про атаку, аби попередити та вберегти від атаки інших.

Соціальний рух, направлений на оповіщення про нові загрози зі сторони кіберзлочинців та підвищенню комп'ютерної грамотності серед законослухняних користувачів Інтернету сприяє позитивному зменшенню типових випадків шахрайства.

Кримінальна відповідальність.

Важливо пам'ятати, що кіберзлочинство є правопорушенням, несе кримінальну відповідальність та визначається Кримінальним кодексом України, а саме у розділі 16 Кримінального кодексу України «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» містить статті, які охоплюють різні види кіберзлочинів:

Стаття 361 передбачає кримінальну відповідальність за несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Ця стаття застосовується до тих, хто намагається отримати несанкціонований доступ до систем та мереж.

Стаття 361-1 передбачає кримінальну відповідальність за створення та розповсюдження вірусів, незалежно від мети таких дій. Ця стаття застосовується до тих, хто зловживає технічними засобами з метою завдати шкоди.

Стаття 362 передбачає кримінальну відповідальність за несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації. Ця стаття застосовується до тих, хто зловживає своїм правом доступу до конфіденці

Спираючись на це право, ви можете звернутися до поліції зі скаргою на кіберзлочинство, скоєне над вами. Але складність полягає у тому, що більшість кіберзлочинців в Інтернеті діють повністю анонімно та відслідкувати їх, а значить спіймати та притягнути до відповідальності майже неможливо, якщо шахрай сам не залишив на себе доказів. Тож можна визначити, що відповідальність за свою конфіденційну інформацію та положення в інтернеті у першу чергу та загалом залежить лише від вас самих.

Висновок. Підсумовуючи, кіберзлочинність викликає серйозне занепокоєння в сучасному цифровому світі, а Фішинг є поширеною формою кібератак. Результати нашого опитування 44-ох осіб підкреслюють поширеність кіберзлочинності та фішингу, як її течії, та потребу людей вживати заходів для захисту від таких нападів. Усвідомлюючи ризики, використовуючи надійні паролі та двофакторну автентифікацію, оновлюючи програмне забезпечення, люди можуть зменшити ризик стати жертвою кіберзлочинців. Вкрай важливо, щоб люди вживали цих заходів, щоб захистити себе від кіберзлочинності та гарантувати, що їх особиста інформація залишається в безпеці та захищеності в Інтернеті.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник. за заг. ред. д-ра техн. наук, професора В. Б. Толубка. К.: ДУТ, 2015. 288 с.

2. Горова С.В. Кіберпрофесіонали і кіберзлочинність // Боротьба з організованою злочинністю і корупцією (теорія і практика): науковопрактичний журнал. Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю. Київ, 2014. № 2 (33), спецвипуск. С. 170-173.
3. Гринчак І.В. Кіберзлочинність як злочин міжнародного характеру. Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького: право, економіка /ІваноФранківський університет права імені Короля Данила Галицького. ІваноФранківськ, 2017. Вип. 12. С. 93-98.
4. Таволжанський О. В. Питання визначення кіберзлочинності в умовах розбудови інформаційного суспільства. Журнал східноєвропейського права. 2017. Вип. 45. С. 97-103.

5 ПСИХОЛОГІЯ ВІРТУАЛЬНОГО ПРОСТОРУ: ЗАЛЕЖНІСТЬ ВІД СОЦІАЛЬНИХ МЕРЕЖ

Доповідачі: Рената ХОТЯКОВА, Юлія ТКАЧУК, Дарія ГРАБОВСЬКА
Керівник: Олена СКОРНЯКОВА
ВСП «Одеський технічний фаховий коледж Одеського національного технологічного університету»

Однією з основних ознак розвитку сучасного суспільства є стрімкий розвиток комп'ютерних інформаційних технологій, який дає можливість сучасній людині навчатися, обговорювати проблеми, які турбують, знайомитися та спілкуватися з друзями, а також перенестися в будь-яку країну світу, дізнатися про її культуру та традиції, використовуючи необмежені можливості всесвітньої мережі Інтернет. І велику роль у нашому житті відіграють соціальні мережі.

Ми вирішили сконцентруватися саме на соціальних мережах і на їх вплив на підлітків.

Нарівні з позитивними сторонами, соціальні мережі мають і негативні наслідки – це інтернет-залежність, вплив на сон і психологічне здоров'я, заниження самооцінки, економія або відсутність часу на живе спілкування. Соціальні мережі, відсуваючи на другий план класичні інститути соціалізації – родину, школу, друзів, – займають усе більш домінуючу роль у процесі соціалізації особистості й здійснюють безпосередній вплив на її ціннісні орієнтації. Усі ці аспекти підштовхнули нас дослідити тему «Вплив соціальних мереж на людину та сучасне суспільство».

Актуальність дослідження полягає у тому, що соціальні мережі на сьогоднішній день об'єднують мільйони підлітків, які спілкуються між собою. Тому є важливим дослідити вплив соціальних мереж на формування їх особистості.

За допомогою тесту нам вдалося опитати людей віком від 14 до 40 років. Серед опитуваних переважну кількість складають саме підлітки. Ми вирішили сконцентруватися саме на цій віковій категорії, тому що на сьогоднішній день соцмережі об'єднують мільйони підлітків, які спілкуються між собою. Тому є важливим дослідити вплив соціальних мереж на формування їх особистості.

Серед опитаних нами людей – найпопулярнішою є соц. Мережею є телеграм, на другому місті – ютуб, на третьому – інстаграм, на четвертому тікток, і найменш популярні – фейсбук і твітер.

Взагалі в YouTube зареєстровано понад 28 млн українських користувачів, в Instagram – понад 16.1 млн, у Facebook – 15.45 млн. TikTok має більше ніж 12 млн українських користувачі.

Тут ми можемо побачити, що 65% опитуваних полюбляють контент, пов'язаний з їх інтересами, близько 16% полюбляють розважальний контент, і близько 13% полюбляють науковий контент.

Насправді, чіткого визначення що таке контент не існує, оскільки контент настільки глибоко проник у життя сучасних користувачів інтернету, що майже вся інформація, яку ви можете зустріти і є контентом.

Існує хибне твердження про те, що контент, який ми споживаємо, має бути виключно навчальним і мати якийсь сенс. Але це не так, бо через постійний потік корисної інформації наш мозок дуже перенапружується і потребує відпочинку. Саме для цього і існує розважальний контент. Він не напружує, розслабляє, і дає змогу відпочити.

Більш ніж 30% опитуваних проводять більше 6 годин на день у соцмережах, а 25% опитуваних не змогли б відмовитися від них. Це свідчить про залежність від соцмереж.

Можливі причини виникнення залежності:

Задоволення від лайків і приємних коментарів. Коли людина викладає допис чи фото у будь-якій із соцмереж, вона заздалегідь не знає, якою буде реакція друзів. Невідомість і можливість великої кількості лайків чи схвальних коментарів вивільняють дофамін, який викликає почуття щастя й ейфорії.

Не потрібно прикладати жодних зусиль. Погодьтесь, для того щоб погортати ленту соцмереж або подивитися відео не потрібно напружуватись і щось робити. Різноманітні додатки і соцмережі це один з найлегших варіантів дозвілля.

Можливість приховати свої «недоліки», бути «ідеальним». У соцмережах ми маємо змогу корегувати свої «недоліки». Це стосується не тільки зовнішності, але й особистості в цілому. Люди можуть видавати себе за інших, або створювати хибне уявлення про себе, таким чином роблячи себе «ідеальними» і зовні, і всередині.

Інтернет-залежність частково виникає тому, що людина в реальному житті не може задовольнити певні свої потреби, тоді й починає робити це в мережі. Наприклад, хтось має низьку самооцінку і намагається у віртуальному світі показати себе іншим / іншою, хтось шукає однодумців або намагається втекти від утоми чи напруги.

Що робить нас такими залежними? Річ у тім, що соціальні мережі є продовженням нас самих. За цим соціальним інстинктом ховається ще сильніша необхідність надання сенсу та цілей нашому світу. Спілкування з іншими дозволяє нам створювати цілі соціальні всесвіти із символів – наприклад, мову, цифри, жести, смайлики – та соціальні правила, які поділяються та зрозумілі кожному.

Також страх пропустити щось є великою рушійною силою використання соціальних мереж, особливо для людей віком до 30 років. Шістдесят сім відсотків користувачів кажуть, що вони бояться, що "щось упустять".

Для розвитку та вкорінення его потрібна платформа, де індивід може себе демонструвати, і соціальні мережі - ідеальне рішення. Вісімдесят відсотків наших розмов в Інтернеті є саморозкриттям порівняно з 30-40 відсотками розмов в автономному режимі. Ми живемо у суспільстві "Я" з нав'язливою ідеєю "я", яка змушує нас оновлювати свій статус і відзначати себе на фотографіях (але, звичайно, лише ті, на яких ми добре виглядаємо).

Соціальне порівняння з іншими людьми та підвищення самооцінки. Люди схильні порівнювати себе, щоб оцінити почуття, сильні та слабкі сторони, здібності та перспективи. Підтвердження ваших соціальних зв'язків змушує вас почуватися значно.

Спілкування має бути з людиною. "Неможливо не спілкуватися" - одна з ключових основ, прийнятих у соціальній та клінічній психології. Соціальний світ конструюється через взаємодію між людьми: ролі, правила, категоризації, стереотипи, нормальність, відхилення – це результати людського спілкування, результат нашого буття людьми, – коментує доктор Ретлідж.

Таким чином, соціальні мережі є продовженням нашого найглибшого психологічного інстинкту: бути соціальними. Вони стають якимось створеним всесвітом без часу і простору, які необхідні в умовах реального життя і для багатьох цей фактор є свого роду визволенням.

Серед вказаних симптомів найрозповсюдженими є такі: порушена концентрація уваги; постійне бажання зайти в соцмережі; порушення пам’яті; фізичне чи розумове виснаження.

25% людей відповіли, що вони часто порушують свій режим сну через соціальні мережі. Дослідження свідчать, що штучне світло пригнічує вироблення гормону мелатоніну, який сприяє сну. Найгірше впливає на нього блакитне світло від екранів смартфонів та ноутбуків.

Вчені виявили, що блакитне світло, яке випромінюють наші ґаджети, відіграє суттєву роль у порушенні сну.

Дослідники, однак, не з'ясували остаточно, чи саме соціальні мережі спричинюють розлади сну, чи це ті, хто вже страждає на безсоння, проводять більше часу в мережах.

Порушення сну може бути не тільки через залежність. Часом буває настільки насичений день, що не було часу на відпочинок і тому вночі хочеться надолужити втрачене, посидівши у соціальних мережах.

Майже всі опитувані виділяють достатньо годин на сон. Хоча, людям підліткового віку бажано спати 8-10 годин на день. Жіночі журнали з фотографіями надто худорлявих моделей, до того ж обробленими у Photoshop, вже давно визнані джерелом низької самооцінки у молодих жінок. Але тепер занепокоєння в деяких груп активістів почали викликати й соціальні медіа. Близько 38% опитуваних вважають, що вони недостатньо привабливі.

Соцмережі спотворюють сприйняття зовнішності. Facebook, Instagram і Snapchat дають можливість накладати на фото фільтри, завдяки яким будь-яка людина може мати інакший вигляд.

Науковці із Гарвардської медичної школи Мак Лін стверджують, що підлітки, які є активними користувачами соцмереж і водночас проходять період статевого

дозрівання і гормональних перебудов, найбільше страждають від "розриву", який створюють фільтри між реальністю та зображенням на екрані. Це сприяє розвитку депресії, розладу харчової поведінки і невпевненості в собі.

Також варто зазначити про тривожність. Багато молодих людей і підлітків можуть відчувати підвищену тривожність, пов'язану із спілкуванням у соціальних мережах. Вони можуть відчувати тиск, постійно публікувати ідеальні фотографії та писати ідеалізовані дописи, які розміщують разом із фото. Дотримуватися негласних правил соціальних медіа може бути важко, і в результаті підлітки починають відчувати високий рівень тривожності.

Молодих людей постійно бомбардують інформацією про те, що роблять їхні друзі, однолітки та кумири, через що вони можуть почуватися самотньо. І, якщо їхні постинги не отримують достатньо «лайків» і коментарів, порівняно з їхніми друзями, молоді люди можуть відчувати невиправдану, необґрунтовану тривожність та починають думати, що вони недостатньо хороші.

Для юнаків і дівчат, які вже борються з тривожністю, використання соціальних мереж може посилити таку проблему. Підлітки можуть відчувати занепокоєння щодо того, що саме вони публікують, як часто вони це роблять, скільки «лайків» і коментарів вони отримують. Дівчата можуть відчувати ще більше занепокоєння, зумовлене спілкуванням в Інтернеті, оскільки вони більше схильні турбуватися про свій імідж і можуть особливо постраждати від кібербулінгу та слат-шеймінгу.

Близько 90% опитаних відповіли, що інформація в соцмережах впливає на їх особисті переконання. Соціальні мережі – один із найсильніших інструментів впливу на людину, що здійснює безпосередній вплив на її ціннісні орієнтації. Перебуваючи у віртуальному світі та вивчаючи ту інформацію, яка розміщена у соціальних мережах, кожен із нас формує свою систему цінностей, яка визначає виняткове ставлення до певних дій, вчинків, явищ як віртуального, так і реального життя; визначає нашу поведінку та майбутню соціальну діяльність, що становить собою ціннісний компонент. У соціальних мережах ми черпаємо стереотипи та моделі поведінки, норми діяльності, формуємо свою соціальну ідентичність, власну самооцінку, що не завжди є адекватною.

25% опитуваних знаходяться у комфортних для себе закритих спільнотах. Це добре, з одного боку, бо закриті спільноти об'єднують людей за спільними інтересами, що дозволяє підлітку задовольнити сильну потребу у спілкуванні адже підлітковий період – це час, коли людина прагне знайти схожих собі за інтересами, вподобаннями.

Але, з іншого боку, якщо дуже багато проводити в них час , то через хибне сприйняття реальності світ може здаватися жорстоким , таким чином можна повністю абстрагуватися від реального спілкування, через що може з'явитися соціофобія та багато інших психологічних проблем.

У 38% опитуваних є інтернет друзі. Безперечно, декому легше дружити он-лайн. В Інтернеті почуваєшся набагато впевненіше, ніж у реальному житті. Також віртуальне спілкування дає можливість сором'язливій людині наперед обдумати свої слова.

Головне не забувати, що ми всі живемо в соціумі і всім людям треба володіти хоча б мінімальними навичками комунікації у реальному житті

Дослідження, опубліковане минулого року в "Американському журналі превентивної медицини", в якому взяли участь 7 тисяч людей у віці від 19 до 32 років,

показало, що ті, хто проводить багато часу в соціальних мережах, вдвічі частіше почувають себе соціально ізольованими. Їм бракує відчуття приналежності групі, а також взаємодії з іншими та повноцінних стосунків.

Але, в нашому випадку все навпаки. 37% людей соцмережі саме рятують від самотності, тож це є позитивним впливом.

Більшість відповіли, що соцмережі впливають на їх життя і позитивно, і негативно. Дійсно, однозначно неможливо визначити їх вплив на наше життя. Серед позитивного впливу можна зазначити такі аспекти як:

Дослідження та критичне мислення. Інтернет надає доступ до багатьох інформаційних ресурсів, які допоможуть підліткам дізнатися багато цікавого й корисного. Це може стати у нагоді під час навчання у школі чи виші або для дослідження сфер інтересів. Також варто навчати дітей, як аналізувати інформацію, щоб вибирати надійні джерела.

Зближення та спільнота. Соціальні мережі можуть сприяти підтриманню зв'язків, дозволяючи підліткам залишатися вдома, але водночас мати контакт з іншими членами сім'ї або друзями, які не живуть поруч. Крім того, підлітки можуть взаємодіяти з іншими у своїй віковій групі, граючи в онлайн ігри, і навчаючись грати в команді.

Самовираження. підлітки можуть навчитися ділитися своїми думками в Інтернеті, що є потужним інструментом для зміцнення впевненості. Вони можуть навчитися спілкуватися з іншими та оцінювати інші точки зору або думки, відмінні від їхніх власних.

Творчість і дослідницькі інтереси. У багатьох відношеннях сучасні технології сприяють творчості та навчанню новим навичкам за допомогою спеціальних програм для різного віку. підлітки можуть досліджувати різні сфери життя, якими вони цікавляться, наприклад, навчання грі на музичному інструменті, написання текстів на задану тему, або вивчення інформації для початківців («чайників»), пов'язаної з різними предметами. Треба зрозуміти, що не саме існування соцмереж може нам нашкодити, а те, що люди не навчилися правильно ними користуватися. Якщо б у соцмережах люди дійсно були б собою, не боялися «невдалих» ракурсів, були б толерантні один до одного і розповсюджували корисну інформацію, то негативного впливу було б набагато менше.

Які поради, на думку опитувачів, мають допомогти людям з інтернет-залежністю:

- Обмежити користування соц. мережами за допомогою таймера або спеціальних програм.
- Заняття спортом, читання або власне хобі (щоб не було вільного часу на соц. мережі).
- Намагатися здобувати інформацію в інших джерелах, а не в інтернеті.
- Не варто ризикувати своїм психічним і фізичним здоров'ям заради віртуального схвалення вашого життя. Іноді важливо та навіть корисно бути поза зоною досяжності. Тому намагайтеся балансувати час, який ви проводите в соціальних мережах і телефонах.

І важливо пам'ятати, що без вашого бажання реально почати контролювати свою присутність у мережах, дива не станеться. Тут справа так само, як з іншими залежностями.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Махній М.М. Мережеве суспільство: кіберпсихологічний путівник. Київ: Academia.edu, 2018. 176 с.
2. Быть человеком. Взаимодействие человека и компьютера в 2020 году. Под ред. Р. Харпера, Т. Роддена, И. Роджерса, Э.Силлена. Исследования корпорации Microsoft, 2014. URL: http://download.microsoft.com/documents/rus/
3. Культура віртуального спілкування: методичні поради /Упр.культури, національностей та релігій Хмельниц.облдержадмін.; ХОУНБ ім.М.Островського. Хмельницький, 2014. 28 с. URL: http://www.ounb.km.ua/vidanya/2014/kvs.pdf
4. Онищенко О. С., Горовий В. М., Попик В. І. Соціальні мережі як чинник розвитку громадянського суспільства : [монографія]/ Онищенко О. С., Горовий В. М.,Попик В. І.; НАН України, Нац. б-ка України ім. В. І. Вернадського. – К., 2013. –220 с
5. CIBERPSY – портал, присвячений кіберпсихології. URL: http://cyberpsy.ru

6 ПСИХОЛОГІЯ ВІРТУАЛЬНОГО СПІЛКУВАННЯ. КІБЕРСОЦІАЛІЗАЦІЯ ОСОБИСТОСТІ

Доповідачі: Юрій ЄПУР, Володимир ОВЧАРЕНКО,
Денис ФІЛЕНКО, Ілля БИЧЕНКО,
Нікіта КІТАЄНКО, Олександр ВИТИКАЧ
Керівник: Олена СКОРНЯКОВА
ВСП «Одеський технічний фаховий коледж
Одеського національного технологічного університету»

У сучасному світі соціалізація людини проходить в умовах глобальної та всепоглинаючої цифровізації. Така трансформація процесу соціалізації визначається сучасною наукою як кіберсоціалізація особистості. Даний термін доречно застосовувати до так званого цифрового покоління, яке має свої певні відмінні характеристики.

До цифрового покоління належать люди, які більшу частину свого життя взаємодіють з цифровими інформаційно-комунікаційними технологіями, які звикли отримувати інформацію через цифрові канали. Цифровому поколінню протиставляється аналогове покоління – люди, які народились до цифрової 2 революції. Найбільш молоді представники аналогового покоління названі «цифровими іммігрантами», а найстарші представники цифрового покоління – «цифровими аборигенами». Умовним початком цифрової революції та зміни поколінь вважається перша половина 80-х років XX століття.

Найстарші представники покоління зумерів народились в часи початку стрімкого поширення в нашій країні персональних комп'ютерів та Інтернету серед домашніх користувачів. Проте більшість з них познайомились з цифровим світом в молодшому шкільному або підлітковому віці одночасно зі зростанням популярності комп'ютерних ігор та перших соціальних мереж. Та все ж таки до цього моменту в них була можливість сформувати свої цінності та особистісні межі без тісної взаємодії з кіберпростором.

Дітям «альфа» Інтернет та смартфон доступні практично від самого народження та є продовженням їх власної реальності, в них набагато сильніше ніж у зумерів розмиті

межі онлайн та офлайн, а публікація особистого контенту в соціальних мережах є нормою.

Хоча процес соціалізації й відбувається на протязі всього життя особистості, проходячи низку важливих стадій, та все ж таки найбільшої актуальності проблема кіберсоціалізації на сьогодні набуває серед представників цих двох поколінь.

У сучасній науці існує два основних підходи до визначення феномену кіберсоціалізації особистості.

Згідно першого підходу кіберсоціалізація розглядається як сукупність феноменів, пов'язаних з залученням людини до культури електронної 3 комунікації, а також засвоєнням норм, цінностей та правил, що визначають специфіку спілкування та взаємодії в кіберпросторі. Тобто кіберсоціалізація зводиться до процесу входження людини до кіберспільноти, прийняття норм, цінностей та правил поведінки в ній. У даному випадку, вектори кіберсоціалізації та традиційної класичної соціалізації можуть розходитися – людина може бути успішно соціалізована в реальному світі та несоціалізована у віртуальному або навпаки.

