рідко останні вчиняють дії, направлені на маскування провокацій зі свого боку, що при розгляді кримінального провадження призводить до ускладнення побудови певної правової позиції захисника. І хоч на законодавчому рівні задекларована змагальність сторін, насправді нею і не пахне», – розповідає суддя Апеляційного суду Київської області **Олег Володимирович Ігнатюк.**

Суддя зазначив, що при перегляді справ про злочини, вчинені внаслідок провокації правоохоронними органами, слід звернути увагу на **чотири фундаментальні рішення ЄСПЛ,** «Тейшейро де Кастро проти Португалії», «Раманаускас проти Литви», «Баннікова проти Російської Федерації», «Вєсєлов та інші проти Російської Федерації».

У справі «Тейшейро де Кастро проти Португалії» винесено вирок засудженому за перевезення наркотиків, основаному на показаннях двох поліцейських, котрі спровокували його до здійснення злочину.

Суддя Ігнатюк провів межу між неналежними діями працівників поліції в ході контрольованої закупки та діями звичайних агентів, які діють під прикриттям з метою отримання доказів щодо вчинення особою злочину без активного підбурювання до його вчинення. Заборона підбурювання поширюється як на працівників поліції, так і на осіб, які діють за їх вказівкою. Перед проведенням контролю за вчиненням злочину працівники правоохоронних органів повинні: володіти достатнім обсягом інформації про причетність особи до вчинення злочину; вступати у злочин лише на етапі його підготовки або вчинення; поведінка агентів повинна бути пасивною.

Про активну поведінку, яку може бути розцінено як провокацію, може свідчити самостійне звернення до особи, повторні пропозиції після відмови особи, наполягання, що пояснюється в рішенні ЄСПЛ у справі **«Раманаускас проти Литви»**. Справа полягала у тому, що заявник скаржився на використання в кримінальній справі доказів, отриманих унаслідок підбурювання з боку поліції, що порушило його право на справедливий судовий розгляд справи щодо нього.

У справі **«Баннікова проти Російської Федерації»** (проведення співробітниками органів федеральної служби безпеки оперативно-розшукового заходу у вигляді перевірочної закупки, котре призвело до скоєння громадянкою злочину, пов'язаного із незаконним збутом наркотичної речовини), заявниця у своїй скарзі в ЄСПЛ стверджувала, що її визнали винною у вчиненні злочину, спровокованого правоохоронними органами через агента-провокатора й що вона не вчинила би злочину без їхнього втручання.

Європейський Суд з огляду на справи, ухвалив, що використання особливих методів ведення слідства – зокрема, агентурних методів, – не може саме по собі порушити право на справедливий розгляд. Ризик підбурювання з боку співробітників міліції, викликаний зазначеними методами, означає, що їхнє використання має бути суворо регламентованим. А в частині розгляду заяви про провокаційні дії, спрямовані на спонукання вчинення злочину з метою його викриття, Європейський Суд, звертає увагу на те, чи був би вчинений злочин без втручання органів влади.

На основі розглянутих метеріалів усіх справ, **Європейський Суд** визнав, що *підбурювання* з боку поліції має місце лише там, де задіяними особами – є посадові *особи, співробітники служб безпеки або особи, що діють за їх розпорядженням* – не обмежувані фактично необхідною пасивною слідчою діяльністю, а такі, що здійснюють такий вплив на особу, як підбурювання до вчинення злочину, що в іншому випадку не був би вчинений, з метою забезпечити докази й почати карне переслідування.

Ярослава Комаренко,
журналіст "Економіка. Фінанси. Право"

КІБЕРАТАКА В УКРАЇНІ

Кібератака на український бізнес

10 липня 2017 року Торгово-промислова палата України зібрала фахівців у сфері бізнесу для обговорення «гарячої» теми – наймасштабнішої кібератаки на українські підприємства.

Обговорення розпочав Президент ТППУ Геннадій Чижиков, і своїми коментарем щодо теми висловив думку більшості присутніх: «Наразі ми маємо більше питань, ніж відповідей». Це дійсно так, оскільки системи захисту українських підприємств виявились аж надто вразливими і піддались нападу хакерів, що спричинило затримку робочих процесів установ.

