

Кібербезпека та/або права людини

№26, 13 липня 2017



Лілія Олексюк ,
голова

Всеукраїнської асоціації "Інформаційна безпека та інформаційні технології" ("ВАІБІТ")

Головна стаття

Закон про кібербезпеку та стратегія кібербезпеки України

Компетентна думка

Кібербезпека банків, або Коли вже недостатньо залізних дверей

Хмарні технології та кібербезпека

Сучасні загрози інформаційній безпеці особи, суспільства та держави: криміналістичний погляд

За інформацією ЄК, лише 12 % європейських користувачів мережі Інтернет почувають себе абсолютно безпечно, здійснюючи онлайн-транзакції. Такі загрози, як шкідливе програмне забезпечення й інтернет-шахрайство, позбавляють приросту кількості споживачів і зводять нанівець зусилля, спрямовані на просування цифрової економіки.

Щодо українських споживачів, то станом на лютий 2016 року в Україні до мережі Інтернет підключено 63 % домогосподарств. Регулярно, тобто раз на місяць, користуються мережею Інтернет 62 % сімей. За даними Світового банку, проникнення мережі Інтернет в Україні щорічно підвищується в середньому на 5 %. Тобто проблеми, пов'язані з довірою у мережі й онлайн-транзакціями, зростатимуть із року в рік.

Півстоліття тому вперше застосовували термін "інформаційна безпека" разом із термінами "інформаційне суспільство", "економіка знань" і пізніше "цифрова економіка" тощо. Тепер все частіше можна почути "кібербезпека", "кібервійна", "кібернапад", "кіберзлочин". Спробуймо для початку розібратись, що це таке.

Інформаційна безпека – збереження конфіденційності, цілісності та доступності інформації. Також повинні враховуватися достовірність, відповідальність, неможливість заперечення і надійність (ISO/IEC 17799:2005). Тобто це дії для убезпечення саме інформації від громадян і засобів, а не навпаки – громадян убезпечувати від інформації, про що іноді можна прочитати на просторах Інтернету.



Термін "кібербезпека" зазвичай стосується корпоративного управління, менеджменту та надання впевненості щодо безпеки, які виходять за межі того, що ми розуміємо як "інформаційну безпеку". Кібербезпека зосереджується на особливих формах складних атак й охоплює їх технічний і соціальний аспекти.

Оскільки існує багато визначень кібербезпеки, цей термін часто розуміють неправильно.

Офіційне визначення ЄС таке:

"Кібербезпека зазвичай стосується заходів і дій, спрямованих на захист кіберпростору в

цивільній і військовій сферах від загроз, які можуть завдати шкоди взаємозалежним мережам та інформаційній інфраструктурі або є пов'язаними з ними. Кібербезпека спрямована на збереження доступності та цілісності мереж та інфраструктури, а також конфіденційності інформації, яка міститься в них."¹

¹ Європейська комісія, Спільне звернення до Європейського парламенту, Ради, Європейського соціально-економічного комітету та Комітету регіонів – Стратегія ЄС із кібербезпеки: відкритий, надійний і безпечний кіберпростір, Брюссель, 2 липня 2013 р., с. 3:

http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667.

ISACA дає таке визначення кібербезпеки:

*"Захист інформаційних активів шляхом боротьби із загрозами безпеці інформації, яка обробляється, зберігається та передається за допомогою інформаційних систем, що взаємодіють за допомогою мереж."*²

² ISACA, Глосарій з кібербезпеки, 2014 р.:

http://www.isaca.org/Knowledge-Center/Documents/Glossary/Cybersecurity_Fundamentals_glossary.pdf.

У своїй публікації *Трансформація кібербезпеки* ISACA описує кібербезпеку детальніше:

*"... Кібербезпека охоплює все, що захищає організації та фізичних осіб від умисних атак, порушень, інцидентів та їх наслідків. На практиці кібербезпека насамперед стосується тих типів атак, порушень та інцидентів, які є цільовими, високотехнологічними та складними у виявленні чи управлінні. ... Кібербезпека зосереджується на так званих складних спрямованих постійних загрозах (APT)³, кібервійнах та їх впливі на організації та людей."*⁴

³ APT (advanced persistent threats) – спрямовані постійні загрози.

⁴ ISACA, *Трансформація кібербезпеки*, США, 2013 р., с. 11:

www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Transforming-Cybersecurity-Using-COBIT-5.aspx



Таким чином, інформаційна безпека має нижчий рівень, ніж кібербезпека, та відрізняється масштабом, мотивами, можливостями і методами атак.

Поглянемо на PESTLE-аналіз – це детальний аналіз різних аспектів підприємства, а саме політичного (Political), економічного (Economic), соціального (Social), технологічного (Technical), юридичного (Legal) та навколишнього середовища (Environmental), підготовлений експертами ISACA.

Фокус інформаційної безпеки та кібербезпеки (PESTLE-аналіз)



Рис. 1. PESTLE-аналіз⁵

⁵ Впровадження європейської кібербезпеки: загальний огляд www.isaca.org/cyber



Кібербезпека, на відміну від інформаційної безпеки, забезпечується не тільки безпосередньо організацією, що захищається, а й іншими постачальниками послуг (телекомунікаційних, сервісних, хмарних тощо).