Другий підхід, започаткований В.А. Плєшаковим, визначає кіберсоціалізацію як процес якісних змін структури самосвідомості особистості та мотиваційно-потребової сфери під впливом інформаційно-комунікаційних технологій. Таке визначення дає можливість розуміти кіберсоціалізацію як процес соціалізації представників цифрового покоління в умовах змішаної реальності.

Кіберсоціалізацію можна розглядати як у позитивному так і в негативному контексті.

Під позитивною кіберсоціалізацією розуміється сукупність процесів 4 безпечного освоєння користувачем кіберпростору, повноцінного використовування його переваг та перенесення корисного досвіду, отриманого у віртуальному середовищі на розв'язування важливих задач у реальній дійсності.

Цифрові технології надають молоді необмежені можливості для навчання, створення та розповсюдження власного контенту, реалізації творчих проєктів, дозволяють стати рівноправними суб'єктами в комунікації між поколіннями, активними творцями інформаційного простору, виражати власну думку та заявляти про свої інтереси. Інтернет відкриває доступ до надзвичайно корисного контенту: онлайн-бібліотеки, фільмотеки, віртуальні вистави, музеї, галереї концертні зали, тематичні парки тощо.

У той же час, негативна кіберсоціалізація характеризується високим рівнем занурення людини у віртуальні комунікації разом з низькою здатністю до саморегуляції при використовуванні інтернет-ресурсів, наявністю девіантних патернів при спілкуванні в інтернет-середовищі та високою вразливістю до агресивного віртуального світу. Інтернет містить величезний об'єм некорисної, низькоякісної інформації маніпулятивного та деструктивного характеру, що може негативно вплинути на формування особистості, сприяти формуванню хибних цінностей, залучанню її до девіантної поведінки.

Отже, кіберсоціалізація сьогодні стає особливим видом традиційної соціалізації та передбачає набуття соціального досвіду представниками найбільш молодого покоління в умовах життя у змішаній реальності та взаємодії з нею. Кіберсоціалізація може

проходити стихійно, а може бути контрольованою. Тому основним завданням сучасних наукових досліджень в даній області є, перш за все, виділення методів супроводження цього процесу, пошук ефективних інструментів його безпечного протікання.

Психологія віртуального спілкування

Віртуальне спілкування - це комунікація між людьми, яка відбувається за допомогою різноманітних електронних засобів зв'язку, таких як електронна пошта, соціальні мережі, чати, форуми та інші. Віртуальне спілкування може здійснюватися на відстані, без присутності співрозмовників один з одним в одному місці.

Основні характеристики віртуального спілкування:

1. **Електронне середовище** - спілкування відбувається за допомогою електронних засобів зв'язку, таких як комп'ютер, телефон або планшет.
2. **Асинхронність** - спілкування може відбуватися в будь-який зручний час для користувачів, інформація може передаватися неодночасно.
3. **Широкий аудиторіум** - віртуальне спілкування може здійснюватися з користувачами з різних країн та часових зон.
4. **Спрощення комунікації** - можливість спілкування в будь-якому місці та в будь-який час спрощує процес комунікації.

Види віртуального спілкування:

1. **Електронна пошта** - спілкування за допомогою електронної пошти.
2. Чати та месенджери - спілкування в режимі реального часу за допомогою текстових повідомлень.
3. **Форуми** - спілкування на спеціальних веб-сайтах за певною темою.
4. **Соціальні мережі** - спілкування на веб-сайтах, де користувачі можуть створювати свої профілі та обмінюватися повідомленнями, фото та відео.
5. **Відеозв'язок** - спілкування за допомогою відеозв'язку.

Інтернет міцно увійшов в життя людей, будучи не тільки джерелом інформації, а й засобом комунікації. Комп`ютерна комунікація має ряд особливостей в порівнянні з реальним спілкуванням. До цих особливостей відносять наступне:

- Розширення можливостей і меж комунікації, оскільки співрозмовників можна знайти у всіх країнах світу;
- Обидва партнери в процесі комунікації знаходяться в звичному життєвому просторі, користуючись різними прийомами передачі інформації;
- Віртуальне спілкування переважно здійснюється в письмовій формі (чат, e-mail), що дає можливість удосконалювати вміння і навички писемного мовлення;
- Крім вдосконалення мовних знань, учасники комунікації отримують про особу партнера інформацію про його поглядах на навколишній світ;
- Обмін повідомленнями дозволяє удосконалювати вміння розуміти письмовий текст, який супроводжується при необхідності поясненнями носія мови, що вивчається. Регулярний обмін електронними листами при віртуальної комунікації дозволяє вдосконалити вміння і навички писемного мовлення, збагачує словниковий запас, розширює соціокультурну компетенцію і кругозір, удосконалює навички роботи з інтернетом.

Для того щоб спілкування у віртуальному просторі не принижувало людину, а, навпаки, сприяло її особистісному зростанню необхідно дотримуватися

загальноприйнятих етичних вимог, правил мережевого етикету. З появою Інтернету в наше життя навіть увійшло таке поняття, як “нетикет” (netiqutte — від англ. net — мережа та франц. etiqutte — етикет).

Сформовано такі правила мережевого етикету:

- пам'ятайте, що Ви розмовляєте з людиною. Не робіть іншим те, чого не хочете отримати від них самі. Поставте себе на місце людини, з якою розмовляєте. Відстоюйте свої погляди, але не ображайте тих, хто навколо Вас. Не забувайте про головний принцип мережевого етикету: повсюдно в мережі знаходяться реальні люди. Будьте терплячі й чемні. Не вживайте ненормативну лексику, не йдіть на конфлікт заради самого конфлікту;

- дотримуйтесь тих самих стандартів поведінки, що й у реальному житті. Люди інколи забувають про те, що "за екраном" знаходиться жива людина, і вважають, що в мережі правила поведінки не такі самі, як у звичайному житті. Не вірте тому, хто каже: "Вся етика спілкування тут полягає в тому, що Ви самі для себе встановите". Якщо Ви стикаєтесь з проблемою етичного характеру в кіберпросторі, — уявіть, що Ви в реальному житті;

- пам'ятайте, що Ви перебуваєте у віртуальному просторі. Якщо Ви вирішили втрутитися в якусь дискусію, то можете зашкодити іншим. Опинившись у новій ділянці віртуального простору, спочатку озирніться. Витратьте час на вивчення обстановки, "послухайте", як і про що говорять люди. Тільки після цього приєднуйтесь до розмови;

- поважайте час і можливості інших. Коли Ви відправляєте електронну пошту або повідомлення до конференції, то фактично претендуєте на чужий час. І тоді Ви відповідаєте за те, щоб адресат не витратив цей час даремно. Слід також пам'ятати про пропускну спроможність каналу, через який відбувається зв'язок. Раніше, ніж Ви відправите людині свій лист, поміркуйте, чи він справді потрібен їй. Якщо ж Ви вагаєтесь, поміркуйте двічі, перш ніж відправити повідомлення;

- зберігайте особистість. У мережі (наприклад, у конференціях) Ви можете зустрітися з тими, кого ніколи б не зустріли в реальному житті, і ніхто не засудить Вас за колір шкіри, очі, волосся, за вашу вагу, вік або манеру одягатися. Однак Вас будуть оцінювати з точки зору того, як Ви пишете. Таким чином, правила граматики відіграють важливу роль. Крім того, переконайтесь, що Ваші послання зрозумілі й логічно витримані;

- допомагайте іншим там, де Ви це можете зробити. Задавайте запитання, спілкуючись у віртуальному просторі. Чому це ефективно? Тому що Ваші запитання читатимуть багато людей, які, може, знають на них відповідь. І навіть якщо кваліфіковано дадуть відповідь тільки декілька чоловік, загальний обсяг знань у мережі збільшиться. Обмін досвідом в Інтернеті — захоплююче заняття;

- не втручайтеся в конфлікти й не припускайте їх. Мережевий етикет проти злісних послань, якими іноді обмінюються окремі учасник дискусії;

- навчіться вибачати іншим їхні помилки. Коли хтось припускається помилки — будь це помилка в слові, безглузде запитання або невиправдано довга відповідь, — будьте до нього поблажливі. Якщо у Вас гарні манери, це ще не означає, що Ви маєте право нав'язувати їх усім іншим. Якщо ж Ви вирішили звернути увагу користувача на припущену помилку, зробіть це коректно й краще в приватному листі;

Кіберкультура та її феномени

Кіберкультура - це сукупність культурних явищ, що виникають у віртуальному просторі, а також змінюють та впливають на культуру та суспільство в цілому. Вона складається зі специфічних проявів та практик, які формуються в Інтернеті, віртуальних іграх, соціальних мережах, веб-сайтах та інших електронних середовищах.

Кіберкультура з'явилася разом з розвитком комп'ютерної техніки та Інтернету в кінці XX століття і стала феноменом культури нового технологічного етапу. Вона включає в себе такі прояви, як віртуальні ігри, мережевий активізм, віртуальну музику, художню літературу, фільми та інше.

Кіберкультура також охоплює різноманітні соціальні прояви, які формуються в електронному середовищі, такі як соціальні мережі, онлайн-спілкування, онлайн-купівля, електронна пошта, блоги та інші. У цих проявах відображаються соціальні та культурні зміни, які відбуваються в сучасному світі під впливом технологічного прогресу та масової доступності Інтернету.

Загалом, кіберкультура може розглядатися як своєрідний субкультурний рух, який визначається взаємодією людини та технології в електронному середовищі та відображається у створенні нових культурних цінностей та способів спілкування та взаємодії.

Кіберкультура є досить різноманітним явищем, яке включає в себе багато різних підкультур та рухів. Тому складно виділити конкретних представників кіберкультури, але можна назвати деякі з них:

Кіберпанк - це напрямок в науковій фантастиці, який виник у 1980-х роках. Кіберпанк характеризується песимістичним взглядом на майбутнє та великою увагою до технологій, комп'ютерів та кібернетики.

Хакерський рух - це група людей, які вивчають та експериментують з комп'ютерною технікою та програмним забезпеченням. Цей рух зародився в середині 20 століття та став одним із ключових чинників розвитку комп'ютерної техніки та кіберкультури.

Кіберспорт - це вид спорту, який виник на основі відеоігор. Це суспільне явище зародилося в 2000-х роках та стало досить популярним серед молоді. Кіберспорт включає в себе різноманітні турніри та змагання з різних відеоігор.

Розглянемо далі деякі з найбільш поширених Інтернет-субкультур.

Комп'ютерні гравці або геймери. **Геймери** — це прихильники комп'ютерних ігор, які вбачають в іграх сенс свого життя, тобто ігри є переважною об'єднавчою цінністю цієї спільноти. Найчастіше геймерами стають підлітки. Зазвичай, гра у підлітка забирає весь вільний від навчання час. Найбільш організованим різновидом геймерів є «квакери», прихильники комп'ютерної гри «Quake». Субкультура геймерів зародилася нещодавно. З появою комп'ютерних ігор, а згодом й Інтернету, молодь стала активно спілкуватися в мережі. Комп'ютерні мережеві ігри для них — це можливість спілкуватися в дії: разом з іншими, часто іноземними однолітками виконувати завдання та перемагати ворогів. Існують також і немережеві ігри, що мають розважальне завдання.

Хакери. Значення слова «хакер» у первинному його розумінні, імовірно, виникло в стінах Массачусетського технологічного університету в 1960-х рр., задовго до того, як

комп'ютери стали предметом масового користування. Тоді воно було частиною місцевого сленгу й могло означати просте, але грубе вирішення якої-небудь проблеми. Згідно з функціями, які виконують хакери, їх поділяють на хакерів-дослідників, хакерів-зломлювачів, вандалів, крекерів, вірмейкерів, кібертерористів, санітарів та кардерів.

Блогери. У класичному розумінні блогером називають будь-яку людину, яка має особистий журнал або щоденник в Інтернеті й час від часу залишає там записи (пости) різного характеру: особисті, рецензійні, новинні, коментарі. Блог — (англ. «web-log») у перекладі саме й означає «мережевий журнал» або «щоденник подій».

Тролі. Визначення «тролінг» зародилося в Інтернет-мережі на початку 1990-х рр. Якщо раніше зрідка виникали спроби поширювати провокаційні повідомлення в Інтернеті лише заради цікавості, то зараз будь-який знаний форум, сайт, група новин та інше, рано чи пізно зазнає тролінгу.

Нами було проведено опитування серед здобувачів 2-го курсу. Результати підтверджують наявну залежність від соціальних мереж у більшості опитаних. Залежність від соціальних мереж призводить до того, що людина більшість часу проводить в мережі, нехтуючи реальними контактами з родиною і друзями, відвідуваннями різноманітних заходів, інколи навіть сном. Велика кількість опитаних нами людей різного віку знаходяться в соціальних мережах понад 5 годин на добу, а це може призвести до затримки сну, депресії, часом втрати пам’яті. Чим більше часу протягом дня людина користується соціальними мережами, тим стає менш задоволена власними життям Зокрема через почуття заздрості: поширюючи інформацію про власні успіхи, не показуючи, як багато зусиль і праці докладаємо щодня, які цього не усвідомлюють, почуваються так, ніби їхнє життя непорівнюване з іншими в соціальних мережах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Культура віртуального спілкування: методикобібліографічні матеріали. К., 2010. 65 с.
2. Засоби комп'ютерної техніки з віртуальними функціями і нові інформаційні технології: зб. наук.праць. Т.1 Редкол.: В.О. Романов. К.: НАН УКраїни, 2002. 112 с.
3. Засоби комп'ютерної техніки з віртуальними функціями і нові інформаційні технології : зб. наук. праць. Т.2 / Редкол.:В.О. Романов та ін. К. : НАН УКраїни, 2002. 124 с.
4. Немеш О. М. Віртуальна діяльність особистості: структура та динаміка психологічного аналізу: монографія К. : Слово, 2017. 391 с.

7 БАЗОВІ ПРАВИЛА БЕЗПЕКИ В ЦИФРОВОМУ СЕРЕДОВИЩІ

Доповідач: Віра ГЕРМАШ
Керівник: Анастасія ДЗЮБАК
Чорноморський морський фаховий коледж
Одеського національного морського університету

Цифрове середовище – це електронних систем, програм і даних, які існують у цифровій формі. Воно включає в себе всі електронні пристрої, комп'ютерні мережі, Інтернет, програми, сервіси, веб-сайти, соціальні мережі та інші цифрові ресурси.

Цифрове середовище є важливою частиною сучасного світу, оскільки воно визначає спосіб, яким люди спілкуються, працюють, навчаються та розважаються. Воно надає можливість обмінюватися інформацією, створювати та зберігати дані, виконувати різноманітні завдання та спілкуватися з іншими людьми у віртуальному просторі.

Цифрове середовище також може включати такі технології, як штучний інтелект, віртуальна реальність, розширена реальність і блокчейн. Це створює нові можливості для розвитку в бізнесі, освіті, науці, медицині та інших сферах життя.

Однак, цифрове середовище також має недоліки, які можуть призвести до серйозних проблем, таких як кібербезпека, конфіденційність даних, цифрова нерівність і залежність від технологій.

Базові правила безпеки в цифровому середовищі:

1) використовуйте унікальні та складні паролі для всіх своїх облікових записів і пристроїв.

Поради щодо створення надійного пароля: він повинен бути достатньо легким для вас, щоб його запам'ятати і не забути, але складним для інших, щоб ніхто не міг його вгадати чи підібрати. Пароль має бути довгим, містити комбінацію великих і малих літер, цифр та спеціальних символів. Ви не можете використовувати той самий пароль для всіх акаунтів і додатків, а також паролі, які легко вгадати, наприклад: ваше ім’я, прізвище, номер телефону та іншу особисту інформацію про вас. Намагайтеся регулярно змінювати паролі;

2) активуйте двофакторну аутентифікацію, де це можливо зробити.

Це забезпечить додатковий рівень захисту, оскільки окрім пароля буде потрібно підтвердження через SMS-повідомлення або спеціальний мобільний додаток;

3) остерігайтеся невідомих посилань і вкладень

Не відкривайте підозрілі посилання або файли, які можуть пошкодити ваш пристрій або викрасти дані. Якщо посилання надійшло з надійного джерела, і ви все ще сумніваєтеся, тоді краще зв'язатися з відправником, щоб переконатися в його достовірності. Встановлення надійного антивірусного програмного забезпечення на ваш комп'ютер або мобільний пристрій допоможе виявити та заблокувати потенційно шкідливі файли та посилання. Якщо все ж таки ви вирішите перейти за цим посиланням, скористайтеся службою перевірки безпеки URL, яка допоможе вам визначити, чи є посилання безпечним;

4) ні за яких обставин не повідомляйте нікому свої особисті дані, паролі та коди, які ви можете отримати, коли намагаєтеся увійти у свій акаунт. Будьте обережні, надаючи особисті дані в Інтернеті, особливо на сумнівних веб-сайтах або через незахищені мережі Wi-Fi;

5) захистіть свої файли та документи за допомогою резервного копіювання;

6) оновлюйте програмне забезпечення

Потрібно регулярно оновлювати операційні системи, браузери та інші програми на своєму пристрої. Оновлення часто включають патчі безпеки, які закривають вразливості і зменшують ризик атак;

7) встановлюйте програми лише з офіційних сайтів;

8) не повідомляйте інформацію щодо ваших банківських карт та рахунків третім особам;

Повідомлення нібито від банківських установ про блокування вашого рахунку тощо. Зазвичай такі повідомлення містять заклики відправити дані. Наприклад, PIN-код картки; 16 цифр, що вказані на картці; термін дії картки, CVV-код. У цьому випадку необхідно зв'язатися з банком за офіційною електронною адресою або офіційним номером телефону для з'ясування ситуації.

9) обережно користуйтеся соціальними мережами та не розміщуйте там особисту інформацію;

10) остерігайтеся сайтів-двійників

Не залишайте свої особисті дані на незнайомих або підозрілих веб-сайтах. Нині поширеним є шахрайство, що полягає у створенні сайтів-двійників. Візуально сторінка виглядає як справжня: вона має таку саму кольорову гаму та містить приблизно таку ж інформацію, що й офіційний сайт, але гіперпосилання містять зайві літери чи цифри. Зробивши покупку або вказавши власні персональні дані на сайті-двійнику, ви потрапляєте у пастку шахраїв. Ви не зможете отримати необхідні вам товари чи послуги, а ваші персональні дані можуть бути використані проти вас. Тому переконайтеся, що ви справді перебуваєте на офіційному веб-сайті, перш ніж вводити свої дані;

11) остерігайтеся фейкових інтернет-магазинів

Фейкові інтернет-магазини можуть пропонувати товари, яких у них немає в наявності або які не в хорошому стані. Остерігайтеся продавців, які пропонують товари за надзвичайно низькими цінами, але вимагають часткової або повної передоплати. Для покупок в Інтернеті краще всього користуватися перевіреними інтернет-майданчиками, адміністратори яких можуть гарантувати повернення грошей, якщо товар не відправлений або неякісний. Якщо вам потрібно скористатися послугами невідомого інтернет-магазину, то обов'язково ознайомтеся з відгуками про продавця і купуйте товари з накладеним платежем, тобто сплачуйте вартість товару після отримання та огляду;

12) безпечне підключення до Wi-Fi мереж.

Висновки: Цифрове середовище в сучасному світі є надзвичайно важливим і поширеним. Інтернет, соціальні мережі, мобільні пристрої та інші цифрові технології використовуються людьми всіх вікових груп та в різних сферах життя. Однак, разом з перевагами, які ці технології надають, існує також ризик для безпеки та конфіденційності користувачів. Якщо дотримуватися базових правил безпеки в цифровому середовищі, тоді все буде добре і ви зможете захистити себе та свої дані.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про основні засади забезпечення кібербезпеки України, Закон України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
2. В. Ю. Биков, О. Ю. Буров, Н. П. Дементієвська. Кібербезпека в цифровому навчальному середовищі. Інформаційні технології і засоби навчання, 2019, Том 70, №2, С. 313 – 331.
3. Основні правила кібергігієни. URL: https://erepublic.org.ua/news/osnovni-pravilakibergigiyeni/
4. Кибербезопасность с человеческим лицом: как донести проблему до каждого. URL: https://trends.rbc.ru/trends/industry/5fa460199a7947a946d4b37e

5. Основні правила захисту даних — кібергігієна для активного Інтернет-користувача. URL: https://eset.ua/ua/blog/view/38/osnovnyye-pravila-zashchity-dannykh-kibergigiyena-dlyaaktivnogo-Internet-polzovatelya

8 МЕТОДИ І СТРАТЕГІЇ ВЕДЕННЯ ІНФОРМАЦІЙНОЇ ВІЙНИ - СПОТВОРЕННЯ ІНФОРМАЦІЇ ТА ФЕЙКИ

Доповідач: Євгеній НОВАК
Керівник: Анастасія КРИВЧЕНКО
ВСП «Одеський технічний фаховий коледж
Одеського національного технологічного університету»

Інформаційна війна – це один з методів ведення війни, можна сказати стратегія використання інформації, для досягнення певних цілей, використовуючи інформаційні джерела (ЗМІ). Також в інформаційну війну додають кібератаки та збір деякої інформації.

Виділяють чотири основних характеристики інформаційної війни. Це портворення інформації, фейки, цілеспрямована інформаційна атака та кібератака.

Спотворення інформації - це коли інформація, яка подається публіці спотвореною (тобто зі зміненим сенсом). Це може бути досягнуто шляхом зміни слів та контексту. Додавання або видалення інформації, які можуть впливати на сприйняття подій.

Тут виділяють такі риси:

Вибіркове використання фактів – використання фактів, що підтримують певну точку зору, а ігнорування тих, що суперечать їй. Це може бути зроблено шляхом вмілої редакції тексту, зміни контексту або просто вибору лише тих фактів, що підтримують певну точку зору.