Також окреме місце в обговоренні зайняло питання щодо форс-мажору: чи є кібератака форс-мажором та як це довести?

«У переліку обставин непереборної сили кібератака досі не значилась – тому нам довелось гідно приймати виклик і шукати правильне рішення в рамках закону. Починаючи з 27 червня 2017 р. юристи ТПП України надали вже понад 1000 консультацій на запити щодо підтвердження форс-мажорних обставин у зв'язку із кібератакою. Ми й досі щодня продовжуємо отримувати понад 100 запитів на консультації. Торгово-промислова палата свідомо взяла на себе роль «голосу» бізнесу до влади і запрошує всіх об'єднати зусилля в пошуку найефективніших рішень захисту кожної окремої компанії зокрема та держави в цілому», – зазначив Чижиков.

Щодо форс-мажорних обставин позицію ТППУ висловила Алла Нестеренко – директор Дирекції правового забезпечення діяльності ТПП України:

«Торгово-промислова палата України зможе засвідчувати факти форс-мажорних обставин тільки на підставі документів, отриманих від Кіберполіції. На наш погляд, це має бути довідка або витяг про відкриття кримінального провадження. Для можливості оперативного реагування на численні звернення та використання достовірної інформації при засвідченні форс-мажорних обставин стосовно ситуації навколо кібератаки, ТПП України звернулася до Кіберполіції з проханням надати офіційне підтвердження термінів (дат початку та закінчення) здій-

нення кібератаки на корпоративні та мережі органів влади, а також роз'яснення, що є юридичною підставою, підтверджуючою здійснення кібератаки на мережі суб'єктів господарювання».

Занепокоєння ситуацією, що склалась висловив і керівник проектів та програм Департаменту безпеки Національного Банку України Антон Кудін:«Причина швидкого розповсюдження та вдалої атаки – невідповідність систем захисту. Нацбанк зробив висновки і буде підвищувати вимоги до кібербезпеки всередині установи за двома напрямками. По-перше, ми плануємо створити центр реагування на комп'ютерні інциденти, а по-друге, – розробимо нові правила для забезпечення безпеки інформації у банківській системі». Також він повідомив фахівців, що дана атака не була одно актовою дією, а є системною стратегією. За його словами, та кібератака, котру ми обговорюємо, розпочалась ще на початку 2017 року і зараз в модифікованому вигляді нанесла удар на завчасно виявлені слабкі місця.

Вчений секретар Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Олександр Корнейко повідомив, що кібератаки розпочались ще задовго до 2017 р.. На його думку, перші схожі атаки мають початок з виборів Президента України у 2015 р. і ситуація, що склалась нині, – «показова вистава», адже при можливостях вірусу постраждали саме бізнес-структури, що означає, що метою не було отримати котрусь конфіденційну чи таємну інформацію.

«В Україні нині достатньо підготовлених кадрів та є накопичений досвід – фахівців із кіберзахисту готує понад 30 вітчизняних вищих навчальних закладів. Нам варто розвивати державно-приватне партнерство, адже поки що бізнес та держава знаходяться по різні сторони фронту, а треба об'єднувати зусилля і допомагати один одному. Ми переможемо, бо правда за нами», – додав Корнейко.

Найбільше питань у фахівців було до Геннадія Дубка – заступника начальника Департаменту кіберполіції Національної поліції України, адже найбільшою складністю для підприємців виявилось звичайне фіксування інфікування комп'ютерних систем працівниками кіберполіції.

«Працівники кіберполіції є у кожному регіоні України – їх можна викликати на підприємство, що постраждало для фіксування факту кібератаки. На сьогоднішній день в департамент кіберполіції звернулися близько 3 тисяч осіб. З офіційними заявами – вже понад 1,5 тисячі. Близько 200 заяв подали підприємства державного сектора, всі інші – приватні підприємці. Нині правоохоронними органами ведеться розслідування: ми шукаємо причетних до організації кібератаки», – повідомив Дубок. Також за словами службовця, департамент спрямував усі сили на розробку нової системи обслуговування населення у подібних ситуаціях.