У більшості випадків йдеться про колективну безпеку учасників діяльності в мережі Інтернет. Тобто велику кількість користувачів, яких не може контролювати одна організація в прямому сенсі цього слова, але які мають доступ до певних колективних ресурсів чи право користування публічними сервісами.

Провайдер сервісів має у цьому випадку велику владу й технічну можливість керувати інформацією та транзитом потоку даних (інтернет-трафіку) через мережі, якими він оперує. Постачальники послуг доступу в Інтернет можуть брати участь в управлінні інтернет-трафіком для конкретних законних цілей, наприклад, для збереження цілісності та безпеки мережі. Вони можуть також вжити заходів, щоб запобігти доступу чи розповсюдженню незаконного або шкідливого вмісту, наприклад, через системи саморегулювання у співпраці з державними органами. Проте інші втручання до інтернет-трафіку можуть вплинути на якість послуг, що надаються інтернет-користувачам, і призвести до блокування, дискримінації або пріоритетності конкретних видів контенту, додатків і послуг. Більше того, деякі з методів, що використовуються в контексті управління доступом, або моніторинг повідомлень можуть підірвати довіру користувачів до мережі Інтернет.

Європейська спільнота для реалізації прав людини в мережі Інтернет (з 2013 року право на доступ до мережі Інтернет є базовим правом людини) ухвалила Рекомендацію CM/Rec (2016) 1 Комітету Міністрів державам-членам із захисту й заохочення права на свободу вираження поглядів та право на приватне життя відносно мережевого нейтралітету (ухвалена Комітетом

Міністрів 13 січня 2016 року на 1244 засіданні заступників міністрів) і [Рекомендацію CM/Rec \(2016\) 5 Комітету Міністрів держав-членів щодо Інтернет-свободи](#) (ухвалена Комітетом Міністрів 13 квітня 2016 року на 1253 засіданні заступників міністрів), визнаючи ризики, пов'язані із регулюванням доступу у мережі Інтернет та можливостями провайдерів сервісів.

Як зазначено в [Рекомендації Rec \(2016\) 5](#), механізми управління Інтернетом, на національному, регіональному або глобальному рівні, мають ґрунтуватися на розумінні Інтернет-свободи. Держави мають права й обов'язки щодо міжнародної політики, пов'язаної з Інтернетом. При здійсненні своїх суверенних прав держави повинні відповідно до норм міжнародного права утримуватися від будь-яких дій, які можуть прямо або побічно завдати шкоди фізичним чи юридичним особам всередині або за межами їх юрисдикції. Будь-яке національне рішення або дія на обмеження прав людини та основних прав в Інтернеті повинні відповідати міжнародним зобов'язанням і, зокрема, базуватися на законі. Дотримуватися повною мірою принципів пропорційності та гарантувати доступ до засобів правового захисту, а також право бути почутим і звертатися із забезпеченням належних гарантій процесу повинні бути важливими в демократичному суспільстві.

ЄС, розуміючи всі можливі наслідки технічного та технологічного регулювання забезпечення доступу до мережі Інтернет, наголошує на необхідності регулювання на рівні закону обмежень, потрібних для забезпечення колективної безпеки. Це стосується і обов'язку держави захищати людей від кіберзлочинів за допомогою ефективного кримінального правосуддя або інших заходів. У разі коли такі заходи містять ризик, пов'язаний з правом на приватне життя, правом на свободу вираження або правом на свободу мирних зборів і асоціацій, вони підлягають умовам і гарантіям проти зловживань. Ці заходи повинні відповідати [статтям 8, 10 і 11 Конвенції про захист прав людини і основоположних свобод](#). Причому вони повинні бути встановлені на рівні закону. Закон має бути доступним, точним, зрозумілим; ставити законну мету; необхідним і пропорційним у демократичному суспільстві й забезпечувати ефективні засоби правового захисту.

Україна приєдналась до [Конвенції про захист прав людини і основоположних свобод](#) вже досить давно, а [Угода з ЄС про асоціацію](#) набрала чинності (тимчасове застосування) кілька років тому. Отже, держава Україна визначилась, що у сфері прав людини дотримуватиметься демократичної європейської моделі державного регулювання (обмеження) прав людини, зокрема в мережі Інтернет.

Чи відповідає на сьогодні законодавче регулювання європейській моделі? Частково так. Що стосується телекомунікаційних послуг – так, щодо кібербезпеки – ні.

У 2006 році Україна приєдналась до [Конвенції про кіберзлочинність](#), зокрема визнала "необхідність співробітництва між Державами і приватними підприємствами для боротьби з кіберзлочинністю і необхідність захисту законних інтересів під час використання та розвитку інформаційних технологій".