Маніпулювання емоціями - це використання інформації, яка викликає сильні емоційні реакції у людей, щоб змінити їхню думку чи поведінку. Це може бути зроблено шляхом використання матеріалу, що викликає страх, ненависть або будь-які інші сильні емоції. Маніпулювання емоціями може бути використане для спрямування громадської думки у певному напрямі, навіть якщо емоційна реакція не відповідає дійсності.

"Відсебячина" у ЗМІ - це використання журналістами неперевірених та суб'єктивних даних, які можуть привести до непорозуміння або створити невірне уявлення про події. Це може включати використання помилкових фактів, неправильних контекстів та інших необґрунтованих тверджень.

Прикладом для цих трьох пунктів може бути така історія.

У 1998 році британський лікар Ендрю Вейкфілд опублікував дослідження, в якому він стверджував, що щеплення від кору та краснухи може спричинити аутизм та інші серйозні порушення розвитку у дітей. Це викликало паніку серед батьків та викликало різке падіння рейтингу щеплень.

Однак, пізніше стало відомо, що дослідження Уейкфілда маніпулійовало і не мало наукового підґрунтя. Журналіст та ЗМІ, ставився до цієї теми необ'єктивно, обирав лише факти, які підтверджували його упередженість, ігноруючи інші факти, які говорили про безпеку щеплень. Це призвело до того, що батьки почали масово відмовлятися від щеплень, що призвело до зростання смертності від різних хвороб, яких можна було б уникнути завдяки щепленням.

На цьому прикладі ми побачили як доктор вибірково використовуючи факти та придумуючи їх, маніпулював емоціями батьків, які хотіли уберегти своїх дітей від побічних ефектів.

Засмічення (або засорення) інформаційного простору. Це створення величезної кількості інформації, яка не має відношення до конкретногї проблеми або має думку, вигідну тим, хто «засмітчує», щоб утруднити доступ до правдивої інформації. Це може бути зроблено шляхом створення величезних обсягів повідомлень, використання ботів та автоматичних програм для створення повідомлень у соціальних мережах. Думаю всі бачили та знають що таке кремлеботи під постами та відео українців.

Вичислити таких «ботів» буває складно, але можна виділити декілька основних рис:

- відсутність фотографій обличчя в профілі
- відсутність власних постів, тільки репости інших
- молодий аккаунт
- серед репостів тільки політичні новини
- нелогічність та недоречність повідомлення

Під постом про річницю вторгнення Німеччини на територію радянського союзу. Боти розцінили це як пост про теперішнє вторгнення та почали його оправдовувати.

Фейки (fake news) – це дезінформація, яка представляється як справжні новини, але такими не є. Вони можуть бути створені та поширені з метою маніпулювання думкою людей. Від спотворення інформації відрізняється тим, що фейк це повністю (від А до Я) видумана історія.

Зазвичай фейкові статті одночасно вміщають в себе три пункти. Це:

- хибні події та факти
- перекручування контексту
- підроблені джерела

Як приклад, із найвідоміших статей в ЗМІ, які мали найжахливіший вплив, це газети Третього Рейху про євреїв. Ці статті поставили громадян Німеччини проти іудеїв та призвели до Голокосту.

Один із найвідоміших фейків, пов'язаних із євреями, це легенда про кривавий обряд, який, за твердженням нацистської пропаганди, євреї проводили з дітьми християнської віри. На основі цієї легенди було створено масштабну кампанію проти євреїв, яка згодом стала однією з причин Голокосту. Також вони використовували

фальшиві документи, такі як Протоколи сіонських мудреців, які, як стверджувалося, були планом єврейської змови проти християнства та західної цивілізації.

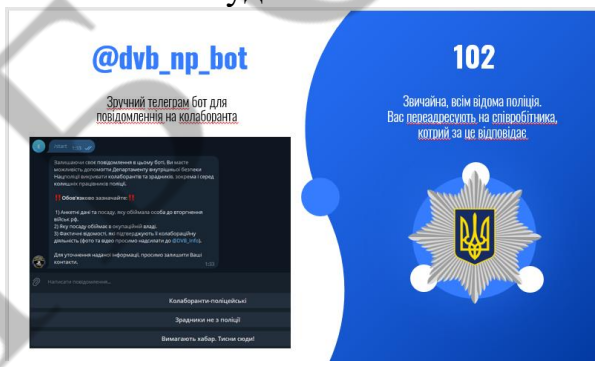
Кібератака - використання комп'ютерних технологій та інтернету для впливу на інформаційні системи та створення кризових ситуацій.

Цілеспрямована інформаційна атака – спрямоване використання інформації для впливу на певну цільову аудиторію та досягнення конкретних цілей.

Як діє ворог та як йому протидіяти?

Створення фейкових новин. Що це та з чого вони складаються ви вже знаєте з цієї презентації. Протидією цьому буде критичне ставлення до новин, які ви бачите. Важливо перевіряти джерела, та факти які вказані в статтях. Пам’ятайте, досвідчені публіцисти завжди виставляють джерела, з яких брали факти, щоб полегшити їх пошук.

Фінансування та підтримка організацій на території України. Якщо ви дізнались про зрадника, колаборнта чи хабарника, ви можете написати в телеграм бота, вказаного на екрані. Там зручно можна вибрати на надіслати заяву. Або скористатись звичним методом, набрати «102» та сповістити туди.



Хакерські атаки. Як їм протидіяти? Дуже просто! Не качайте підозрілі файли які вам надіслали незнайомці. Використовуйте надійні паролі, хоча б від соц. мереж та фінансових систем. Також можна використовувати анті-віруси по типу Аваст чи Нортон.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Панчук Д. М. Фейк // Велика українська енциклопедія. URL: https://vue.gov.ua/Фейк

2. Фейки: Інструкція з перевірки фейків [Електронний ресурс] // Медіадрайвер: [вебсайт]. – Електрон. дані. – Режим доступу: http://mediadriver.online/fejki/instruktsiya-z-perevirki-fejkiv/.

3. Що таке діпфейк? [Електронний ресурс] // Цифрова освіта: [вебсайт]. – Електрон. дані. – Режим доступу: https://osvita.diia.gov.ua/news/what-is-a-deepfeak
4. Як визначити та зловити фейк? [Електронний ресурс] // Інститут масової інформації: [вебсайт]. – Електрон. дані. – Режим доступу: https://imi.org.ua/advices/yak-vyznachyty-ta-zlovyty-fejk-i2388

9 ДІЇ БАНКУ ЩОДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОГО ДИСТАНЦІЙНОГО ОБСЛУГОВУВАННЯ КЛІЄНТІВ

Доповідач: Каріна ПОЛІЩУК
Керівник: Інна КАСАПОВА
ВСП «Одеський технічний фаховий коледж Одеського національного технологічного університету»

На сьогодні, дуже просто та зручно відправляти платежі не виходячи з дому, за допомогою інтернет-банкінгу.Але чи завжди можна бути впевненим,що з вашого рахунку спишеться тільки зазначена вами сума? І чи не потрапите ви в сіті шахрая.

За твердженнями експертів, основна і найголовніша загроза, яка чатує на будь-якого користувача Інтернет-банкінгу в Україні - це ризик шахрайського злому і несанкціонованого доступу до коштів на рахунку.

«Єдиною істотною небезпекою, яка може підстерігати користувачів цих систем, є ризик протиправного заволодіння їх коштами зловмисниками, з використанням можливостей систем «Інтернет-банкінгу», втім, як і будь-яких інших типів систем дистанційного обслуговування».

А тому банки намагаються використовувати різні системи і механізми, покликані якщо не гарантувати, то, в крайньому випадку, підвищити безпеку використання онлайн банкінгу.

Шифрування даних. Сьогодні вже всіма банками, які надають послугу Інтернет-банкінгу, застосовується SSL-шифрування даних, що передаються від комп'ютера користувача в систему банку і назад. Цей захід безпеки дозволяє виключити поширений раніше вид шахрайства «man in the middle»: дані про платіж перехоплювалися на етапі, коли вони відправлені від клієнта, але ще не дійшли в банк, шахрай міняв дані і тільки після цього відправляв їх в банк. Щоб скористатися всіма перевагами захищеної передачі даних, слід дотримуватися елементарних заходів безпеки в Інтернеті - не реагувати на підозрілі повідомлення (отримані нібито від вашого банку) і не переходити з невідомих посиланнях [1]

Одноразові паролі одержувані в банкоматі. При такій системі захисту, крім звичайного логіна і пароля, для входу в систему і підтвердження операцій користувач повинен ввести одноразовий пароль, список яких він може отримати в банкоматі свого банку. З точки зору безпеки така система має перевагу - щоб здійснювати операції по картковому рахунку через інтернет-банкінг, особа повинна як мінімум мати в наявності безпосередньо саму карту, а також знати ПІН-код, щоб отримати список паролів в банкоматі. Разом з тим не можна не відзначити ряд недоліків такої системи захисту. По-перше, список паролів, роздрукований у вигляді чека з банкомату, вам доведеться зберігати для підтвердження майбутніх операцій. А це означає, що якщо ви випадково

втратите або викинете чек (або просто використовуєте всі паролі), вам доведеться йти за новим. Найчастіше список паролів можна отримати далеко не в кожному банкоматі банку, і цілком ймовірно, що вам доведеться їхати за ним на інший кінець міста. До того ж, списком можуть заволодіти зловмисники.

Одноразові смс паролі. Цей спосіб аутентифікації користувача в системі інтернет-банкінгу є чи не найпоширенішим в пропозиціях українських банків. При такій системі кожна операція, яку ви робите за допомогою онлайн банкінгу, повинна бути підтверджена одноразовим паролем, який ви отримаєте в СМС-повідомленні на ваш мобільний телефон. При цьому ваш мобільний номер повинен бути «прив'язаний» до номера рахунку.

Така система має ряд переваг.

По-перше, вона досить проста у використанні - вам не потрібне спеціальне обладнання, а процедура підтвердження операції займає всього пару хвилин.

По-друге, вона дозволяє убезпечити ваш обліковий запис від використання зловмисниками - навіть якщо шахраям стане відомий ваш логін і пароль для входу в систему, вони не отримають доступ до ваших грошей, а ви дізнаєтеся про спробу провести несанкціоновану операцію з СМС-повідомлення.

На цьому переваги системи закінчуються. Дійсно, зловмисникам досить складно заволодіти одноразовим паролем, чинним протягом короткого часу. Якщо тільки вони не заволоділи вашим мобільним телефоном. І зовсім марною система буде в тому випадку, якщо ви користуєтеся інтернет-банкінгом з мобільного телефону і зберігаєте паролі в браузері. Тоді, вкравши у вас телефон, шахрай отримає ваш рахунок в повне розпорядження [1]

Якщо ваш банк використовує аутентифікацію користувача по СМС, постарайтеся дотримуватися таких правил:

- не користуйтеся Інтернет-банкінгом з мобільного телефону;
- ніколи не зберігайте паролі від облікового запису в браузері;
- в разі втрати або крадіжки мобільного телефону - негайно зверніться в банк з проханням заблокувати ваш обліковий запис Інтернет-банкінгу [2].

Електроний цифровий підпис (ЕЦП)

Цей механізм частіше використовується при обслуговуванні банками компаній, але іноді його пропонують і населенню. Плюс ЕЦП в тому, що він дозволяє однозначно ідентифікувати користувача.

Недолік же полягає в тому, що ЕЦП також може бути вразлим для шахраїв. Зловмисники можуть дістатися до ключа від вашої цифрового підпису, заразивши ваш комп'ютер шкідливим програмним забезпеченням. Існують «трояни», які вміють знаходити і красти на зараженому комп'ютері аутентифікаційні дані (ідентифікатори, паролі і навіть ключі ЕЦП) користувачів для доступу до різних сервісів (в тому числі і серверів віддаленого обслуговування клієнтів банків.

Якщо для підтвердження ваших фінансових операцій через інтернет ви використовуєте ЕЦП, не забувайте користуватися антивірусними програмами і регулярно перевіряти ваш комп'ютер на предмет зараження комп'ютерними вірусами. Також експерти не радять залишати ключ ЕЦП підключеним до комп'ютера, якщо ви його не використовуєте [1].

Крім перерахованого вище, банки часто застосовують додаткові заходи для забезпечення безпечного користування інтернет-банкінгом:

- обмеження використання особистого сертифіката - система деяких банків дозволяє використовувати електронний ключ (електронний сертифікат) тільки на тому комп'ютері, на якому він був згенерований.Таким чином, здійснювати платежі через Інтернет-банкінг ви зможете тільки зі свого особистого комп'ютера (хоча переглядати виписки по рахунку можна і на інших пристроях);
- віртуальна клавіатура - призначена для того, щоб шахраї не могли "прочитати" ваші реєстраційні дані при введенні їх з звичайної клавіатури за допомогою комп'ютерних вірусів («троянів»);
- обмеження тривалості сесії - в разі неактивності користувача, сесія в системі Інтернет-банкінгу через певний час (зазвичай 10-15 хвилин) буде закрита.Після цього для відновлення роботи потрібно заново пройти аутентифікацію;
- історія підключень - за допомогою цієї функції користувач Інтернет-банкінгу дізнається, якщо хтось крім нього підключався до системи, а також зможе відстежити всі несанкціоновані операції, якщо вони були зроблені.[2]

Безпечне користування інтернет-банкінгом «ПРИВАТ 24»

Правило №1. Якщо ви продаєте товар на інтернет-майданчику, для отримання переказу на картку за продаж товару необхідно зазначити лише номер картки.

Вимоги покупця назвати інші дані (CVV2-код, строк дії картки, баланс чи тип картки) для переказу грошей на вашу картку повинні викликати у вас підозри.[4]

Правило№2. Не залишайте номер свого фінансового телефону в Інтернеті.

Тим, хто веде бізнес, рекомендують завести окремий контрактний телефон для переговорів з контрагентами.

Не використовуйте фінансовий номер під час контактів з широким загалом. Це може призвести до крадіжки вашої SIM-картки шахраями через перевипуск у відділеннях мобільного оператора.[4]

Правило№3. Якщо ви здійснюєте купівлі через Інтернет в маловідомих вам людей, рекомендуємо використовувати післяплату.

Якщо ви платите на перевірених майданчиках інтернет-гігантів, використовуйте під час розрахунків Інтернет-картку. [4]

Повідомити про факти шахрайства з боку третіх осіб

Співробітник банку ніколи не запитує особисту інформацію!Якщо вам телефонували та намагалися отримати особисту інформацію: CVV2-код, паролі, ПІН-код тощо, повідомте нам. Ми врахуємо ваш приклад під час розробки нових методів запобігання шахрайству.

Якщо ваша особиста інформація все-таки стала відома третім особам, ви також можете подати заявку. Її опрацюють фахівці з безпеки та запобігання шахрайським операціям.

Як подати звернення про шахрайство?

1. У додатку Приват24 перейдіть у меню «Налаштування» → «Комунікації» → «Дзвінки».
2. Натисніть «Перевірити номер телефону» → «Контактували з шахраєм?».
3. Виберіть відповідні варіанти обставин, натисніть «Відправити».

Також подати звернення про шахрайство ви можете за телефоном 3700, в чаті «Допомога Онлайн» або у відділенні банку.

Якщо відбулося шахрайське списання коштів із вашої картки, обов'язково зверніться до підтримки банку за телефоном 3700 або в чат «Допомога Онлайн». [4]

Безпечне користування інтернет-банкінгом «UKRSIBBANK»:

Щоб захистити себе від шахраїв користуючись інтернет-банкінгом «UKRSIBBANK» потрібно:

- Ніколи нікому не називати свій пароль і одноразові паролі з SMS. Пам'ятати, співробітники банку ні за яких обставин не можуть запитувати таку інформацію.
- Встановити на комп'ютер ліцензійний антивірус.
- Не записуйте свій пароль в блокнот, не зберігайте його в смартфоні. Якщо забудете, пароль можна відновити онлайн всього за кілька хвилин.[3]

Банк забезпечує користування інтернет-банкінгом таким чином:

- Надсилає одноразові паролі для підтвердження платежів Пароль діє кілька хвилин і його можна використати тільки один раз.
- Автоматично завершує сесію якщо ви не робите ніяких дій протягом 15 хвилин. Якщо ви забудете вийти з UKRSIB online, ніхто не зможе скористатися вашим обліковим записом.
- Блокує обліковий запис, якщо пароль або код з SMS був введений неправильно декілька разів. Ви відновите свій доступ онлайн або через контакт-центр всього за кілька хвилин.
- Відправляємо листи про вхід з телефонів і комп'ютерів, з яких ви раніше не входили в систему.[3]

Якщо у вас виникли побоювання, що шахраї отримали доступ до вашого рахунку через Інтернет-банкінг, експерти радять зробити наступні дії:

- відключити комп'ютер від Інтернету;
- вернутися в контакт-центр (а при необхідності - в відділення) вашого банку, розказати про проблему і попросити заблокувати ваш обліковий запис;
- перевірити комп'ютер на предмет зараження шкідливим програмним забезпеченням;
- відновити роботу з системою онлайн банкінгу тільки тоді, коли ви переконалися, що загроза відсутня;
- змінити пароль від облікового запису.

Якщо ваші підозри виправдалися, і з рахунку було списано несанкціоновані вами платежі, слід написати заяву про те, що сталося в банк і в правоохоронні органи. В цьому випадку не рекомендується здійснювати ніяких дій на вашому комп'ютері (встановлювати або видаляти програмне забезпечення і т.п.) до прибуття співробітників правоохоронних органів або фахівців банку, оскільки будь-які зміни можуть перешкодити розслідуванню інциденту.[2]

Безпека інтернет-банкінгу є важливою темою в Україні, як і в багатьох інших країнах. Тут є кілька основних аспектів, які варто враховувати, щоб забезпечити безпеку вашого інтернет-банкінгу:

1. Використовуйте надійне програмне забезпечення: Переконайтеся, що ваш комп'ютер або мобільний пристрій мають актуальне антивірусне програмне забезпечення та брандмауер. Регулярно оновлюйте це програмне забезпечення, щоб захистити себе від нових загроз.
2. Надійний доступ до Інтернету: Використовуйте безпечні мережі Wi-Fi із надійним шифруванням. Уникайте використання непідтверджених або відкритих мереж, особливо для проведення фінансових операцій.
3. Сильні паролі: Використовуйте складні паролі для своїх інтернет-банкінгових облікових записів. Паролі повинні містити комбінацію букв верхнього та нижнього регістрів, цифр і спеціальних символів. Уникайте використання очевидних паролів, таких як дата народження чи ім'я.
4. Двофакторна аутентифікація: Використовуйте двофакторну аутентифікацію, яка додає додатковий шар захисту до вашого облікового запису. Це може бути SMS-підтвердження, мобільний додаток аутентифікації або фізичний пристрій, такий як ключ безпеки.
5. Уважно перевіряйте посилання: Перед тим, як вводити свої облікові дані, переконайтеся, що ви належним чином перевіряєте посилання на веб-сайт банку. Уникайте натискання на посилання в ненадійних електронних листах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. https://bankchart.com.ua/e_banking/statti/bezpeka_internet_bankingu_v_ukrayini_praktichniaspekti
2. https://bank.gov.ua/ua/payments
3. https://ukrsibbank.com/services/corporate-clients/ukrsib-business/
4. https://privatbank.ua/safeness/internet-safeness

10 СУЧАСНА ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА КІБЕРБЕРПЕКИ ФАХОВОГО КОЛЕДЖУ ЗВ'ЯЗКУ ТА ІНФОРМАТИЗАЦІЇ ДУІТЗ

Доповідачі: Катерина ТУСМЕНКО,
В'ячеслав РАТУШНИЙ,Євген МАРТИНЕНКО
Керівник: Кононович В.Г.
Фаховий коледж зв'язку та інформатизації
Державного університету інтелектуальних технологій і зв'язку

Політика інформаційної безпеки Фахового коледжу зв'язку та інформатизації ДУІТЗ (Коледжу) - це внутрішній нормативний документ, який відображає позицію Коледжу, а також визначає основні принципи та завдання системи управління інформаційною та кібербезпекою Коледжу. Політику складено відповідно до вимог законодавства України та рекомендацій міжнародних стандартів інформаційної безпеки ISO/SEC 27000.

Інформаційні ресурси мають певну цінність для Коледжу, а, отже, потребує відповідного захисту. Кібербезпека передбачає захист інформації від різноманітних загроз для підтримки неперервності та наукової діяльності, зменшення прямої та

непрямої школи від несанкціонованого використання інформації, збільшення прямої та непрямої користі від наявності інформації та розширення можливостей ведення основної діяльності Коледжу.

Незалежно від форми інформації та ресурсів, які використовуються для її передачі та зберігання, необхідно завжди забезпечувати відповідний рівень захисту інформації. Політика є нормативною основою для захисту інформації Коледжу з метою забезпечення: конфіденційності; цілісності; доступності.

ІКБ досягається шляхом упровадження сукупності необхідних засобів захисту, до яких мажуть входити політики, регламенти, рекомендації, інструкції, організаційні структури та програмні функції.

Основними завданнями інформаційної та кібербезпеки є захист від зовнішніх та внутрішніх,навмисних та ненавмисних загроз.

Політика розроблена відповідно до вимог чинного законодавства України, а саме:Законів України «Про вищу освіту», «Про інформацію», «Про захист інформації у інформаційно-комунікаційних системах», «Про захист персональних даних», та інших правових документів, актів.

Політика розповсюджується на весь Коледж у цілому та повинна використовуватися для всіх критичних бізнес-процесів, інформаційних систем та сервісів Коледжу, які можуть негативно впливати на результати діяльності Коледжу своєю відсутністю або функціонуванням з помилками.