До обговорення долучились і представники найбільших компаній, котрі зазнали втручання у роботу електронних систем.

Про особливості робочого процесу під час масштабної кібератаки розповів голова Авіаційного комітету при ТПП України, перший заступник генерального директора Міжнародного аеропорту «Бориспіль» Євген Дихне: «Після кібератаки всі підприємства змушені жити по-новому, а це значить – витрачати багато грошей на безпеку та вибудовувати систему управління підприємства по-іншому. «Бориспіль» працює по-новому з січня цього року. До кібератак на підприємстві готувалися ще з грудня, тому напад вдалося оперативно відбити. Аеропорт не припинив свою роботу і кілька днів працював не використовуючи дата центр. Крім електронних систем надважливим є й людський фактор – пильність персоналу. Також треба підвищувати рівень корпоративної культури. Постраждалі від вірусу підприємства можуть за лічені години «підняти» свою роботу, якщо попередньо побудувати альтернативну робочу мережу. Мета – не вберегтися від усіх можливих кібератак, а побудувати менш вразливу мережу та забезпечити її швидке відновлення після локальних зупинок».

Рішення підприємства про перехід на «ручний режим» роботи було єдиновірним і це допомогло уникнути більшого ураження і, відповідно, більш негативних наслідків. На думку Дихне, завжди треба бути готовим до найгіршого сценарію розвитку подій, але ще важливіше – завчасно розробити план дій щодо подолання проблеми.

За словами заступника голови правління «Приватбанку» Олександра Дрелінга, через кілька тижнів в Україні прогнозують нову хвилю кібератак, націлену на комп'ютерні мережі, що працюють на операційній системі Linux, а це 70 % ринку: і банківського, і державного. Щоб мінімізувати наслідки нових атак і по-максимуму захистити від них країну і підприємства, потрібно підготувати централізовані, загальні рекомендації не тільки банкам, але й іншим компаніям, щоб вони були готові до другої хвилі.

За деталями дискусії, фахівці дішли висновку, що потрібно по-іншому підійти до питання оцінки загроз, необхідно переходити на поведінковий аналіз, а не реагувати на готові проблеми.

Найбільш яскравий коментар з цього приводу надав партнер юридичної фірми Axon Parters Дмитро Гадомський:

«Замість боротьби з наслідками кібератаки («мочити» M.E. Doc, наполягати на форс-мажорі тощо) компаніям потрібно «зафіксувати збитки». А зекономлені на цьому сили, час і гроші направити на підготовку до наступних атак. Як мінімум, варто прочитати EULA вашого вендора, щоб уже з самого початку знати, що жоден вендор не несе відповідальності за свій софт».

Директор Інституту комп'ютерних інформаційних технологій Національного авіаційного університет Олександр Юдін вважає за необхідність сформувати робочу групу з фірм довірчої зони. Створення команди професіоналів, які поєднані однієї ідеєю полегшить реагування на кіберзагрози.

«Мушу констатувати той факт, що ми маємо справу з кібервійною. Бізнес повинен бути готовим до того, що кібератаки триватимуть. Під час дискусії ми зробили зріз проблеми, щоб на основі почутого виробити ефективний механізм захисту вітчизняних підприємців та підготовки до нової хвилі атак», –

сказав голова Комітету з електронних комунікацій при ТПП України Володимир Коляденко.

В результаті обговорення можна чітко стверджувати, що дана кібератака має послугувати Україні як навчальна тривога, відштовхуючись від якої треба прогнозувати всі можливі подальші сценарії, і головне – бути до них готовими.

Відкрито кримінальне провадження

27 червня внаслідок несанкціонованої кібератаки постраждали тисячі державних та приватних установ. Директор департаменту комунікацій Національної поліції України Ярослав Тракало повідомив про відкриття 23 кримінальних проваджень за ст. 361 Кримінального Кодексу Україні – втручання в роботу електрообчислювальних приладів, або комп'ютерних мереж.