І в розвиток цієї [Конвенції](#) Україні необхідно було розробити механізми співпраці держави і приватного сектору в частині забезпечення кібербезпеки (далі – заходи кібербезпеки), але зберігаючи "належний баланс між правоохоронними інтересами і повагою до основних прав людини". Також слід було переглянути кримінальне законодавство України в частині розробки процедурних питань з метою отримання належних доказів у злочинах з використанням інформаційно-телекомунікаційних мереж і технологій, формулювання самого складу злочину в цифровому світі. Одним із завдань було забезпечення як спеціалістами, які зможуть без лому і виїмки серверів розслідувати злочини, так і спеціалістами, які адекватно зможуть встановити відповідні факти в суді.

Як ви розумієте, не все так добре за 11 років після приєднання до [Конвенції про кіберзлочинність](#). Наразі існує лише [Стратегія кібербезпеки України](#), затверджена [Указом Президента України](#) 1,5 роки тому, та [законопроект 2126а](#), що подавався на розгляд Верховної Ради України і був переданий на повторне друге читання.

Аналізуючи [законопроект № 2126а](#) на предмет наявності заходів із кібербезпеки, зауважимо, що жодного із перерахованих вище в ньому немає. Внесення змін до кримінального та процесуального законодавства, встановлення механізмів державно-приватного партнерства також відсутні. Так само відсутнє і розшифрування (тлумачення), як досягається додержання принципів кібербезпеки. До речі, кібербезпека і кіберзахист в українській варіації – дві різні речі, як кажуть в Одесі. В інших країнах під кібербезпекою якраз і розуміють заходи із захисту, про що йшлося вище. На нашу думку, прийняття зазначеного закону не забезпечить реалізацію мети, яка описана в його преамбулі: в законопроекті немає статей на реалізацію принципів забезпечення кібербезпеки, а визначення об'єктів критичної інфраструктури та всіх пов'язаних із ними питань взагалі віднесено на інший рівень – постанов і розпоряджень Кабміну.

До речі, термін "кібербезпека" із законопроекту має цікаву деталь: "кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі";".

Закон України "[Про основи національної безпеки України](#)" визначає національну безпеку так:

"національна безпека – захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам у сферах правоохоронної діяльності, боротьби з корупцією, прикордонної діяльності та оборони, міграційної політики, охорони здоров'я, освіти та науки, науково-технічної та інноваційної політики, культурного розвитку населення, забезпечення свободи слова та інформаційної безпеки, соціальної політики та пенсійного забезпечення, житлово-комунального господарства, ринку фінансових послуг, захисту прав власності, фондових ринків і обігу цінних паперів, податково-бюджетної та митної політики, торгівлі та підприємницької діяльності, ринку банківських послуг, інвестиційної політики, ревізійної діяльності, монетарної та валютної політики, захисту інформації, ліцензування, промисловості та сільського господарства, транспорту та зв'язку, інформаційних технологій, енергетики та енергозбереження, функціонування природних монополій, використання надр, земельних та водних ресурсів, корисних копалин, захисту екології і навколишнього природного середовища та інших сферах державного управління при виникненні негативних тенденцій до створення потенційних або реальних загроз національним інтересам".

Нічого не здивувало? Так от кібербезпека має забезпечити своєчасне виявлення, запобігання і нейтралізацію загроз національним інтересам.

Однією із загроз ([стаття 7 Закону України "Про основи національної безпеки України"](#)) є

"в інформаційній сфері:

прояви обмеження свободи слова та доступу до публічної інформації;

поширення засобами масової інформації культу насильства, жорстокості, порнографії;

комп'ютерна злочинність та комп'ютерний тероризм;

розголошення інформації, яка становить державну таємницю, або іншої інформації з обмеженим доступом, спрямованої на задоволення потреб і забезпечення захисту національних інтересів суспільства і держави;

намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації".

Здається, трохи перемудрували.

Про права та обмеження прав у **законопроекті** не йдеться, але цікавий юридичний виверт "забезпечення кібербезпеки в Україні ґрунтується на принципах: 1) верховенства права, законності, поваги до **прав людини і основоположних свобод та їх захисту у порядку, визначеному законом**" доводить протилежне: чи вже існує якийсь закон, де описаний порядок захисту прав і свобод, чи його буде ще розроблено – відповіді законопроект не дає.

Якщо мали на увазі законодавчі акти про захист персональних даних чи про доступ до публічної інформації, чи про забезпечення доступу до мережі Інтернет – то можна було б і послатись на них. Взагалі, питань більше, ніж відповідей. Добре, що є можливість переглянути законопроект (закладені до нього норми) критично.

ВИСНОВОК:

У цій статті не ставилась мета детально розглянути порушення конкретних прав і свобод у зв'язку із заходами для забезпечення кібербезпеки, лише основні поняття, принципи та їх сутність для розуміння того, що співіснування прав і свобод можливе. Безпека створюється не в обмін на права і свободи, а лише разом із ними. Ніщо не коштує так багато, як свобода. І обмеження (а не заборони!!!) задля колективної безпеки можна і потрібно впроваджувати, але за однієї умови – закон має бути доступним, точним, зрозумілим; ставити законну мету; необхідним і пропорційним у демократичному суспільстві й забезпечувати ефективні засоби правового захисту.

Закон і тільки закон має бути!

© ТОВ "Інформаційно-аналітичний центр "ЛІГА", 2017

© ТОВ "ЛІГА ЗАКОН", 2017