Основним завданнями інформаційної безпеки (ІБ) Коледжу є:

- забезпечення інформаційної безпеки працівників та студентів Коледжу;
- управління ІБ, визначення ролей у галузі ІБ, створення та підтримування системи управління інформаційною безпекою (СУІБ) Коледжу;
- класифікація інформаційних активів;
- здійснення оцінки ризиків ІБ;
- забезпечення безпеки інформаційних активів відповідно до категорії їх класифікації та оцінки ризиків;
- моніторинг подій ІБ, реагування на них і управління інцидентами ІБ;
- забезпечення неперервності інформаційної діяльності Коледжу;
- безпечне управління життєвим циклом ІС.

Серед основних об’єктів, на які розповсюджується дія ІБ Коледжу, розглядаються такі види ресурсів:

- інформаційні ресурси;
- програмне забезпечення;
- фізичні ресурси;
- серверні ресурси.

Для кожного ресурсу визначаються можливі ризики інформаційної безпеки та шляхи їхньої мінімізації, тобто Коледж використовує ризик-орієнтований підхід, який забезпечує розуміння, моніторинг та зменшення ризиків основної діяльності.

Коледж дотримується таких правил щодо ІБ та безперебійної діяльності:

- працівники Коледжу беруть участь у підтриманні відповідного рівня ІБ в межах своїх обов’язків та повноважень і несуть відповідальність за його порушення в межах,

встановлених чинним законодавством України, внутрішніми нормативними документами Коледжу та цією Політикою;

- під час розроблення, впровадження та функціонування програмно-технічних комплексів враховуються вимоги ІБ;
- публічні сервіси Коледжу та внутрішні мережі Коледжу повинні відповідати вимогам стандартів з ІБ;
- коледж забезпечує зі свого боку виконання усіх вимог ІБ, які наявні і угодах з третіми сторонами стосовно використання інформаційних активів;
- для зменшення ризиків виникнення інцидентів ІБ в Коледжі створюються умови для систематичного навчання працівників з метою дотримання норм і вживання заходів ІБ;
- про кожен інцидент ІБ працівники Коледжу негайно інформують безпосереднього керівника. Документами з ІБ Коледжу повинні бути передбачені процедури аналізу та реагування на той чи інший інцидент ІБ, за результатами аналізу вживаються заходи щодо недопущення повторення подібних інцидентів;
- в коледжі складаються, діють, систематично тестуються та оновлюються плани безперебійного функціонування Коледжу на випадок непередбачуваних критичних ситуацій.

Коледж використовує такі підходи щодо забезпечення ІБ:

- створення та затвердження переліку відомостей, що мстять інформацію з обмеженим доступом, службову інформацію;
- створення та затвердження переліку критичних бізнес-процесів;
- встановлення правил доступу до інформаційних ресурсів та програмно-технічних комплексів;
- забезпечення контролю фізичного та логічного доступу до всіх визначених ресурсів;
- забезпечення парольного захисту програмних та сервісних ресурсів;
- забезпечення антивірусного захисту програмних та сервісних ресурсів;
- забезпечення захисту мережі;
- забезпечення віддаленого доступу до ресурсів мережі Коледжу;
- забезпечення ідентифікації та автентифікації усіх наявних інформаційних ресурсів Коледжу;
- забезпечення криптографічного захисту інформації.

Додаткові документи політики інформаційної безпеки (далі – документи Політики) – це нормативно-розпорядчі документи Коледжу, які регламентують заходи ІБ піл час функціонування окремих інформаційних систем і сервісів для потреб Коледжу.

Кожен документ Політики може містити такі відомості щодо вимог ІБ, необхідних для функціонування відповідних інформаційних систем (ІС):

- загальні вимоги безпеки ІС;
- вимоги до рівня захищеності ІС;
- вимоги до організації мережної безпеки;
- вимоги до виявлення інформаційних ризиків та загроз;
- вимоги до керування доступом доінформаційних активів;
- вимоги до керування моніторингом та сповіщеннями;

- вимоги до захисту від шкідливого коду;
- вимоги до віддаленого доступу доінформаційних активів;
- вимоги до забезпечення продуктивності ІС;
- вимоги до функціонування служби підтримки користувачів.

Загальні вимоги ІБ ІС у документах Політики стосується таких питань:
- предмет захисту в межах бізнес-процесу, який передбачає функціонування ІС;
- вимоги до захисту інформації, заходів ІБ та шляхи їхнього застосування;
- рівні ІБ;
- засоби ІБ.

Вимоги до рівня захищеності ІС у документах Політики стосується таких питань:
- безпека облікових записів користувачів;
- сумісність ІС з програмними платформами та супутнім програмним забезпеченням (ПЗ);
- вимоги до встановлення та видалення ПЗ авторизованими фахівцями;
- вимоги до файлової системи та дозволів операційної системи (ОС);
- вимоги до конфігурації апаратнихзасобів.

Вимоги до організації мережної безпекиу документах Політики стосується таких питань:
- рівні захисту локальної мережі від незахищених та ненадійних зовнішніх мереж;
- вимоги до мережних екранів;
- вимоги до виявлення вторгнень до мережі.

Вимоги до виявлення інформаційних ризиків та загроз у документах Політики стосується питань:
- перелік ризиків та загроз;
- фактори, наслідком яких може бути отримання (або загроза отримання) інформації через несанкціоновані канали;
- фактори, наслідком прояву яких може бути порушення цілісності або доступності інформації;
- моделі порушників;
- заходи щодо зменшення вразливості інформаційних активів.

Вимоги до керування доступом до інформаційних активів та загроз у документах Політики стосується питань:
- надання прав доступу користувачам та їх скасування;
- вимоги до аутентифікації та до ідентифікації користувачів;
- вимоги щодо авторизації користувачів на основі ролевої системи доступу.

Вимоги до керування моніторингом та сповіщеннями у документах Політики стосується питань:
- вимоги щодо реєстрації подій, їх ідентифікації;
- захист від експлуатаційних проблем реєстрації подій;
- вимоги до забезпечення сповіщень щодо критичних ситуацій.

Вимоги до захисту від шкідливого коду у Політики стосується питань:
- виявлення шкідливих програм на основі баз сигнатур вірусів та евристичного аналізу; вимоги до своєчасного оновлення антивірусного ПЗ та баз сигнатур вірусів;
- вимоги до функціонування антивірусного ПЗ у межах бізнес-процесу.

Вимоги до віддаленого доступу користувачів до інформаційних активівКоледжу у документах Політики стосується питань:
- загальні вимоги до віддаленого доступу доінформаційних активів;
- вимоги до організації з'єднання на основі стека протоколів TCP/IP;
- вимоги до віддаленого доступу засобами веб технологій;
- вимоги до віддаленого доступу з використанням захищених мереж.

Вимоги до забезпечення продуктивності інформаційних систем/сервісів у документах Політики стосується питань: доступністьінформаційних активів; надійність функціонування апаратного забезпечення та ПЗ; неперервність та своєчасність виконання бізнес-процесу;резервне копіювання інформаційних активів та плани відновлення на випадок виникнення критичних ситуацій.

Вимоги ІБ до функціонування служби підтримки користувачів у документах Політики стосується питань: визначення відповідальних підрозділів, груп працівників для підтримки ІС;технічні засоби підтримки користувачів; вимоги до оперативності підтримки користувачів.

Підрозділ з питань ІБ забезпечує процес розроблення, впровадження, функціонування, моніторингу, підтримання та вдосконалення СУІБ.

ІніціативиПідрозділу ІБ щодо функціонування СУІБ подаються на розгляд комісії Вченої Ради Коледжу з питань інформатизації, рішення якої щодо питань ІБ є обов'язковим для виконання усіма працівниками Коледжу.

Документи Політики розробляються Адміністраторами ІС і затверджуються відповідальним за ІБ.

Постійний контроль впровадження, виконання, вдосконалення та підтримки Політикив актуальному стані здійснює Підрозділ ІБ. Постійний контроль впровадження, виконання, вдосконалення та підтримки документів Політики в актуальному стані здійснюють Адміністратори ІС.

Стратегія розвитку ІТ Коледжу, усі проекти, які пов'язані з ІТ, узгоджуються з цією Політикою. В Коледжі управління ризиками ІБ здійснюється Адміністраторами ІС та Підрозділом ІБ шляхом складання, впровадження, тестування та оновлення планів забезпечення безперебійного функціонування ІС на випадок непередбачених критичних ситуацій. Аналіз ризиків та загрозІБ проводять Адміністратори ІС.

Кожен працівник Коледжу забезпечує підтримку відповідного рівня ІБ Коледжу. В межах своїх службових обов'язків та повноважень працівники повинні виконувати та відповідати за виконання вимог Політики,законодавчих, регуляторних і внутрішніх норм і несуть відповідальність за їх порушення згідно з чинним законодавством України та нормативними документами Коледжу. Для зниження ризиків виникнення інцидентів ІБ керівництво Коледжу створює працівникам умови для систематичного навчання нормам та заходам ІБ.

Здобувачі освіти та представники третіх сторін несуть відповідальність за порушення вимог ІБ Коледжу згідно з чинним законодавством України.

Усі представники третіх сторін проходять навчання для поінформованості та регулярно отримують оновлені дані щодо політик та процедур Коледжу.

Висновок. Запропонована Політика інформаційної безпеки відповідає чинній нормативно-правовій базі; запровадження Політики інформаційної безпеки та ряду

інших документів підвищить захищеність інформації та попередить можливі втрати від комп'ютерних атак.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі НД ТЗІ 3.7-003-2005. ДСТСЗІ СБ України Київ. 22 с.
2. Нашинець А. Ю., Бурячок В. Л., Коршун Н. В. та ін.. Технологія забезпечення інформаційної і кібербезпеки в закладах вищої освіти в Україні. Інформаційні технології і засоби навчання, 2020, Том 77, №3. С. 337 – 354.
3. Типове положення про службу захисту інформації в автоматизованій системі НД ТЗІ 1.4-001-2000. ДСТСЗІ СБ України. 37 с.

11 ІНФОРМАЦІЙНА ГІГІЄНА ТА МЕДІА-ГРАМОТНІСТЬ ЯК ВАЖЛИВИЙ АСПЕКТ В СУЧАСНОМУ ІНФОРМАЦІЙНОМУ СВІТІ

Доповідач: Євгеній СЕМЗЕНИШ
Керівник: Дмитро ДЖАБРАЇЛОВ
ВСП «Одеський технічний фаховий коледж
Одеського національного технологічного університету»

У далекому минулому люди вміли впливати один на одного тільки під час безпосереднього спілкування за допомогою слів, інтонації, жестів, міміки.

З розвитком технологій люди змогли використовувати інші засоби впливу на один одного, такі як письмові листи, телефон, радіо, телебачення тощо. В сучасному світі із зростанням популярності інтернету та соціальних мереж люди отримали ще більше можливостей впливати на інших, використовуючи електронну пошту, чати, месенджери, коментарі в соціальних мережах та інші цифрові інструменти. Однак, з ростом таких можливостей також зросла і кількість дезінформації та фейків, що поширюються через цифрові канали комунікації, тому важливо бути обережним та перевіряти достовірність інформації, яку ми отримуємо в Інтернеті.

Інформаційна війна - це форма боротьби, в якій сторони використовують інформаційні технології та медіа-ресурси з метою впливати на думку, переконання та поведінку населення, зокрема в контексті політики, військової діяльності, економічних та соціальних питань. Вона може мати як внутрішні, так і міжнародні аспекти, і використовуватися як у воєнний, так і в мирний час.

З чого складається інформаційна війна:

1) Збір тактичної зброї - включає в себе збір інформації про супротивника, його слабкі місця та можливості, а також про його зброю і тактику.

2) Забезпечення безпеки власних інтернет-ресурсів - це процес захисту власних мереж та інтернет-ресурсів від кібератак та інших загроз, що можуть завдати шкоди діяльності та інформації.

3) Пропаганда та дезінформація - використання різних каналів комунікації, таких як соціальні мережі, медіа, блоги тощо, з метою впливу на масову свідомість та переконання громадськості, зокрема за допомогою поширення неправдивої інформації.

4) Підрив якості інформації супротивника - це процес внесення неправдивої, перекрученої чи недостовірної інформації в інформаційний простір супротивника з метою підриву довіри громадськості до його лідерів, влади, або важливих суспільних інститутів.

Події 2008 року у Грузії, 2013-2014 років в Україні призвели до того, що інформаційну війну Росії проти України більше не розглядають лише як незручність для населення, політичних діячів, експертів і науковців, а як серйозну загрозу безпеці, яка може призвести до смертельних наслідків.

«Особливості інформаційної війни»

Інформаційна зброя відрізняється від інших засобів введення війни тим, що її використання може бути невидимим і складним для виявлення, оскільки дії здійснюються в цифровому просторі. Інформаційні атаки можуть бути проведені навіть без прямого доступу до комп'ютерних систем або інших інфраструктур, оскільки їх мета - вплив на людей та їх поведінку.

Інформаційна зброя надає багато варіативних форм і способів застосування, включаючи дезінформацію, маніпуляцію, обмеження доступу до інформації, кібератаки та багато іншого. Це дозволяє провідникам інформаційної війни використовувати різні підходи залежно від цілей та мети.

«Участники інформаційних війн»

Учасники інформаційних війн можуть бути різними державними та недержавними акторами, включаючи:

1. Державні актори: це можуть бути різні державні органи, такі як військові, розвідувальні та інші служби, а також офіційні політичні органи, такі як міністерства закордонних справ або президентська адміністрація.

2. Недержавні актори: це можуть бути терористичні організації, кримінальні угруповання, хакерські колективи, приватні компанії та інші недержавні суб'єкти.

3. Журналісти та ЗМІ: журналісти та ЗМІ можуть бути використані для поширення дезінформації та маніпулювання громадською думкою.

4. Активісти та групи впливу: це можуть бути різні соціальні та політичні групи, які використовують інформаційну зброю для підтримки своїх інтересів.

5. Індивідуальні хакери та кіберзлочинці: ці групи можуть використовувати кібератаки та інші методи для здобуття конфіденційної інформації або завдання шкоди комп'ютерним системам та мережам.

6. Громадські організації та активісти за права людини: ці організації можуть використовувати інформаційну зброю для залучення уваги до своїх проблем та залучення громадської підтримки.

7. Підрозділи дезінформації та пропаганди: ці підрозділи можуть бути створені спеціально для проведення інформаційних операцій та зброї.

«Дезінформація»

Події 2 травня 2014 року в Одесі були трагічними і складними, і їхнє тлумачення може варіюватися в залежності від джерела і переконань. Однак, деякі російські ЗМІ використовували ці події, щоб пропагувати свою версію подій та спрямовувати дезінформацію на населення.

Зокрема, деякі російські ЗМІ поширювали тезу про те, що трагедія була "масовим вбивством російської мови та мирних російських людей", і що це було сплановано і здійснено українськими націоналістами та урядом. Також, деякі ЗМІ спробували звинуватити правоохоронні органи та українську владу у сприянні та навіть причетності до трагедії.

«Контроль інформаційного простору»

Росія має досить довгу історію контролю інформаційного простору, включаючи використання пропаганди, цензури та інших методів для впливу на зміст інформації, що розповсюджується в медіа.

Останніми роками Росія активно використовує Інтернет та соціальні мережі для поширення пропаганди та впливу на інформаційний простір. Росія блокує незалежні джерела інфорамції, українськи ЗМІ на окупованих територіях та російськи, які не виконують доручення держави.

«Інформаційна Гігієна та Медіаграмотність»

Інформаційна гігієна та медіа-грамотність є важливими аспектами в сучасному інформаційному світі. Інформаційна гігієна - це комплекс заходів, що спрямовані на забезпечення безпеки користування інформацією та виключення негативного впливу на здоров'я, психологічний та соціальний стан людини. Вона включає в себе знання про те, як використовувати інформацію в Інтернеті, які джерела довіри, а також як захистити свої персональні дані.

Медіа-грамотність - це здатність людини аналізувати, розуміти та критично оцінювати інформацію, яка йде з різних медіа. Це включає знання про те, які медіа довіряти, як правильно інтерпретувати інформацію та як визначати факти від фікції. Медіа-грамотність дозволяє людині зрозуміти, що насправді відбувається в світі, збільшити свою культуру спілкування та бути впевненими в своїх діях.

Оскільки сучасне суспільство переповнене інформацією, важливо, щоб люди були освіченими та медіа-грамотними, щоб вони могли зробити свідомий вибір, який ґрунтується на об'єктивних фактах та аналізі. Інформаційна гігієна та медіа-грамотність є важливими для збереження здоров'я, стабільності та демократії в суспільстві.

«Маніпулювання громадською думкою»

Росія веде активну інформаційну кампанію щодо України, зокрема з метою маніпулювання громадською думкою на своїх територіях та у світі. Ця кампанія складається з різноманітних заходів, включаючи використання дезінформації, пропаганди та вигаданих історій.

Одним із найбільш поширених методів маніпулювання є використання дезінформації та фейків. Російські ЗМІ та відомства часто випускають неправдиві повідомлення та новини, що мають на меті викликати відчуття страху, недовіри та невпевненості. Наприклад, російські ЗМІ можуть висувати непідтверджені твердження про "український фашизм" або "українську агресію проти мирних громадян".

Другим методом маніпулювання є використання пропаганди. Російські ЗМІ та відомства часто зображають Україну та її владу як агресивну та нестабільну, тоді як Росію зображають як жертву ситуації. Цей підхід має на меті формування негативного ставлення до України та її влади, а також підтримання позитивного ставлення до Росії та її лідера.

Третій метод - вигадування історій. Російські ЗМІ можуть створювати історії, які не мають наочних доказів або не мають жодного зв'язку з реальністю, та розповсюджувати їх як правду. Це може включати вигадування подій, які ніколи не відбувалися, або перекручування реальних подій.

«Кібератаки»

Росія активно використовує кібератаки як один з інструментів своєї гібридної війни проти України. Кібератаки є дієвим засобом впливу на українську інфраструктуру, економіку, а також на громадську думку.

Одним з найвідоміших прикладів кібератак Росії проти України є кібератака на енергетичну систему України в грудні 2015 року. Кібератака призвела до відключення електроенергії на певних територіях України, що спричинило значні проблеми для населення та підприємств.

Крім того, Росія також використовує кібератаки для здійснення шпигунських операцій та крадіжки конфіденційної інформації. Наприклад, в липні 2020 року група хакерів, які пов'язані з російськими спецслужбами, вчинила кібератаку на українську компанію "Eney" з метою крадіжки конфіденційної інформації.

Російські кібератаки також спрямовані на маніпулювання громадською думкою в Україні. Це включає в себе використання соціальних мереж та інтернет-медіа для поширення пропаганди, фейкових новин та дезінформації. Наприклад, в 2014 році було запущено російську пропагандистську кампанію "Війна із Україною - це війна із фашизмом", яка мала на меті негативно впливати на громадську думку в Україні та за її межами.

«Створення ботів та фейкових акаунтів»

Росія використовує ботів та фейкові акаунти для поширення дезінформації, збільшення свого впливу на громадську думку та підірвання довіри до демократичних процесів в інших країнах. Основні методи створення та використання ботів та фейкових акаунтів Росією можуть включати:

1. Створення мереж фейкових акаунтів, що спілкуються між собою та інших публічних облікових записів, для створення враження значної підтримки чи невдоволення певними політичними, економічними, соціальними чи культурними питаннями.

2. Розсилання масових повідомлень, коментарів та повідомлень в соціальних мережах, які містять дезінформацію, штучно створені факти, чутки, або залишають враження більшої підтримки чи невдоволення, ніж вона фактично є.

3. Атаки на офіційні веб-сайти, в тому числі й урядові, з метою зміни, видалення, або розміщення фальшивої інформації.

4. Використання ботів для автоматичного підпису на петиції, коментування новин та відео, та інші активності в інтернеті, що дають враження значної кількості підтримки або невдоволення певною темою чи подією.

Наразі інформаційна війна Росії проти України триває, і її наслідки відчуваються не тільки в Україні, а й за її межами. Російські інформаційні кампанії спрямовані на дестабілізацію ситуації в Україні та інших країнах, на підрив авторитету української держави і західних демократій загалом.

Ця інформаційна війна є частиною ширшої геополітичної гри Росії, яка прагне вплинути на ситуацію у світі та захистити свої інтереси. Тому питання боротьби з інформаційною війною стає вкрай важливим для захисту інтересів України та інших країн.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Найбільш вражаючі приклади інформаційних війн 21 століття. https://businessviews.com.ua/ru/studies/id/najbilsh-vrazhajuchi-prikladi-informacijnih-vijn-21-stolittja-2037/
2. Інформаційна війна / Р. В. Пилипчук // Енциклопедія Сучасної України [Електронний ресурс] / Редкол.: І. М. Дзюба, А. І. Жуковський, М. Г. Железняк [та ін.] ; НАН України, НТШ. – К. : Інститут енциклопедичних досліджень НАН України, 2011. – Режим доступу: https://esu.com.ua/article-12460
3. Інформаційна війна – зброя масового знищення! https://www.pravda.com.ua/rus /articles /2006/04 /20/ 4399050/
4. 2. Інформаційні війни: тенденції та шляхи розвитку. https://ms.detector.media/ manipulyatsii/post/6479/2012-08-12-informatsiini-viinitendentsii-ta-shlyakhi-rozvitku/

12 ЯК ЗАХИСТИТИ ПЕРСОНАЛЬНІ ДАНІ В ІНТЕРНЕТ СЕРЕДОВИЩІ

Доповідач: Даніїл КОВАЛЕНКО
Керівник: Ірина ФЕДОРЕНКО
ВСП «Козелецький фаховий коледж ветеринарної медицини Білоцерківського національного аграрного університету»

Кібербезпека – це сукупність методів і заходів, які допомагають захищати комп'ютерні системи, мережі, пристрої та програми від кібератак, які можуть завдати шкоди або отримати несанкціонований доступ до даних, інформації або ресурсів[1,2,3]. Кібер безпека важлива для забезпечення конфіденційності, цілісності та доступності електронних інформаційних ресурсів, а також для захисту національних інтересів, життєво важливих сфер діяльності та особистої безпеки користувачів[1,3].

Кібер безпека включає різні аспекти, такі як:

- Превентивні методи захисту, які спрямовані на запобігання кібератакам шляхом використання антивірусних програм, фаєрволів, шифрування даних тощо[2].
- Реактивні методи захисту, які спрямовані на виявлення та нейтралізацію кібератак шляхом моніторингу мережевого трафіку, аналізу індикаторів кіберзагроз, реагування на кібер інциденти тощо[1].
- Відновлювальні методи захисту, які спрямовані на відновлення нормального функціонування систем і мереж після кібератак шляхом резервного копіювання даних, оновлення програмного забезпечення, усунення вразливостей і т.д.[1].

Ось кілька базових правил безпеки у цифровому середовищі, які можуть допомогти захистити вас від кіберзлочинців:

1. Використовуйте сильні паролі та не використовуйте один і той же пароль для різних сервісів.

2. Не діліться своїм паролем з іншими людьми, включаючи членів родини.
3. Перевіряйте URL-адресу сайту, перш ніж вводити будь-яку особисту інформацію або здійснювати оплату.
4. Увімкніть двофакторну аутентифікацію, коли це можливо, для збільшення рівня безпеки вашого облікового запису.
5. Не відкривайте невідомі файли, що приходять по електронній пошті або через інші канали зв'язку.
6. Не використовуйте відкриті Wi-Fi мережі для надання конфіденційної інформації.
7. Оновлюйте програмне забезпечення на своєму комп'ютері та мобільному пристрої, щоб уникнути вразливості.
8. Не дозволяйте програмам, які вимагають доступ до вашого місцезнаходження, доступу до непотрібної інформації.
9. Будьте обережні зі сторонніми додатками та розширеннями, які можуть вмістити шкідливий код.

1. Використання сильних та унікальних паролів для різних сервісів може допомогти захистити ваші особисті дані та облікові записи від кіберзлочинців. Якщо використовується слабкий пароль або той же самий пароль для кількох різних сервісів, то зловмисник, який зламав ваш обліковий запис в одному сервісі, може використовувати цей пароль для доступу до інших сервісів, що містять вашу особисту інформацію.

Застосування сильних та унікальних паролів може ускладнити роботу зловмисникам, що намагаються зламати ваші облікові записи, оскільки вони не зможуть легко вгадати або скомпрометувати ваш пароль. Сильні паролі повинні містити комбінацію великих та малих літер, цифр та спеціальних символів, а також бути довгими.

Використання унікальних паролів для кожного облікового запису забезпечує додатковий захист для ваших даних. Якщо зловмисник зламує один з ваших облікових записів, то він не зможе скористатися тим же паролем для доступу до інших облікових записів. Це може значно зменшити ризик порушення безпеки та захисту вашої особистої інформації.

2. Є кілька причин, чому не можна ділитись своїм паролем з рідними:

2.1 Безпека даних: Якщо ви ділитеся своїм паролем з рідними, то вони можуть отримати доступ до ваших особистих даних, таких як електронна пошта, банківські рахунки та соціальні мережі. Це може бути небезпечним, якщо хтось із вашого оточення несвідомо причетний до злочинних дій або стає жертвою кібератак.

2.2 Ризик втрати контролю: Якщо ви ділитеся своїм паролем з рідними, вони можуть змінити його без вашого дозволу або використовувати його без вашої згоди. Це може призвести до втрати контролю над вашими обліковими записами та даними.

2.3 Нерозуміння ризиків: Ваші рідні можуть не розуміти ризиків, пов'язаних зі зберіганням паролів, та недбало ставитися до їх безпеки. Це може призвести до витоку конфіденційної інформації або кібератак.

Висновок: Пароль - це особиста інформація, яку варто тримати при собі. Якщо ви хочете дозволити іншій людині доступ до своїх облікових записів, то краще

використовувати спеціальні сервіси для діління паролів, які забезпечують надійний захист даних.

3. *Перевірка URL-адреси сайту перед введенням будь-якої особистої інформації* або здійсненням оплати може допомогти у запобіганні кібершахрайства та захистити ваші особисті дані. Ось декілька причин, чому це важливо:

3.1 Запобігання фішингу: Фішинг - це метод шахрайства, коли зловмисники створюють підроблені веб-сайти, щоб виманити ваші особисті дані. Перевірка URL-адреси сайту перед введенням будь-якої інформації може допомогти вам виявити підроблені сайти, які можуть мати подібну адресу до оригінального сайту.

3.2 Захист від кібератак: Зловмисники можуть створювати підроблені сайти, щоб виконати кібератаки на ваш комп'ютер або мобільний пристрій. Перевірка URL-адреси сайту перед введенням будь-якої інформації може допомогти запобігти попаданню на такі сайти.

3.3 Збереження конфіденційності: Якщо ви вводите свої особисті дані або реквізити оплати на недостовірному сайті, зловмисники можуть отримати доступ до цих даних і використовувати їх для кіберзлочинів. Перевірка URL-адреси сайту перед введенням будь-якої інформації може допомогти зберегти ваші конфіденційні дані в безпеці.

Висновок: Перевірка URL-адреси сайту перед введенням будь-якої особистої інформації або здійсненням оплати - це важливий крок, який допоможе вам запобігти кібершахрайству та захистити ваші особисті дані.

4. *Якщо ви хочете збільшити рівень безпеки свого облікового* запису, я настійно рекомендую вам ввімкнути двофакторну аутентифікацію (2FA), якщо це можливо.

2FA - це метод аутентифікації, який вимагає від користувача двох факторів, щоб довести свою ідентичність: щось, що він знає (наприклад, пароль), і щось, що він має (наприклад, токен або код, який генерується спеціальним додатком на мобільному телефоні).

Існують різні способи використання 2FA, наприклад, використання спеціальної програми аутентифікації, яка генерує одноразові коди, або використання SMS-повідомлень або електронної пошти для отримання кодів.

Якщо ваш провайдер облікових записів підтримує 2FA, ви можете ввімкнути його в налаштуваннях облікового запису. Для цього зазвичай потрібно підключити додаток аутентифікації, який забезпечує безпечне зберігання токенів або кодів аутентифікації.

Включення 2FA дозволить вам значно збільшити рівень безпеки вашого облікового запису, тому я рекомендую вам використовувати цей метод аутентифікації, якщо він доступний.

5. *Не відкривання невідомих файлів, що приходять по електронній пошті* або іншими каналами зв'язку, є одним з найбільш ефективних заходів безпеки, які ви можете вжити для захисту свого комп'ютера або мобільного пристрою від шкідливих програм.

Такі файли можуть містити віруси, шкідливі програми або шкідливі посилання, які можуть призвести до інфікування вашого пристрою або до злому ваших

конфіденційних даних. Це може призвести до крадіжки вашої особистої інформації, такої як паролі, банківські реквізити, номера кредитних карток тощо.

Щоб захистити свій пристрій від таких загроз, ніколи не відкривайте файли, які ви не очікуєте, або які приходять від невідомих джерел. Якщо ви отримуєте електронний лист або повідомлення з незвичайним вмістом або з додатком, який ви не очікували, краще не відкривайте його, або спочатку перевірте його на наявність вірусів або шкідливих програм з допомогою антивірусного програмного забезпечення.

Завжди будьте пильні щодо отримання незапрошених електронних листів або повідомлень та не відкривайте невідомі файли, щоб забезпечити безпеку своєї системи.

6. *Надання конфіденційної інформації через відкриті Wi-Fi* мережі може бути небезпечним, оскільки ці мережі не є захищеними і можуть бути піддані атакам з боку зловмисників.

Коли ви використовуєте відкриту Wi-Fi мережу, ваші дані, такі як логіни, паролі, банківські дані та інша конфіденційна інформація, можуть бути перехоплені зловмисниками, які можуть використовувати цю інформацію для крадіжки вашої особистої інформації або злочинних дій.

Тому, використовуючи відкриту Wi-Fi мережу, краще утриматися від надання конфіденційної інформації, щоб уникнути можливих проблем зі збереженням приватності та безпеки даних. Якщо вам дійсно потрібно надати конфіденційну інформацію, використовуйте власний бездротовий зв'язок або використовуйте віртуальну приватну мережу (VPN), що забезпечить захист ваших даних та приватності.

7. *Оновлення програмного забезпечення на вашому комп'ютері* та мобільному пристрої є дуже важливим з причин безпеки та захисту ваших пристроїв та даних від потенційних загроз.

Кожне оновлення програмного забезпечення містить нові корисні функції, вдосконалення та виправлення помилок, які покращують безпеку, функціональність та продуктивність пристроїв. Однак, одним з головних принципів цих оновлень є виправлення вразливостей, які можуть бути використані зловмисниками для атак на ваш пристрій.

Зловмисники постійно шукають способи, якими вони можуть використати вразливості в програмному забезпеченні для зламування систем безпеки і крадіжки приватної інформації. Оновлення програмного забезпечення може запобігти таким атакам, тому що вони містять виправлення вразливостей, які були виявлені в попередніх версіях програмного забезпечення.

Отже, регулярне оновлення програмного забезпечення на вашому комп'ютері та мобільному пристрої може допомогти захистити вас від потенційних загроз та забезпечити безпеку та приватність вашої інформації.

8. *Заборона програмам отримувати доступ до вашого місцезнаходження* та іншої непотрібної інформації може допомогти захистити вашу приватність та зберегти ваші особисті дані.

Деякі програми можуть вимагати доступ до вашого місцезнаходження або інших особистих даних, але це не завжди необхідно для їх роботи. Якщо програма отримує доступ до цих даних, вона може використовувати їх для неправомірних цілей,

наприклад, для відстеження ваших дій, продажу цих даних третім сторонам або для спаму вас рекламою.

Деякі програми можуть також збирати непотрібну інформацію про вас, таку як ваші контакти, історію браузера або іншу особисту інформацію, яка може бути використана для відстеження вас або для несанкціонованого використання.

Тому, якщо ви не бажаєте, щоб програми збирали вашу особисту інформацію, вам необхідно відмовитися від надання доступу до неї. Це може бути зроблено налаштуваннями вашого пристрою або через запит на дозвіл від програми, коли вона вперше запускається.

Таким чином, заборона програмам отримувати доступ до вашого місцезнаходження та іншої непотрібної інформації може допомогти зберегти вашу приватність та запобігти неправомірному використанню ваших особистих даних.

9. *Будьте обережні зі сторонніми додатками та розширеннями*, що ви встановлюєте на свій комп'ютер, браузер або мобільний пристрій, оскільки вони можуть містити шкідливий код. Це може призвести до компрометації ваших пристроїв та поширення вірусів або зловмисних програм на вашій системі.

Шкідливі програми можуть використовувати ваш пристрій для збору конфіденційної інформації, такої як паролі та інші особисті дані, а також для виконання атак на інші комп'ютери та мережі. Це може призвести до втрати даних, фінансових втрат та інших серйозних наслідків.

Щоб захистити свої пристрої та інформацію, встановлюйте додатки тільки з відомих джерел та перевіряйте їх перед встановленням. Також регулярно оновлюйте свої програми та операційну систему, щоб уникнути вразливостей, які можуть бути використані зловмисниками. Не дозволяйте невідомим додаткам отримувати доступ до своєї системи та інформації, а також не відкривайте невідомі файли та посилання, які можуть містити шкідливий код.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. https://www.microsoft.com/uk-ua/security/business/security-101/what-is- cybersecurity
2. https://datalabsua.com/ua/cyber-security-what-is-this-and-why-it-is- important/
3. https://nordvpn.com/uk/cybersecurity/

13 ЦИФРОВЕ СЕРЕДОВИЩЕ. БЕЗПЕКА ВІРТУАЛЬНОГО СПІЛКУВАННЯ

Доповідач: Богдан БОБРИЧЕНКО
Керівник: Інна ШЕВЧЕНКО
Комунальний заклад
«Балтський педагогічний фаховий коледж»

Ми живемо в світі, де інформація є все більш важливим ресурсом. Засоби масової інформації відіграють вирішальну роль у створенні та поширенні цієї інформації. Цифрові медіа впливають на розвиток людини, тому важливо розуміти їх всеохоплючий вплив на формування особистості. Серед пріоритетів здоров’я та безпеки у світовій

освіті поряд із фізичним і психологічним благополуччям є наука і технології, зокрема цифрова грамотність.

Стрімкий розвиток цифрових технологій спричинив появу величезних можливостей для дітей і молоді стосовно спілкування, встановлення зв'язків, навчання, обміну інформацією та доступу до неї, а також висловлення своїх поглядів і думок з самих різноманітних питань. [1]

Цифрове середовище, зокрема мережа Інтернет, сьогодні є не лише важливим джерелом інформації, але і способом комунікації, який нівелює перепони для спілкування.

У науковій і практичній літературі доволі часто вживається два поняття «цифрове середовище» і «мережа Інтернет». Тому важливо з'ясувати співвідношення між ними. Визначення поняття «цифрове середовище» у законодавстві України не наводиться, однак в науковій літературі вказують, що це словосполучення не тільки ввійшло у звичайну мову, а починає використовуватися і в юридичній лексиці.[3]

Цифрове середовище – це ширше поняття, ніж мережа Інтернет. Цифрове середовище включає у себе не лише веб-сайти (і веб-сторінки як складові веб-сайтів), а й електронні документи, файли, в тому числі об'єкти, які використовуються на відповідних пристроях, що не передбачають паперової форми документообігу (комп'ютери, ноутбуки, планшети, телефони, інші види так званих «гаджетів»).

Через глобальний вплив COVID-19 діти проводять все більше часу в Інтернеті. Але водночас більш широкий і легкий доступ до онлайнових послуг становить більшу загрозу для безпеки як в цифровому середовищі, так і в реальному житті. Люди живуть та діють у цифровому просторі (ЦП), який є кіберпростором у контексті безпеки життя та діяльності людини. Діти народжуються, зростають, навчаються і працюють із гаджетами, що під'єднані до мереж і стають природним середовищем. Їх життя та навчання пов'язані з широким використанням цифрових технологій і відповідною необхідністю досягнення цифрової компетентності. [4]

Пов'язані з кібербезпекою інциденти почали відбуватись частіше і регулярно потрапляють у заголовки новин, чим викликають все більшу тривогу. Кожного дня цифрове середовище ускладнюється і наша залежність від даних та взаємодії у мережі зростає, розвиток стійкості до кіберзагроз – широкомасштабних подій з руйнівними наслідками, які розвиваються по каскадному принципу, ще ніколи не був настільки важливим

Кібербезпека є неодмінною складовою щоденного життя не лише підприємств, міністерств та держави, але й пересічних користувачів мережі Інтернет та приладів, які до неї підключені. Вона охоплює все, що стосується захисту особистої інформації, інтелектуальної власності, даних, а також державних і галузевих інформаційних систем від крадіжки і пошкодження. Кібергігієна – це базові правила цифрової (кібер) безпеки при роботі в Інтернеті. Через масове збільшення кількості інтернет-шахрайств, кібергігієна стала актуальною темою обговорення в суспільстві впродовж останніх років.

Комунікація у віртуальному просторі має свої особливості. Так, інформаційно-комунікаційні технології є важливим інструментом у житті під час здобуття освіти,

соціалізації, самореалізації. Водночас, безконтрольне та безвідповідальне їх використання містить ризики для здоров'я, розвитку та благополуччям дітей , зокрема:

- контактні ризики (сексуальні експлуатації та зловживання, домагання для сексуальних цілей («грумінг», розбещення), онлайн-вербування дітей для вчинення злочинів, участь у екстремістських політичних чи релігійних рухах або для цілей торгівлі людьми);
- ризики контенту (принизливе та стереотипне зображення та надмірна сексуалізація жінок та дітей; зображення та популяризація насильства та нанесення собі ушкоджень, зокрема, самогубств; принизливі, дискримінаційні або расистські вирази або заклик до такої поведінки; реклама, контент для дорослих);
- ризики поведінки (залякування, переслідування та інші форми утисків, розповсюдження без отримання згоди сексуальних зображень, шантаж, висловлювання ненависті, хакерство, азартні ігри, незаконне завантаження або інші порушення прав інтелектуальної власності, комерційна експлуатація);
- ризики для здоров'я (надмірне використання призводить до позбавлення сну та фізичної шкода).

Всі перераховані вище ризики не є вичерпними, постійно оновлюються та здатні негативно вплинути на фізичне, емоційне та психологічне благополуччя людини.

З огляду на сказане, необхідно формувати компетентності щодо безпечної поведінки в цифровому просторі та потенційної небезпеки безвідповідального ставлення до використання мережі Інтернет, суспільну культуру нетерпимого ставлення до порушення прав, свобод, безпеки дитини взагалі та в цифровому середовищі зокрема, критичне мислення під час сприйняття інформації та вчити правилам інформаційної гігієни, щоб запобігти впливу подібних ризиків та потраплянню дітей в небезпечні ситуації

Важливо розуміти, що цифрова безпека – це процес. Ви не можете сьогодні щось встановити, придбати якусь магічну кнопку, яка б дозволила захистити усі ваші дані, інформацію ваших друзів, колег і т.д. Ви постійно дізнаєтесь про нові загрози та про нові інструменти, які з'являються – щось використовуєте, а щось ні. Важливо розуміти, на які загрози ви можете натрапити.

В рамках DIGITAl FORUM for Civil Society Ніколай Кванталіані розповів про правила, якими варто погодитися, навчитися користуватися та запам'ятати, основні рекомендації щодо захисту власних даних, безпечного користування електронними пристроями та інформаційними ресурсами. [5]

1. Використовуйте ліцензійне програмне забезпечення скрізь, зокрема на телефонах і планшетах, робочих та домашніх комп'ютерах.
2. Регулярно оновлюйте все програмне забезпечення. Останнім часом Windows оновлюється та перезавантажується без вашого бажання: ви хочете попрацювати, а його не хвилює, що у вас конференція.
3. Встановлюйте антивірусні програми та firewall (міжмережевий екран, фаєрвол). Антивірус вирішує проблему зараження вірусами, а фаєрвол відслідковує міжмережеві зв'язки нашого комп'ютера та мережі Інтернет і, відповідно, допомагає нам захищатись від загроз ззовні.

4. Встановлюйте пароль на вхід у пристрій (телефон, планшет, комп'ютер). Вам потрібен саме складний унікальний пароль. Складний унікальний пароль – це такий, котрий містить великі літери, маленькі літери, спеціальні символи, і розмір його загалом не менше 14 символів – це мінімальний стандарт, а ще краще 20 чи 30. Унікальність – це означає, що кожен обліковий запис повинен мати власний пароль. Тобто в Facebook у нас повинен бути один пароль, а на поштовій скриньці Gmail - зовсім інший.

5. Використовуйте менеджер паролів. Якщо ми створюємо для кожного облікового запису унікальні паролі, то з їх кількістю виникають труднощі. Ви можете використовувати той менеджер, який для вас є зручним і якому ви довіряєте.

6. Розділяйте облікові записи. Наприклад, у нас є поштові скриньки окремо для роботи і для дому. Якщо зламали нашу домашню скриньку, то не отримали доступ до робочої, і навпаки. Навіть, якщо ми комунікацію розділяємо між різними месенджерами: наприклад, частина переписки в WhatsApp, а частина в Viber – це вже захищає інформацію, тому що тим, хто атакує, треба отримати доступ до ще одного каналу комунікації.

7. Блокуйте пристрої. Наприклад, якщо ви йдете випити кави, то важливо заблокувати свій пристрій, щоб людина, яка йде повз ваш робочий стіл, не отримала доступ. На мобільному телефоні краще встановити відключення після 60 секунд, щоб він самостійно заблокувався, якщо ви його залишили на столі.

8. Видаляйте історію з браузера та кеш. Коли ви працюєте в інтернеті, то сайти, на які ви заходите, відправляють на ваш комп'ютер невеличкі файли, щоб знати, що це були ви, та відповідно індексують усі ваші дії. Наприклад, CCleaner – це програма, за допомогою якої можна видаляти такі тимчасові файли. Це потрібно для того, щоб людина, яка працюватиме на комп'ютері після вас, не могла подивитись, що саме ви шукали, тобто щоб ви були більш анонімними.

9. Не зазначайте очевидні відповіді для відновлення доступу до свого облікового запису. Якщо таємне питання для відновлення паролю – дівоче прізвище вашої мами, то ця інформація є загальнодоступною, її можна знайти в соціальних мережах та легко отримати доступ до вашої скриньки.

10. Не використовуйте для відновлення доступу незахищені поштові скриньки. Якщо у вас є добре захищена поштова скринька на Gmail, а інша скринька на Mail.ru, і вони пов'язані між собою функцією відновлення, тоді потенційно ви є вразливими.

11. Користуйтесь секретними месенджерами, якщо вирішили вести таємну переписку. Наприклад, Viber, Signal, таємні чати в Telegram. Одна із важливих складових – це не лише передача зашифрованої комунікації, але й її зберігання. Якщо ви комусь передали таємну інформацію, то вона є у вас і у вашого колеги. Відповідно, якщо ви не хочете, щоб це в подальшому було виявлено, краще відразу видаляти інформацію.

12. Використовуйте месенджери з шифруванням від пристрою до пристрою – Signal, WhatApp, Viber, а в Telegram - секретний чат. В такому випадку у сервіс-провайдера немає можливості читати вашу переписку.

13. Не клікайте на підозрілі посилання.

14. Не ловіться на фішинг. Фішинг - вид шахрайства, метою якого є виманювання у довірливих або неуважних користувачів мережі персональних даних клієнтів онлайнових аукціонів, сервісів з переказу або обміну валюти, інтернет-магазинів.

15. Робіть резервні копії важливих файлів в хмарних сховищах. Хмарні сховища – це Google Диск, Dropbox. Статистично є дуже ймовірним, що може трапитись пошкодження жорсткого диску або флешки без можливості відновлення. Якщо ви користуєтесь Gmail поштою, то можете використовувати Google Диск. Якщо у вас є таємні файли, то ви можете їх попередньо зашифрувати, а потім завантажити в хмарне сховище автентифікатором.

16. Використовуйте технології VPN (Virtual Private Network — віртуальна приватна мережа) при підключенні до публічного Wi-Fi. VPN – це тунель від вашого ПК до іншого комп'ютера, а потім до мережі Інтернет. По суті, це створення надійного тунелю, що захищає ваші дані в ненадійній мережі.

ВИСНОВКИ. Звичайно, ніхто не заперечує той факт, що Інтернет сьогодні – найважливіше джерело інформації і роботи для багатьох людей. Але важливо у всьому знати міру, адже Інтернет – це не все життя. А «зловживання» їм приводить до таких наслідків, як марна трата часу і шкоди для здоров'я.

Безпека в інтернеті – дуже важлива проблема нинішнього часу. І стосується вона всіх, від дітей до пенсіонерів. Вона стає все актуальнішою у зв'язку з масовим приходом в інтернет користувачів, майже, а то і зовсім, чи не підготовлених до погроз, їх чекають. Адже страждає не один користувач, а й багато інших, об'єднані в одну глобальну структуру

Зрозумійте, що реально тільки те, що відбувається з вами тут і зараз, а не у віртуальному світі, мережеві ресурси навіть не помітять вашого зникнення, зате ви побачите, наскільки вам вільніше і легше стане без них. Повірте, що ваш вигаданий світ ніколи не замінить вам реального спілкування з людьми.

І пам'ятайте одне, не варто приносити в жертву своє реальне життя, адже навколишній світ набагато цікавіший, навчіться використовувати ресурси соціальних мереж з користю для себе і тільки в міру гострої необхідності. Тож подумайте про свою безпеку завчасно. І вона у Ваших руках!

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Захист дітей у цифровому середовищі: рекомендації для індустрій 2020. Опубліковано у Швейцарії Женева, 2020 р. https://thedigital.gov.ua/storage/uploads/files/news_post/ 2021/1/za-initsiativi-mintsifri-pidgotuvali-rekomendatsii-shchodo-zakhistu-ditey-u-tsifrovomu-seredovishchi/COP_Guidelines_Industry_UA_fin66.pdf
2. Колесник, Оксана Олександрівна. Формування етики спілкування підлітків у мережі Інтернет у навчальному процесі загальноосвітньої школи М-во освіти і науки України, Харків. нац. пед. ун-т ім. Г. С. Сковороди. - Харків, 2016.
3. Савич С.С. Авторське право у цифровому середовищі: проблема монополії правовласника та забезпечення умов вільного використання творів/С.С. Савич// Бюлетень Міністерства Юстиції України. – 2015. - № 1. – С. 87.

4. Биков В.Ю. Цифрова трансформація суспільства і розвиток комп'ютерно-технологічної платформи освіти і науки України. Матеріали методологічного семінару НАПН України "Інформаційно-цифровий освітній простір України: трансформаційні проце.
5. Together Європейський простір «21 правило цифрової безпеки» https://euprostir.org.ua/practices/133410

14 БОРОТЬБА З ФЕЙКАМИ ТА ДЕЗІНФОРМАЦІЄЮ В УМОВАХ ІНФОРМАЦІЙНОЇ ВІЙНИ

Доповідач:Вікторія КУШКО
Керівник: Олена СКОРНЯКОВА
ВСП «Одеський технічний фаховий коледж
Одеського національного технологічного університету»

В даний час фейки і дезінформація є серйозною загрозою для суспільства, особливо в умовах інформаційної війни, коли сторони конфлікту активно використовують їх для досягнення своїх цілей. Під час інформаційного суспільства, де інтернет та соціальні мережі стали невід'ємною частиною нашого життя, проблема фейків та дезінформації стала особливо актуальною. В умовах інформаційної війни, коли одні люди прагнуть маніпулювати громадською думкою, боротьба з фейками та дезінформацією стає важливим завданням для захисту інтересів та підтримки стабільності.

Одним з основних інструментів інформаційної війни є фейки та дезінформація. Фейки – це хибні повідомлення, які поширюються групою людей обману і маніпуляцією суспільства. Дезінформація, своєю чергою, постійне поширення хибної чи неправильної інформації. Вони можуть впливати на політичну ситуацію, психологічний стан, економіку. Боротьба з фейками та дезінформацією потребує посилених заходів.

Основне завдання фейків та дезінформації в інтернеті на період інформаційної війни полягає у маніпуляції над суспільством впливу на думку оточуючих. Це може бути досягнуто шляхом створення та розповсюдження хибної чи спотвореної інформації з метою навіяти певну точку зору або переконати людей у чомусь, що не відповідає дійсності. Дезінформація може використовуватися для створення напруженості та конфліктів всередині країни чи між країнами. Метою інформаційної війни є не лише вплив на громадськість, а й отримання контролю над інформаційним потоком, що може надати перевагу у досягненні різних цілей.

В умовах інформаційної війни боротьба з фейками та дезінформацією стає особливо важливим завданням для всього світу. Сьогодні багато людей отримують інформацію з інтернету, по радіо, телевізору, і багато хто не має достатніх знань і навичок, щоб відрізняти правду від брехні. В країнах створюють спеціальні органи боротьби з дезінформацією. За ці роки потік перекручених, а часто й просто вигаданих новин не лише не зменшився, а навпаки, зріс.

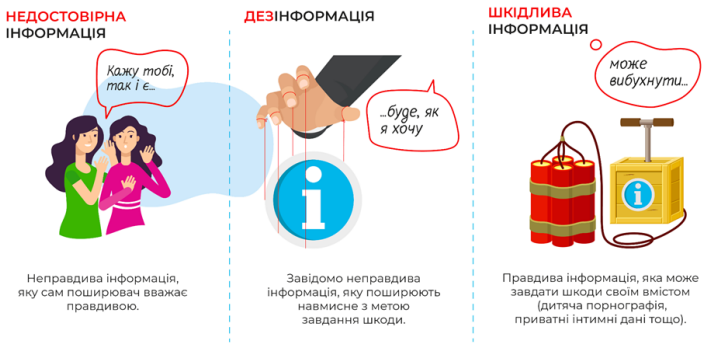


Рис.1 - Види неправдивої інформації

Іноді ефективна робота журналіста практично неможлива. Дані із незалежних джерел - на вагу золота. Інформаційний потік заповнюють пости, фотографії та відеокліпи користувачів соцмереж, а також дані, які публікують народ країн. Перевірити ще раз інформацію буває дуже важко, і вони не завжди дають уявлення про реальну ситуацію. Для боротьби з фейками та дезінформацією важливо насамперед забезпечити доступність до достовірної інформації. Необхідно допомагати створенню та розвитку незалежних новин, підтримувати журналістську етику та свободу слова.

Одним із ключових моментів у боротьбі з фейками та дезінформацією є розвиток здатності до оцінки інформації та вміння працювати з медіа-ресурсами в суспільстві. Але це не завжди просто, оскільки багато людей не знають, як відрізнити правду від брехні у потоці інформації.

Найважливішим фактором у боротьбі з фейками та дезінформацією є створення системи відбору інформації за певними критеріями та контроль джерел інформації. Такі системи повинні ґрунтуватися на використанні сучасних технологій, які можуть допомогти в визначенні фейків та дезінформації.

Інформаційна війна становить велику небезпеку, оскільки вона поєднуватиметься з технічними атаками; так само вона націлена на слабку ланку – на людину. Люди повинні навчитися аналізувати отриману ними інформацію, перевіряти її достовірність та відрізняти правду від брехні. Досягнення цієї мети можливе шляхом освіти та розвитку критичного мислення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Фейк як інструмент інформаційної війни. https://yur-gazeta.com/ publications/ practice/inshe/feyk-yak-instrument-informaciynoyi-viyni.html
2. Муратова Н., Тошпулатова Н., Алимова Г. Fake news: дезинформация в медиа : пособие. Ташкент :Innovatsion rivojlanish nashriyot-matbaa, 2020. 104 с.
3. Черниш Р. Ф. Фейк як один із інструментів негативного впливу на національну безпеку України в умовах ведення гібридної війни. Часопис Київського університету права. 2019. № 2. С. 109–114. DOI: 10.36695/2219-5521.2.2019.19.
4. Центр протидії дезінформації при РНБО. URL: https://cpd.gov.ua/category/reports/#.
5. ЦПД при РНБО України ініціює створення міжнародного хабу з протидії інформаційним загрозам. Рада національної безпеки і оборони України : [сайт]. URL: https://www.rnbo.gov.ua/ua/Diialnist/5708.html.

15 СИСТЕМИ ЗАХИСТУ ОСОБИСТИХ РАХУНКІВ КЛІЄНТІВ БАНКІВ

Доповідач: Надія САХАРОВА
Керівник: Інна КАСАПОВА
ВСП «Одеський технічний фаховий коледж Одеського національного технологічного університету»

Безпека банків в Україні є важливою з точки зору фінансової стабільності країни та захисту інтересів клієнтів банків. Банки є важливими інституціями в економіці, які здійснюють функції зберігання та перерозподілу фінансових ресурсів. У разі невірного керування банківською діяльністю, або несправності механізмів банківської системи, може відбутися криза, яка може негативно вплинути на економіку країни та загрожувати безпеці фінансових активів клієнтів банків.

Тому, банки в Україні повинні дотримуватись строгих нормативно-правових вимог щодо захисту фінансових активів клієнтів, забезпечення кібербезпеки, міцності банківської системи, здійснювати регулярний моніторинг та аудит внутрішніх процесів та операцій. Для забезпечення цих вимог банки мають вести політику ризик-менеджменту, включаючи виявлення, оцінку та контроль ризиків, пов'язаних з їх діяльністю. Крім того, банки повинні бути готовими до негативних наслідків кризових ситуацій та розробляти плани дій для запобігання таким ситуаціям.

Безпека банку – це його стан захищеності від зовнішніх та внутрішніх загроз, який дозволяє надійно зберегти та ефективно використовувати фінансовий, матеріальний та кадровий потенціал.

Банк, при забезпеченні безпеки, повинні чітко притримуватись банківської таємниці. Банківською таємницею згідно з частиною першою статті 60 Закону України «Про банки і банківську діяльність» [1] є - інформація щодо діяльності та фінансового стану клієнта, яка стала відомою банку у процесі обслуговування клієнта та взаємовідносин з ним чи третім особам при наданні послуг банку.

Банківською таємницею, зокрема, є:

1. відомості про банківські рахунки клієнтів, у тому числі кореспондентські рахунки банків у Національному банку України
2. операції, які були проведені на користь чи за дорученням клієнта, здійснені ним угоди
3. фінансово-економічний стан клієнтів;
4. системи охорони банку та клієнтів;
5. інформація про організаційно-правову структуру юридичної особи - клієнта, її керівників, напрями діяльності;
6. відомості стосовно комерційної діяльності клієнтів чи комерційної таємниці, будь-якого проекту, винаходів, зразків продукції та інша комерційна інформація;
7. інформація щодо звітності по окремому банку, за винятком тієї, що підлягає опублікуванню;
8. коди, що використовуються банками для захисту інформації.
9. інформація про фізичну особу, яка має намір укласти договір про споживчий кредит, отримана під час оцінки її кредитоспроможності.

Розглянемо докладніше, що таке банківський рахунок та які дані надаються банкам клієнтами, що його відкривають.

Банківський рахунок - це рахунок, який клієнт (фізична або юридична особа) відкриває в банку для зберігання грошових коштів та здійснення фінансових операцій, таких як перекази коштів, оплата рахунків тощо. Рахунок має свій унікальний номер, який ідентифікує його в банківській системі. Банківський рахунок може бути відкритий в різних валютах залежно від потреб клієнта та політики банку.

Для відкриття рахунку в банку зазвичай потрібно надати наступні документи та інформацію:

1. Паспорт або інший документ, що посвідчує особу.
2. Ідентифікаційний номер (ІПН).
3. Контактні дані (телефон, електронна пошта, адреса).
4. Довідку про доходи або інші документи, що підтверджують джерела доходів.
5. Для відкриття рахунку для підприємства також потрібні статут, довідка про реєстрацію, документи, що підтверджують повноваження осіб, які мають право діяти від імені підприємства.
6. Внесення початкового внеску на рахунок.

Документи та інформація, що потрібні для відкриття рахунку, можуть відрізнятися в залежності від банку та типу рахунку.

“З метою зниження ризиків шахрайства надавачі платіжних послуг застосовуватимуть посилену автентифікацію”, - було повідомлено в НБУ.

Так, надавачі платіжних послуг зобов’язані застосовувати посилену автентифікацію користувачів під час:

- отримання ними дистанційного доступу до рахунків;
- ініціювання дистанційної платіжної операції;
- будь-яких інших дій у разі підозри вчинення шахрайства чи інших неправомірних дій (або існування такого ризику).

Такі норми містить постанова Правління Національного банку України від 03 травня 2023 року № 58 "Про затвердження Положення про автентифікацію та застосування посиленої автентифікації на платіжному ринку", що набула чинності 10 травня 2023 [2].

Обробка персональних даних здійснюється всіма банками країни. Докладну інформацію про їх обробку та зберігання можна дізнатись на сайті окремого банку. В даному випадку розглянемо на прикладі АТ “ПУМБ”

Банк збирає тільки ті персональні дані (наприклад, Ваше ім'я і прізвище, логін і пароль доступу, адреса електронної пошти, номер контактного телефону, дата народження, стать і т.д.), які свідомо і добровільно надані Вами як суб'єктом персональних даних в цілях використання послуг, що надаються Банком, сервісів Сайту, що відповідно до вимог законодавства є згодою суб'єкта персональних даних на обробку своїх персональних даних відповідно до сформульованої в цій Політиці мети їх обробки.

При відвідуванні Сайту фіксуються всі входи до системи. Інші відомості по трафіку користувача не обробляються і не зберігаються.

Персональні дані використовуються в цілях забезпечення надання Банком банківських, фінансових та інших послуг, Інтернет-сервісів Сайту, обміну інформацією, новинами, відносин у сфері реклами та комунікації відповідно та на виконання законів України, у тому числі, але не виключно: «Про банки і банківську діяльність». «Про захист персональних даних», «Про ратифікацію Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних», «Про інформацію», «Про рекламу», а також з урахуванням принципів та правил Регламента General Data Protection Regulation (GDPR) Європейського Союзу.

Розглянемо обробку персональних даних на прикладі АТ «Пумб».

Метою обробки персональних даних є надання банківських, фінансових послуг, встановлення ділових стосунків та договірних відносин, підготовки статистичної, адміністративної та іншої інформації, відповідно до вимог законодавства, а також внутрішніх документів АТ «ПУМБ» з питань банківської діяльності. АТ «ПУМБ» може використовувати знеособлені дані з метою таргетингу рекламних та/або інформаційних матеріалів за віком, статтю, іншими даними; проведення статистичних досліджень.

Персональні дані зберігаються протягом строку не більше, ніж це необхідно відповідно до мети їх обробки.

Після того, як суб'єкт персональних даних перестав бути користувачем Сайту шляхом видалення свого облікового запису на Сайті, його персональні дані також автоматично видаляються.

Строк зберігання персональних даних при наданні банківської, фінансової послуги залежить від виду фінансової (банківської) послуги і може визначатися відповідно до нормативно-правових актів (в тому числі НБУ) та бути встановлений від 5 до 10 років (при відмові у наданні послуги або інших виняткових випадках строк може відрізнятися) [3].

Передача персональних даних між банком та клієнтом відбувається завдяки системі BankID Національного банку. Це державна система віддаленої ідентифікації, яка забезпечує передачу персональних даних користувачів від банку, в якому відкрито рахунок, до суб'єкта, який надає користувачу послугу.

Електронна дистанційна ідентифікація фізичних осіб з використанням Системи BankID НБУ відбувається шляхом передачі персональних даних такої особи від абонента ідентифікатора (банку, в якому відкрито рахунок користувача), до абонента надавача послуг, який надає послугу користувачу та є безпечною для користувачів. Тільки користувач (власник персональних даних) може ініціювати передачу цих даних від абонента ідентифікатора до абонента надавача послуг. Отже, ніхто, крім вас, не може ініціювати цей процес! Інформація передається в зашифрованому вигляді відповідно до вимог законодавства України [4].

У разі розголошення інформації, що являє собою банківську таємницю банківська установа та її працівники несуть кримінальну відповідальність.

Згідно з частиною другою статті 1076 Цивільного кодексу України у разі розголошення банком відомостей, що становлять банківську таємницю, клієнт має право вимагати від банку відшкодування завданих збитків та моральної шкоди. [5]

Статті 231 та 232 Кримінального кодексу України [6] встановлюють кримінальну відповідальність за порушення банківської таємниці.

Стаття 231. Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю.

Умисні дії, спрямовані на отримання відомостей, що становлять комерційну або банківську таємницю, з метою розголошення чи іншого використання цих відомостей, а також незаконне використання таких відомостей, якщо це завдало істотної шкоди суб'єкту господарської діяльності, - караються штрафом від трьох тисяч до восьми тисяч неоподатковуваних мінімумів доходів громадян.

Стаття 232. Розголошення комерційної або банківської таємниці

Умисне розголошення комерційної або банківської таємниці без згоди її власника особою, якій ця таємниця відома у зв'язку з професійною або службовою діяльністю, якщо воно вчинене з корисливих чи інших особистих мотивів і завдало істотної шкоди суб'єкту господарської діяльності, - карається штрафом від однієї тисячі до трьох тисяч неоподатковуваних мінімумів доходів громадян з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років.

Системи захисту особистих рахунків клієнтів банків включають ряд технологій і практик, розроблених для запобігання несанкціонованому доступу, втраті або крадіжці особистої фінансової інформації. Ось декілька ключових елементів цих систем:

1. Аутентифікація: Банки використовують різні методи аутентифікації, щоб переконатися, що людина, яка намагається отримати доступ до рахунку, є законним власником. Це може включати паролі, PIN-коди, біометричні дані (наприклад, відбитки пальців або розпізнавання обличчя) та двофакторну аутентифікацію, коли потрібно підтвердити свою особу двома різними способами.

2. Шифрування: Банки використовують різні форми шифрування для захисту даних, коли вони передаються або зберігаються. Шифрування перетворює читаємі дані на код, який можна розшифрувати тільки за допомогою спеціального ключа.

3. Системи виявлення вторгнень: Ці системи спостерігають за мережевим трафіком та блокують підозрілу активність, яка може вказувати на спробу вторгнення.

4. Антивірусне програмне забезпечення: Банки встановлюють антивірусне програмне забезпечення на своїх серверах та робочих станціях, щоб захистити систему від шкідливого програмного забезпечення.

5. Освіта клієнтів: Банки також залучаються до освіти своїх клієнтів щодо безпечних практик онлайн, таких як не розголошення паролів та не відкриття підозрілих електронних листів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України “Про банки і банківську діяльність” від 07.12.2000 № 2121-III [Інтернет-ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2121-14/page4#Text

2. Офіційний сайт НБУ – Застосування посиленої автентифікації користувачами платіжних послуг, з метою запобігання шахрайства [Інтернет-ресурс] – Режим доступу: https://bank.gov.ua/ua/news/all/z-metoyu-znijennya-rizikiv-shahraystva-nadavachi-platijnih-poslug-zastosuvatimut-posilenu-avtentifikatsiyu-16500

3. Офіційний сайт АТ «Пумб» - Загальні принципи конфіденційності та захисту персональних даних [Інтернет-ресурс] – Режим доступу: https://about.pumb.ua/info/personal_data
4. Офіційний сайт НБУ - Про Систему BankID Національного банку [Інтернет-ресурс] – Режим доступу: https://bank.gov.ua/ua/bank-id-nbu
5. Цивільний кодекс України. Кодекс України; Закон, Кодекс від 16.01.2003 № 435-IV [Інтернет-ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/435-15#Text
6. Кримінальний кодекс України. Кодекс України; Кодекс, Закон від 05.04.2001 № 2341-III [Інтернет-ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2341-14#Text

16 БЕЗПЕКА В ІНТЕРНЕТ-БАНКІНГУ

Доповідач: Вікторія ТОКАРЧУК
Керівник: Кубова Т.М.
Фаховий коледж нафтогазових технологій, інженерії та інфраструктури сервісу ОНТУ

Порядок дій у разі виявлення випадку несанкціонованого доступу до рахунку або підозри на компрометацію логіну, пароля або ключа. У випадках виявлення несанкціонованого доступу або підозри на несанкціонований доступ до рахунку або компрометації/ підозри на компрометацію логіну, пароля або ключа; нероботоспроможності системи Enter EXIM або комп'ютера потрібно негайно повідомити Контакт-центр за телефонами: 0-800-50-44-50 (дзвінки по Україні безкоштовні), +38 044-247-38-38.

При цьому обов'язково необхідно здійснити звірку залишку коштів на рахунку та перелік останніх платежів. У разі виявлення несанкціонованого платежу у найкоротший термін передати до банку письмове повідомлення, в якому докладно викласти всі обставини несанкціонованого доступу.

Механізми захисту:

1. Шифрування даних – використовується для забезпечення конфіденційності переданої інформації. Всі електронні документи передаються в зашифрованому вигляді. Шифрування даних здійснюється на сесійних ключах за протоколом TLS.
2. Електронно-цифровий підпис (ЕЦП) – використовується для забезпечення автентичності (доказ авторства) і цілісності документа в Інтернет-банкінгу. Саме електронний документ з ЕЦП є доказовою базою при вирішенні конфліктної ситуації. В Enter EXIM реалізовані алгоритми ЕЦП - RSA ключем.
3. Двофакторна аутентифікація – використовується для забезпечення суворої аутентифікації клієнта при роботі з Інтернет-банкінгом. Для аутентифікації можуть використовуватись пристрої захисту: генератор одноразових паролів (Vasco) та захищений носій особистого ключа для електронно-цифрового підпису (iKey або MiniKey).

У час віртуалізації багатьох процесів життя, а зокрема розрахунків у мережі Інтернет, варто не забувати, що шахраї також не сплять. Багато українців, маючи гіркий досвід втрати банківських коштів, бояться користуватись сервісами Інтернет-банкінгу. Та є прості правила, як можна убезпечити себе від подібних розчарувань та втрат.

Свою формулу захисту вивів співзасновник monobank Олег Гороховський. Він переконаний, що 99,9% випадків ІТ-шахрайства вдалося б уникнути, якби клієнти керувалися простими рекомендаціями з техніки безпеки.

1. Входьте у клієнт-банк лише за прямим посиланням, яке ви зберегли в своєму браузері при першому вході.

Це потрібно для того, щоб ви не натрапили на дуже схоже, але фальшиве посилання, що імітує оригінальний клієнт-банк. Банки зазвичай не відправляють листів з посиланнями на вхід в свій клієнт-банк, у будь-якому разі ігноруйте такі посилання.

2. Якщо вам дзвонять чи пишуть нібито з банку і просять повідомити будь-який ПІН-код, пароль чи якусь іншу конфіденційну інформацію, НІКОЛИ не надавайте таких даних.

3. Паролі і коди можуть вкрасти з вашого комп'ютера чи фізично чи з допомогою троянських програм, тому важливе правило: НЕ ЗБЕРІГАЙТЕ паролі на комп'ютері. Навіть смартфон надійніший у цьому випадку, але теж на 100% не є гарантією безпеки. Краще паролі придумувати за певним своїм (не примітивним) алгоритмом і запам'ятовувати, а не записувати.

4. Краще взагалі відмовитись від десктопних клієнт-банків, а користуватись мобільними додатками. Хороші банки при цьому розпізнають вхід із десктопа як нетипову активність і завадять крадіжці великої суми з вашого рахунку.

5. Не ведіться на будь-які телефонні чи онлайн-прохання про терміновий переказ коштів. Часто люди добровільно перераховують кошти під надуманими шахраями приводами. Зазвичай просять хабар за звільнення родича з в'язниці, оплатити лотерейний квиток, який вже нібито виграв автомобіль і багато інших психологічних фішок.

Це можна порівняти з гіпнозом вуличних ворожок, яким людина може останнє віддати.

ЗАГАЛЬНІ ПИТАННЯ ІР-БЕЗПЕКИ

При впровадження Internet-banking водночас проводять зміни поточної політики /Р-безпеки банку. Сервери системи Internet-banking, як правило, розміщують в окремому мережевому сегменті з доступом з мережі Internet, що контролюється на міжмережевому екрані (Firewall), і з внутрішньої захищеної мережі банку.

АРМ Адміністратор, АРМ Операціоніст і Шлюз для інтеграції Internet-banking із САБО розміщують у внутрішній захищеній мережі банку, де розташований сервер САБО.

НА МІЖМЕРЕЖЕВОМУ ЕКРАНІ ДОДАЮТЬ ТАКІ ПРАВА ДОСТУПУ:

1. для обслуговування клієнтів дозволено вхідні з'єднання з мережі Internet тільки на TCP-порти Web-сервера Internet-banking (протокол HTTPS) і Сервера застосувань Internet-banking (протокол IBTP);
2. для роботи АРМ Операціоніст дозволено вхідні з'єднання з внутрішньої захищеної мережі банку тільки на TCP-порти Web-сервера Internet-banking (протокол HTTPS) і Сервера застосувань Internet-banking (протокол IBTP);
3. для роботи Шлюзу і АРМ Адміністратор дозволяються вихідні з'єднання з внутрішньої захищеної мережі банку тільки на TCP-порти Сервера БД системи Internet-banking;

4. заборонено всі вхідні з'єднання з мережі Internet і з внутрішньої захищеної мережі банку до сегменту із серверами Internet-banking для всіх інших TCP-портів та інших IP-протоколів;
5. заборонено всі вихідні з'єднання зі сегментів із серверами Internet-banking;
6. заборонено всі вхідні з'єднання у внутрішню захищену мережу банку, де розташований сервер САБО (це загальне правило, що не залежить від наявності системи Internet-banking).

Тому потрібно завжди бути на сторожі, дотримуватись правил техніки Інтернет-безпеки та елементарної ІТ-гігієни. За цим стоять ваші гроші.

17 БЕЗПЕКА ЕЛЕКТРОННОЇ КОМЕРЦІЇ

Доповідач: Ольга ЧОРНА
Керівник: Інна КАСАПОВА
ВСП «Одеський технічний фаховий коледж
Одеського національного технологічного університету»

Зважаючи на актуальність проблеми безпепечного пошуку товарів в електронних магазинах, метою нашої розвітки є розглянути основні різновиди безпеки електронної комерції та отримати уявлення про те, як знайти та купити певний товар, що продається в електронних магазинах через Інтернет.

Аналіз сучасних сайтів свідчить про значне збільшення Інтернет шахрайств, яке з кожним роком набирає все більших обертів. Проте, з огляду на складність та дискусійність поняття електронної комерції , є багато способів розпізнавання шахрайства та правила безпеки електронної комерції.

Багато людей вже давно не можуть уявити своє життя без смартфона. Цей факт визначає як особливості нашого дозвілля, а й принципи сучасного бізнесу. Людям значно простіше шукати інформацію, спілкуватися, дивитися відео та робити покупки у своєму мобільному телефоні. Від таких зручностей відмовитись неможливо. Мобільна комерція вступає у гру та займає лідерські позиції.

Мобільна комерція - це принцип ведення бізнесу, який передбачає продаж товарів і послуг без фізичної присутності покупців і продавців, за допомогою лише смартфонів, через додатки. Поняття інтернет-магазинів давно нікого не дивує – на сайтах можна купити продукцію практично будь-якого бренду. Тепер мова йде про додатки з тими ж можливостями, але ще більшим рівнем персоналізації та зручності.

Термін “m-commerce“, який і означає мобільну комерцію, означає також – перегляд, покупку і продаж продукції чи послуг через мобільні пристрої. Іншими словами, це повноцінна онлайн покупка, здійснювати яку найзручніше з мобільного телефону (планшету), який виконує роль основного інтерфейсу користувача для ряду сервісів.

Мобільна комерція – лише різновид електронної комерції. Обидва поняття припускають продажі та покупки онлайн за допомогою софту. Для цього не потрібен фактичний контакт і навіть наявність у продавця фізичного магазину. Але мобільна електронна комерція передбачає не просто сайт, на який можна зайти, використовуючи браузер (що доступно практично для будь-якого інтернет-магазину та через смартфон),

а програма, яка встановлюється на смартфон і робить доступ до покупок ще більш простим та зручним.

Переваги та недоліки мобільної комерції

Переваги мобільної комерції:

– доступність для ваших користувачів. Вони мають постійний і комфортний доступ до покупок у вас з будь-якої точки світу, в будь-який час. Для замовлення достатньо клікнути по іконці на екрані смартфона. Головне, щоб був доступ до інтернету.

– зручність. Користувачам більше не потрібно шукати ваш сайт в інтернеті та відкривати його у браузері. Більше того, не всі інтернет-магазини добре адаптовані під мобільні пристрої, що може зробити спонтанні покупки незручними. Ваші потенційні покупці у такому разі просто підуть до інших продавців.

– можливість робити покупки набагато швидше. У додатку ваші покупці можуть зберегти свої дані, їм не доведеться вводити їх щоразу для нової покупки. Це стосується і даних про доставку, інформації про покупця, і платіжних даних. А чим легше і швидше можна здійснити покупку, тим більше користувачі схильні купувати та повертатися до вас знову та знову.

– лояльність до ваших покупців. Адже чим комфортніше їм з вами, тим вища їхня вірність вашому бренду.

– можливість персоналізації. Додатки мобільної комерції дозволяють вам пропонувати користувачам додаткові товари, ґрунтуючись на їх перевагах та покупках, робити знижки та спеціальні пропозиції, пропонувати систему бонусів, надсилати нагадування про залишені кошики або товари у збереженому. Клієнти цінують турботу про себе та індивідуальні пропозиції.

Недоліки мобільної комерції:

– якщо ваша цільова аудиторія складається не тільки з тих, хто все робить через смартфон, а й із прихильників ПК та ноутбуків – вам доведеться розробляти додатковий інструмент для роботи з клієнтами у браузері. Який - залежить тільки від ваших цілей та переваг. Але якщо цей інструмент у вас є, m-Commerce рішення стануть відмінним доповненням для задоволення 100% вашої цільової аудиторії.

– IOS або Android. Якщо у вашій цільовій аудиторії перевага у бік однієї системи менша, ніж 99%, вам доведеться передбачити розробку програми так, щоб вона коректно функціонувала на обох (або трьох, чотирьох тощо) платформах.

Тим не менш, мобільна комерція допомагає охопити ще ширшу аудиторію і поліпшити її досвід користувача.Саме у взаємодії перерахованих компонентів формується довіра споживачів до підприємств електронної комерції. Основ-ним користувачі вважають безпеку проведення платіжних трансакцій і конфіденційність їхньої персональної інформації. На захист інтересів користувачів спрямовані законодавчі акти, технологічні й організаційні заходи, процедури страхування і контролю. Не менш важливим користувачі вважають гаранту-вання послідовності та цілісності трансакцій і правомочність їх проведення всіма сторонами.

Електронна комерція (або e-commerce) – це сфера економіки, де з використанням Інтернету можливе проведення комерційних операцій між підприємствами або між підприємством та споживачами.Зі зростанням індустрії електронної комерції, зросли також випадки кіберзлочинів. Зловмисники

використовують різні засоби для наживи або просто, щоби дестабілізувати онлайн-бізнес конкурентів. На щастя, кожну загрозу вашому онлайн-магазину можна запобігти з використанням потрібних інструментів.

Інтернет шахрайство з кожним роком набирає все більших обертів. Не виключенням стала й популярна платформа онлайн-оголошень OLX. Тисячі людей, які купують товари в інтернеті, часто стають жертвами шахраїв, які за роки існування онлайн-торгівлі вигадали чимало схем, за допомогою яких за кілька секунд заробляють гроші на довірливих клієнтах. Схема проста, але досить популярна. Шахрай дає оголошення про продаж товару на OLX, знаходиться покупець, в якого просять невелику передплату – наприклад, 200 грн. Вся Україна продає і купує різні товари на цій площадці. Але є і «новачки», які вперше виставляють своє оголошення з надією на успішний продаж. Яке ж здивування і радість їх очікує, коли на Viber чи не одразу приходять повідомлення від «покупців».

Фішинг в OLX Доставка: Фішинг - це сучасний вид шахрайства, який спрямований на незаконне отримання даних користувачів: логіна, пароля, платежів, одноразових паролів, іншої інформації з обмеженим доступом. Якщо просто, фішинг — це як вовк в овечій шкурі . Його ідея в тому, щоб під виглядом сайту, якому ви довіряєте, виманити у вас особисті дані, найчастіше — платіжні дані карти.

Як розпізнати фішинг в OLX Доставка. Пам'ятайте найголовніші правила:

– посилання в особисті повідомлення - ЗЛО: не переходьте за посиланнями, які вам відправляють в особистих повідомленнях нібито для купівлі товару / скасування угоди / повернення ваших коштів і подібне;

– в OLX Доставка немає ніяких збоїв/помилок, при яких угода скасовується і вам потрібно знову вводити дані карти для повернення коштів або повторної оплати. Якщо продавець не відправить товар — кошти повертаються на вашу карту автоматично (дивіться Коли покупцю повернуться гроші по OLX Доставка);

– актуальна і 100% вірна інформація про статус вашої угоди є тільки у вашому профілі OLX, на вкладці «OLX Доставка» — завжди перевіряйте там, особливо якщо ви отримали повідомлення про помилку при замовленні / про скасування замовлення (до слова, якщо ви отримали таке повідомлення — дивіться попереднє правило);

– ми НЕ відправляємо ніяких SMS і Viber повідомлень від OLX Доставка — повідомлення приходять тільки на вашу поштову скриньку і в додатку OLX;

– в роботі послуги OLX Доставка відсутні будь-які індивідуальні форми і посилання для здійснення угоди / отримання коштів по угоді.

А тепер детальніше про правила безпеки:

– не переходьте в месенджери:обговорюйте деталі угод тільки в чаті OLX і не переходьте в сторонні месенджери — там ми не зможемо забезпечити безпеку (наприклад, якщо вам пропонують обговорити деталі в Viber, Telegram, WhatsApp і ін.).

– оформляйте угоди з OLX Доставка тільки на OLX:купуйте товар тільки на https://www.olx.ua або в офіційному додатку OLX.

– перевіряйте адресу сайту, перш ніж перейти за посиланням і звертайте увагу на домен: повна версія сервісу OLX.ua виглядає olx.ua, мобільна версія - m.olx.ua, бізнес-сторінка на OLX - name.olx.ua.

– рекомендують не відкривати посилання від незнайомих або малознайомих співрозмовників — це, в тому числі, і базове правило безпеки в Інтернеті.
– при отриманні сервісних листів, звертайте увагу на домен — у OLX він завжди ***@olx.ua. Будь-які інші варіанти (наприклад, ***@olx.uy) є підробленими і можуть привести вас до шахраїв.
– важливо: зараз Служба підтримки OLX працює в двох каналах — телефонна лінія та письмова підтримка по email через форму зворотного зв'язку «Чат». Посилання в Центрі підтримки клієнтів має вигляд help.olx.ua/.
– найпростіший спосіб розпізнати фішинг — це знати як працює послуга. Ознайомтеся з нею в нашому розділі Послуга OLX Доставка, щоб в тому числі не попастися на «підставні» інструкції від шахраїв.
– зверніть також увагу на адресу чату — olx.ua.dostavka24.rent, він не відноситься до OLX адже на оригінальній OLX сторінці після olx.ua завжди стоїть знак "/".

“Ми в OLX постійно працюємо над удосконаленням кіберзахисту на платформі, щоб наші користувачі могли здійснювати безпечні угоди. Однак варто пам’ятати, що захищеність в онлайні залежить від кожного з нас. Шахраї використовують методи соціальної інженерії. Вони добре знають, якими діями та словами схилити “клієнта” до швидкої та необдуманої угоди. Коли користувачі більше цікавляться безпекою у мережі та прокачують свої знання, а компанії створюють власні ініціативи, можна ефективніше боротися з шахраями та насолоджуватися безпечним онлайн-шопінгом”, — коментує Віктор Нобіуз, керівник відділу бізнес-аналітики OLX Україна.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Безпека електронної комерції [Електронний ресурс]: навч. посібн. / І.М. Пістунов, Є.В. Кочура ; Нац. гірн. ун–т. – Електрон. текст. дані. – Д. : НГУ, [2014. – 125 с.] – Режим доступу: http://pistunovi.narod.ru/6_E_K.
2. С. Виганяйло. Аспекти економічної безпеки електронної комерції. Економіка. Фінанси. Право. – 2021. – [№ 4. – С. 28-30.] – DOI: https://doi.org/10.37634/efp.2021.4.5.
3. Про електронну комерцію Закон України від [03.09.2015 № 0957] / [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/675-19#Text/.
4. Електронна комерція : Навч. посібник / А. М. Береза, І. А. Козак, Ф. А. Левченко та ін. – К. : КНЕУ, [2012. – 326 с.]

18 ІНФОРМАЦІЙНА БЕЗПЕКА. МЕТОДИ ВЕДЕННЯ ІНФОРМАЦІЙНОЇ ВІЙНИ В ЦИФРОВОМУ СЕРЕДОВИЩІ

Доповідач: Аліна ЯРОШЕНКО
Керівник: Олена СКОРНЯКОВА
ВСП «Одеський технічний фаховий коледж Одеського національного технологічного університету»

Інформаційна війна в цифровому середовищі — це процес використання цифрових технологій, методів для впливу на громадську думку та маніпулювання інформацією, що формує у суспільстві чи групі людей потрібну точку зору.

Цілями інформаційної війни є:

1. послабити моральні і матеріальні сили супротивника та посилити власні;
2. створення атмосфери бездуховності й аморальності, негативного відношення до культурної спадщини противника;
3. маніпулювання населенням країни з метою створення політичної напруженості та хаосу;
4. внесення у суспільну та індивідуальну свідомість ворожі, шкідливі ідеї та погляди;
5. залякування супротивника своєю могутністю.

Це передбачає заходи пропагандистського впливу на свідомість людей в ідеологічній та емоційній галузях.

Для ведення інформаційної війни недостатньо мати свій власний ресурс, оскільки тоді можна впливати лише на вузьку аудиторію. Тому атакуюча сторона має взяти під контроль певний інформаційний канал, наприклад популярну групу в соціальній мережі чи відомого блогера, чи сайт, тобто увійти в інформаційне поле супротивника.

Основні методи ведення інформаційної війни в цифровому середовищі:

1) дезінформація та фейкові новини — відкрите поширення неправдивої інформації, викривлення змісту документів чи ретельно вигадані фейки, що поширюються в соціальних мережах.

Дезінформація намагається впливати на громадську думку та формувати негативне ставлення до певної особи, групи або країни. Може бути поширена через соціальні медіа, блоги, форуми та інші онлайн-ресурси.

2) хакерські атаки та кібершпигунство — злам комп'ютерних систем, викрадення даних та шпигунство в мережі. Після крадіжки інформація може бути використана у інформаційній війні, наприклад, це може бути її розкриття чи навіть спотворення правдивих даних.

Також можуть розповсюджуватись шкідливі програми або проводитись атаки на інші системи. Інформаційна атака зі зламаного акаунта людей, яким довіряють певні кола та групи громадян, спроможна вчинити справжню паніку. Ще зламаний акаунт, в умовах інформаційної війни, можуть задіяти для політичної агітації тощо.

3) розпалювання конфліктів — провокування віртуальних конфліктів між користувачами соціальних мереж. Деякі користувачі намагаються розпочати розмову з провокативних питань в групі, або в гілці обговорення на тему з зовсім іншої галузі.

4) соціальна інженерія — спроби зламу механізмів довіри між особами або спроби маніпулювання інформацією, яка може викликати емоційну реакцію.

5) боти та фейкові аккаунти — автоматизовані акаунти, створені з метою поширення інформації.

6) використання інтернет-тролів — це можуть бути люди, які спеціально зареєстровані в соціальних мережах для того, щоб поширювати дезінформацію та негативні коментарі.

7) використання соціальних мереж та месенджерів — це є потужним засобом впливу на громадську думку. За допомогою рекламних кампаній, ботів та інших інструментів, можна поширювати дезінформацію та маніпулювати громадською думкою.

Важливо розуміти, що війна - це війна, навіть коли ми говоримо про інформаційне протистояння. В ній завжди є брудні методи. Є думка яка говорить: якщо в інформаційній війні одна сторона оперує брехнею, а інша правдою, то друга сторона програє, оскільки вона обмежене лише своєю правдою. Вона не може видати неіснуючі підтвердження, а от сторона, яка оперує брехнею, може видавати будь-які здогадки за факти без обмежень.

І ця брехня постійно заповнює інформаційне поле, що з часом заважає відрізняти правду від брехні. Зараз інформаційний простір настільки забруднений фейковою інформацією, що стає практично неможливо відрізнити реальні чи хибні твердження.

Виходить, що людина або вірить всьому, у тому числі і брехні, або не вірить нічому, у тому числі і правді.

В умовах інформаційних війн активність ботів стає набагато більшою, але часто їх доволі просто визначити за певними ознаками:

1. використання загальних за змістом фраз;
2. відсутність певної послідовності та логіки у коментарі;
3. невідповідність темі публікації;
4. розміщення певного коментаря на багатьох ресурсах. Якщо тексти повідомлення абсолютно ідентичні на різних ресурсах - це яскрава ознака дії ботів;
5. публікування коментарів з чіткою періодичністю та велика швидкість їх публікації в ніби-то «живій» розмові.

Часто задачі ботів зводяться до висміювання певних фактів, переведення дискусії у інше русло або переведення розмови «на особистості».

Якщо бот-коментарі ставить реальна людина, то вони часто є більш адаптованими. Однак оскільки за день людина залишає сотні коментарів, вони будуть шаблонними.

У випадку дискусії із ботом, ви не можете нічого і нікому довести, адже Ви просто пишете людині чи машині, мета якої не висловлювати власну думку, а просто виконувати певні задачі, такі як продукувати певні настрої в суспільстві, завалювати пабліки беззмістовними і безглуздими текстами. Це потрібно враховувати, коли читаєте новини чи коментарі. Не варто втягуватись в довжелезні дискусії з усіма особами в Інтернеті.

Протидія методам інформаційної війни в цифровому середовищі потребує комплексу заходів, які включають технічні, правові, культурні та освітні аспекти і може включати наступне:

1) підвищення критичного мислення та медіаграмотності — потрібно забезпечувати доступ до точної та достовірної інформації, сприяння розвитку критичного мислення та здатності аналізувати та перевіряти джерела інформації. Люди повинні навчитись розрізняти хибні новини та фейки від правдивої інформації, а також виявляти та запобігати маніпулюванню.

2) регулювання соціальних мереж та інтернет-платформ — соціальні мережі та інтернет-платформи повинні встановлювати правила для забезпечення достовірності та обґрунтованості інформації, приймати заходи для боротьби з хибними новинами та фейками, а також забезпечувати захист від бот-атак.

3) розвиток кібербезпеки — розробка технологій та алгоритмів, які можуть розпізнавати та блокувати шкідливий контент, використання криптографії та інших методів для захисту конфіденційної інформації. Важливо захищати системи та інформацію від кіберзагроз.

4) контрінформаційні кампанії — створення контенту, що протидіє дезінформації та впливає на аудиторію, допомагаючі їй розуміти ситуацію з більш точної та об'єктивної перспективи.

5) сприяння розбудові громадянського суспільства — важливо підтримувати діалог між різними групами населення та зміцнювати громадську активність. А також приймати закони, що регулюють діяльність в мережі.

6) підтримка незалежних ЗМІ та журналістів — важливо підтримувати незалежність ЗМІ та журналістів, які дотримуються етичних принципів та стандартів журналістики.

Деякі поради з інформаційної гігієни:

1) уникайте повторюваної інформації. Це один з найстаріших механізмів маніпулювання думкою суспільства. Часте повторення інформації записує її у нашу підсвідомість та змушує повірити в неї, якщо, наприклад, в публікації одна й та ж думка повторюється багато разів різними словами.

2) знижуйте інформаційне навантаження. Контролюйте кількість та якість інформації, яку Ви споживаєте. Старайтесь дізнаватись лише необхідне та корисне для вас. Читайте не тільки заголовки. Взагалі, заголовки мають коротко переповідати суть новини, але насправді часто не відповідають змісту публікації.

3) вивчайте різні точки зору на одну проблему. Не довіряйте першій новині та першій думці. Краще – знайдіть декілька авторитетних джерел від різних людей.

4) насторожуйтесь, коли бачите емоційні висновки та особисті думки авторів новин.

5) шукайте, кому вигідно, щоб ви дізнались новину та повірили в неї. Чого хочуть домогтися певними повідомленнями та закликами? Хто від цього виграє?

ВИСНОВОК. Безперервне щоденне спілкування в соціальних мережах, новинному трафіку вносить важливі корективи у сприйняття реальності. Для того щоб не бути ошуканим та мати максимально об’єктивні відомості варто навчитись визначати ознаки інформаційних війн і намагатись не ставати їх жертвами. Крім того, пам’ятайте про важливість комп’ютерної інформаційної безпеки, оскільки зламані акаунти можуть стати інструментом інформаційної війни.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Пода Т. А. Інформаційна війна як стратегія формування політичної свідомості (соціально-філософський аналіз) / Т. А. Пода // Вісн. Нац.авіац. ун-ту. - 2014. - № 1. - С. 67-70.

2. Політанський В.С. Світові моделі та фундаментальні принципи інформаційного суспільства. Науковий вісник Ужгородського національного університету: серія «Право». Випуск 43, том 1. 2017. С.34- 39

3. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. – 144 с.

4. Гібридна війна і журналістика. Проблеми інформаційної безпеки: навчальний посібник / за заг. ред. В. О. Жадька ; ред.-упор. : О. І. Харитоненко, Ю. С. Полтавець. – Київ : Вид-во НПУ імені М. П. Драгоманова, 2018. – 356 с.

19 СТРАТЕГІЇ ВЕДЕННЯ ІНФОРМАЦІЙНОЇ ВІЙНИ

Доповідачі: Дмитро ПЯТНІЧЕНКО, Ілля АНТОНОВ
Керівник: Олена СКОРНЯКОВА
ВСП «Одеський технічний фаховий коледж
Одеського національного технологічного університету»

Пропаганда – це комунікація, яка в основному використовується, щоб вплинути на аудиторію чи переконати її просувати програму, яка може бути необ'єктивною та може вибірково подавати факти, щоб заохотити певний синтез чи сприйняття, або використовувати навантажену мову для створення емоційної, а не раціональної реакції. до інформації, яка надається. Пропаганду можна знайти в широкому спектрі різноманітних контекстів.

Рис.1 – Пропаганда на заголовках видань

Інформаційна війна - це стратегічна боротьба, яка використовується для впливу на громадську думку, створення спотвореної чи маніпулятивної інформації, ідеологічної пропаганди та дезінформації з метою досягнення певних політичних, економічних або військових цілей.

Основна мета інформаційної війни - це зміна уявлень, переконань та поведінки громадськості, зокрема шляхом впливу на засоби масової інформації, соціальні мережі та інші канали комунікації. Її проводять як у мирний період, так і під час конфліктів чи воєн.

Сучасна інформаційна війна в основних своїх принципах є **дезінформація та маніпуляція громадською думкою** , воно штучно створюються та поширюються фейкові новини, спотворена інформація та псевдо експертиза, з метою зміни поглядів та настроїв аудиторії. Також можно зауважити і про **кібератаки** здебільшого вони здійснюються на різні інформаційні системи, включаючи державні структури, військові об'єкти, корпорації, медіа та інші цілі, з метою зламу, крадіжки чутливої інформації, розповсюдження вірусів, блокування роботи систем або спотворення даних.

Соціальні мережі та інтернет за допомогою соціальних мереж, форумів, блогів та інших онлайн-платформ поширюються пропагандистські матеріали, викликаються соціальні конфлікти, проводяться спроби маніпуляції

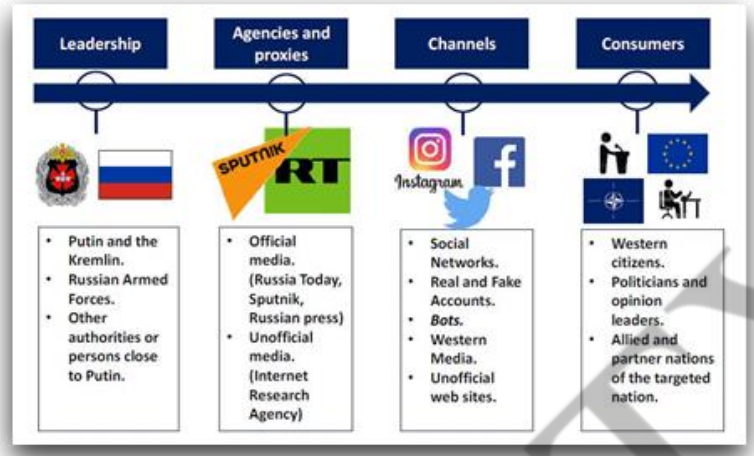


Рис.2 - Види неправдивої інформації

В умовах інформаційної війни боротьба з фейками та дезінформацією стає особливо важливим завданням для всього світу. Сьогодні багато людей отримують інформацію з інтернету, по радіо, телевізору, і багато хто не має достатніх знань і навичок, щоб відрізняти правду від брехні. В країнах створюють спеціальні органи боротьби з дезінформацією. За ці роки потік перекручених, а часто й просто вигаданих новин не лише не зменшився, а навпаки, зріс.

Також в інформаційні війні є ефект фреймінгу. Що це таке?

Ефект обмеження рамка-ми або **фреймінг** (англ. framing effect) — це когнітивне упередження, коли люди реагують на певний вибір по різному залежно від контексту, тобто того, як такий вибір подається — як програш чи виграш.

На даний момент інновації більш досконалих і автономних ІСТ породила нову революцію у військовій справі, яка охоплює використання державами ІСТ як у кіберпросторі, так і на фізичному полі бою для ведення війни проти своїх противників. Три найпоширеніші революції у військовій справі відбулися у вигляді кібератак, автономних роботів і управління зв'язком.

У сфері кіберпростору існує дві основні види зброї: мережево-центрична війна, що позначає інтегроване командування, контроль, зв'язок, комп'ютери, розвідку, спостереження та розвідку. Крім того, атаки в кіберпросторі, ініційовані однією нацією проти іншої країни, мають основну мету отримати інформаційну перевагу над атакованою стороною, що включає в себе порушення або відмову потерпілої сторони в здатності збирати та поширювати інформацію.

Приклади. Російсько-українська війна

✓ Основні статті: Російська інформаційна війна проти України та Дезінформація під час російського вторгнення в Україну у 2022 році

✓ У 2022 році українські сили скористалися недоліками російських комунікацій, дозволивши їм підключатися до українських мереж, підключатися та спілкуватися.

Після цього українські сили підслуховують і відключають російський зв'язок у вирішальній частині розмови.

✓ Намагаючись заручитися підтримкою перед своїм вторгненням в Україну, Росія увічнила наратив, який стверджував, що український уряд вчиняє насильство проти власного російськомовного населення. Публікуючи велику кількість дезінформації в Інтернеті, альтернативний наратив був підхоплений у результатах пошуку, таких як Google News.

Також один із важливих аспектів в інформаційній війні є дезінформація людей.

Дезінформація — це неправдива інформація, навмисно поширена з метою введення людей в оману.Її не слід плутати з дезінформацією, яка є неправдивою інформацією, але не навмисною.

Там, де дезінформація стосується неточностей, які є результатом помилки, дезінформація є навмисною неправдою, оприлюдненою задумом.Дезінформація може бути використана для створення дезінформації, коли відома дезінформація цілеспрямовано та навмисно поширюється.Дезінформація була визначена як «суперницька кампанія, яка використовує численні риторичні стратегії та форми знання — включаючи не лише брехню, але й істину, напівправду та обтяжені цінностями судження — для використання та посилення суперечок, зумовлених ідентичністю.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Тренди дезінформації та пропаганди в соціальних медіа. URL: https://intent.press/publications/medialiteracy/2022/trendi-dezinformaciyi-ta-propagandi-v-socialnih-media-pivdnya-ukrayini-za-5-misyaciv-vijni/
2. Коруц У. Інформаційна війна як інструмент пропаганди війни: правові підстави протидії. Підприємництво, господарство і право. 2020. № 8. С. 334-339.
3. Кост І. Російська пропаганда в Україні як інформаційна складова конфлікту. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3332/3010
4. Малик І. Механізми протидії негативним впливам інформаційної пропаганди. Humanitarian vision. 2015. Vol. 1. Num. 2. С. 47-54. URL: http://nbuv.gov.ua/UJRN/hv_2015_1_2_10

20 БАЗОВІ ПРАВИЛА БЕЗПЕКИ В ЦИФРОВОМУ СЕРЕДОВИЩІ: КІБЕРБЕЗПЕКА ТА МЕРЕЖЕВЕ СПІЛКУВАННЯ

Доповідач: Тетяна КОЖУХАР
Керівник: Ірина ЛИСОВСЬКА
Білгород-Дністровський фаховий коледж природокористування, будівництва та комп'ютерних технологій

Можливість отримати будь-яку інформацію не виходячи з дому: зараз це не фантастика, а реальність. Сучасний світ важко уявити без інтернету, але у кожної функції є свої недоліки. Інтернет сьогодні, це можливість дізнатися щось нове, почати спілкування з незнайомими людьми, але це все веде за собою і погані наслідки, якщо

не вміти виставляти власні кордони в інтернет-спілкуванні, то можно зіткнутися з таким поняттям як КІБЕРБУЛІНГ.

Треба розуміти, що комунікації сьогодні можуть бути не лише в реальному житті, а і онлайн, тому потрібно вміти захищати свої дані і ретельно фільтрувати все те, що викладається в мережу інтернет, тому що особиста безпека повинна бути на першому місці, адже те що потрапило в інтернет, назавжди залишається там, навіть після видалення данних з персональної сторінки в соц. мережі, вони все одно залишаються в базах даних будь якої соціальної мережі.

Мережеве спілкування- це особлива форма комунікації, в процесі якої відбувається взаємодія людей один з одним в мережі Інтернет, та здійснюється шляхом обміну знаковими, або мультимедійними повідомленнями.

З появою мережевого спілкування з'явилося таке поняття як кібербулінг.

Кібербулінг – психологічне насильство в мережі, переслідування з боку однолітків, що проявляється у вигляді знущань, насмішок, залякувань, інших дій, які негативно впливають на психічний стан підлітка.

Проявляється це у вигляді різних знущань, насмішок, залякування, що дуже негативно впливає на психічний стан людини, особливо підлітка. Агресор може застосовувати дві форми агресії: пасивну та активну. Пасивна агресія- це нереалізованість власних емоцій, точніше їх пригнічення. Може проявлятися в мережевому спілкуванні таким чином:

- заборона
- знецінювання інтересів
- ігнорування ваших бажань і емоцій
- образи представленні як гумор.

Активна агресія- це шкідливі дії спричиненні іншим людям, або окремій людині.

Взагалі треба розуміти, що найчастіше з кібербулінгом стикаються саме діти-підлітки. Поступово у них створюються відчуття безвиході, навіть вдома вони постійно відчувають тривогу, вони можуть впадати в депресію. Інформаційна атака може призвести навіть до суїциду.

Люди, які стикаються з кібербулінгом в інтернеті рідко звертаються за допомогою, часто сумніваються, що їх зрозуміють, та бояться заборони користування інтернетом, але необхідно знати, що знущання в мережі карається законодавством, і варто відразу звертатися в правоохоронні органи з наданням доказів.

Приклади ознак кібербулінгу включають:

- поширення брехні про когось або розміщення фотографій, які компрометують когось, у соціальних мережах;
- надсилання повідомлень або погроз, які ображають когось або можуть завдати комусь шкоди, через платформи обміну повідомленнями;
- видання себе за когось іншого і надсилання повідомлень іншим людям від його імені.

Особистий булінг та кібербулінг часто пов'язані між собою. Але кібербулінг залишає цифровий слід – записи, які можуть слугувати доказами, що дозволить зупинити цькування.

У чому різниця між булінгом і жартами?

Усі друзі жартують між собою, але іноді важко сказати, чи хтось просто розважається, чи намагається нашкодити вам, особливо в Інтернеті. Іноді вони насміхаються, але говорять, що це «просто жарти» і пропонують «не сприймати це так серйозно».

Але, якщо ви відчуваєте образу або думаєте, що інші насміхаються з вас, а не веселяться разом з вами, то жарт зайшов занадто далеко. Якщо це продовжується навіть після того, як ви попросили людину зупинитися, і ви досі відчуваєте себе засмученим/ою, то це може бути булінгом.

Коли знущання відбуваються в Інтернеті, це може призвести до небажаної уваги з боку широкого кола людей, включаючи незнайомих людей. Де б це не сталося, якщо вам це неприємно, ви не маєте цього терпіти.

Необхідно також усвідомити, що будь-яка особа заслуговує на повагу: як в Інтернеті, так і в реальному житті.

Є різні можливості захистити себе в інтернеті, наприклад компанія Google дає 5 порад щодо захисту своїх даних:

- Пройдіть перевірку безпеки Google: ...
- Підняти рівень безпеки свого облікового запису за допомогою Програми додаткового захисту ...
- Використовуйте менеджер паролів ...
- Регулярно оновлюйте програмне забезпечення ...
- Якщо загубили телефон, заблокуйте його

Цифрова безпека - це не лише про захист особистих кордонів в інтернет-спілкуванні, але і про вміння захищати свої данні наприклад встановлення авторських прав на власний контент, також треба вміти захищати свої дані, такі як номер телефону, пошту , аккаунти в інтернеті. Дотримання простих правил власної безпеки, допоможе уникнути «зустрічі» з *кібермисливцями.*

Ким є типові інтернет-співрозмовники?

Соціологічні опитування про безпеку дітей-підлітків в інтернет мережі надають такі дані про контакти:

- родичі – 43 %;
- віртуальні друзі – 21%;
- незнайомі люди – 36%.

Однак за великим рахунком віртуальні друзі – теж незнайомці. Таким чином, велику частину свого часу в мережі діти приділяють спілкуванню з сторонніми людьми, діляться своїми переживаннями, секретами, планами.

Кібермисливці – хороші психологи, встановивши контакт на форумі, при обміні миттєвими повідомленнями в чаті, вони досить швидко набувають статусу друзів.

Спочатку входять в довіру, оточуючи турботою і розумінням проблем, вислуховують, підтримують. Після цього «друг» поступово вносить до розмови нотки сексуальності, відбувається обмін фото, демонстрація матеріалів еротичного характеру.

Мета кібермисливця – особиста зустріч.

В Україні є офіційний веб-сайт Міністерства цифрової трансформації України, на цьому сайті можна знайти інформацію про те як захистити свої данні і себе в цифровому просторі.

Українці все частіше користуються інтернетом — це зручно та швидко, але водночас не слід забувати про особисту безпеку в інтернеті.

Мінцифри дає 5 основних порад, як себе убезпечити:

1. Не надавайте своїх даних. Нікому. В інтернеті чимало заманливих пропозицій: «Саме ваш номер може виграти приз». Бачили таке? Або вам телефонували чи надсилали смс-повідомлення з подібним змістом. Не ведіться, у більшості — це шахраї. Вони попросять у вас пароль від банківської картки, номер телефону або ще щось. Найкращим варіантом буде припинити розмову, навіть якщо пропозиція буде дуже заманлива.
2. Перевіряйте інформацію. Не поширюйте новини із занадто гучними заголовками. Можливо, це фейк. Перевірте: спитайте в знайомих, які розбираються в темі, або перегляньте новинну стрічку інших сайтів. Також, не менш важливо - перевіряти інформацію, якщо вас просять пожертвувати гроші на якусь операцію чи зробити репост посту із новиною подібного змісту. Пам’ятайте, шахраї часто видають себе за благодійників.
3. Захищайте паролі. Щодня користуєтесь Facebook або сплачуєте в інтернеті? Благаємо, тільки не кажіть, що використовуєте один пароль усюди. Міняйте паролі з певною частотою, радимо використовувати для цього спеціальні менеджери паролів (приміром, 1password, LastPass або KeePass). Зберігайте паролі в надійному місці, а краще — запам‘ятовуйте.
4. Використовуйте двохфакторну автентифікацію. Google, Facebook, Instagram постійно пропонує налаштувати подвійне підтвердження входу? Погоджуйтеся! Це не страшно: окрім паролю, вам зателефонують або надішлють код, так ваші дані в соцмережах будуть ще більш убезпечені. До речі, завершуйте сеанс одразу після виходу із соцмережі.
5. Користуйтеся офіційними програмами. Перевіряйте програми, які завантажуєте - радимо з офіційних джерел. Офіційні програми проходять перевірку на наявність фішингу - несанкціонованого збору та передачі даних. Тож, користуючись саме офіційним програмним забезпеченням, ви будете певні, що не заразите комп’ютер чи смартфон якимось вірусом. Також радимо використовувати лише перевірені мережі інтернет-з’єднання.

Україна є першою країною за розвитком цифравої галузі.

Прикладом є мобільний застосунок «ДІЯ», «ДАР».

Висновок: Безпека в інтернеті це дуже важливо, тому треба дотримуватися всіх правил і стежити за тим, що ти публікуєш в інтернеті. І якщо від коронавірусу рятує маска та миття рук із милом, то від цифрового вірусу — розумне користування і спеціальний застосунок. Не полінуйтеся, про всяк випадок, встановити антивірус. І якщо ви колись стикались с таким поняттям, не треба мовчати і боятися, говоріть про такі випадки, тому що це важливо і потрібно. Лише своїм прикладом ви, можливо, допоможете комусь зрозуміти, що він перебуває у токсичних, деструктивних відносинах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1.Барліт А.Ю. Форми і методи подолання (мінімізації) соціально-педагогічної та психологічної проблеми булінгу в освітньому середовищі / А.Ю.Барліт, О.О.Барліт // Горизонти освіти. – 2012. – №2. – С. 44-46.
2. Безпальча Р. Шляхи мирного розв'язання конфліктів у школі, 2012. Режим доступу: https://issuu.com/uccg/docs/bezp_shlyakhy_mrk
3. Блог Людмили Петрановської, педагога, психолога і публіциста.
4. Булінг – важлива проблема для дітей в Україні. ЮНІСЕФ розпочинає кампанію проти булінгу.
5. Визначення психічного здоров'я та рівнів психологічної адаптації людини. Критерії здоров'я ВООЗ.
6. Воронцова Е. Програма «Профілактика та подолання булінгу у закладах освіти»
7. Вчимося бути толерантними. Тренінговий курс для молоді, Донецьк, 2008. Режим доступу: http://cent.dn.ua/docs/trening_tolerance.pdf
8.Інтернет, в якому ми живемо. Режим доступу: http://kyrsu2018.blogspot.com/p/blogpage_58.html
9. Кацалап В.В., Савкова І.О .Програма тренінгових занять «СТОП- Булінг» орієнтована на профілактику насилля в шкільному середовищі.
10. Коли вашу дитину цькують. Посібник для батьків.
11. Коментар до Кримінального кодексу України.
12. Комплект освітніх програм «Вирішення конфліктів мирним шляхом. Базові навички медіації». – К. – 2018. – 140 с.
13.Що українці знають і думають про права людини: загальнонаціональне дослідження / [І. Бекешкіна, Т.Печончик, В.Яворський та ін.]; під заг. ред. Т. Печончик. – Київ, 2017. –308 с.
14.Як запобігти булінгу? Поради та вправи на емпатію. Режим доступу: https://naurok.com.ua/post/yak-zapobigti-bulingu-poradi-ta-vpravi-dlya-rozvitku- empaty