За його словами, протягом доби до Департаменту кіберполіції НПУ надійшло понад тисячу повідомлень про незаконне втручання в роботу комп'ютерних мереж.

За даними інформаційного агентства UNN (http://www.unn.com.ua), хакерських атак зазнали державні підприємства та установи, а саме Нацбанк, Ощадбанк, ПриватБанк, Укрпошта, Укренерго, Укргазвидобування, а також міжнародні аеропорти "Бориспіль" та "Київ".

Ситуацію прокоментував Прем'єр-міністр України – Володимир Гросйман: "Безпрецедентна атака, але наші ІТ-шники роблять свою роботу і захищають критичну інфраструктуру. Важливі системи не постраждали. Атака буде відбита, а зловмисники — виявлені".

29 червня в.о. голови Національного банку України Яків Смолій, повідомив про відновлення роботи частини вражених структур з посиланням на прес-службу НБУ, зазначає UNN.

Зміни до Податкового кодексу у зв'язку із кібератакою в Україні

Міністерство фінансів України ініціювало внесення змін до Податкового кодексу, що дозволять не накладати штрафних санкцій до платників податків за несвоєчасну реєстрацію податкових накладних у зв'язку з кібератакою.

Хакерський напад на ряд установ України спричинив затримку абсолютно всіх фінансових та інформаційних процесів, починаючи від припинення роботи банківських терміналів до порушення роботи державних органів.

Прецедент не оминув і Державну фіскальну службу України, яка мала накладати штрафи на платників податків за несвоєчасне подання податкової звітності, тобто накладних, що були виписані в період з 1 до 15 червня 2017 р..

Очевидно, що така проблема виникла не з вини платників податків, а через вірус. Та на жаль, чинний Податковий кодекс не передбачає такої ситуації для незастосування санкцій.

Саме тому Мінфін спільно з ДФС вирішили внести корективи в дану норму законодавства і 4 липня на засіданні Кабінету Міністрів України було схвалено Проект Закону України "Про внесення змін до Податкового кодексу України щодо реєстрації податкових накладних та/або розрахунків коригування до податкових накладних у Єдиному реєстрі податкових накладних".

За даними Мінфіну, законопроект дозволить не застосовувати до платників податків штрафні санкції за несвоєчасну реєстрацію податкових накладних, що були видані з 01.06 до 15.06, і котрі будуть зареєстровані до 15.07.2017.

Проект вже схвалено в КМУ і наступним кроком були його подання на розгляд Верховної Ради України.

Суть запропонованих Мінфіном та ДФС змін полягають у тому, що до платників податків, котрі зіткнулись з проблемою реєстрації податкових накладних через форс-мажорні обставини – а саме кібератаку, котру раніше не було визнано такою в нормативному акті, не можуть бути застосовані штрафні санкції за порушення граничних строків реєстрації податкових накладних у Єдиному реєстрі податкових накладних, за умови реєстрації даних накладних до 15 липня 2017 р..

Оскільки проект ще не надійшов на розгляд ВРУ, у Мінфіні очікують коментарів від нардепів та, безпосередньо, його схвалення, оскільки проект мінімізує негативні наслідки вірусу для бізнесу України, – повідомляє Міністр фінансів України Олександр Данилюк.

З текстом законопроекту можна ознайомитись на офіційному сайті Міністерства фінансів України [*https://www.minfin.gov.ua*].

Ярослава Комаренко,
журналіст "Економіка. Фінанси. Право"

АУДИТОРИ УКРАЇНИ БУРХЛИВО ОБГОВОРЮЮТЬ НОВИЙ ЗАКОНОПРОЕКТ: "ПІДВОДНІ КАМЕНІ" ПРОПОНОВАНИХ НОРМ

Ініційований **Міністерством фінансів України** ***законопроект №6016 «Про аудит фінансової звітності та аудиторську діяльність»*** має бути прийнятим до кінця 2017 р.. Такий термін визначено не дарма, адже прийняттям закону реалізуються умови **Угоди України з Європейським Союзом**, що була підписана у 2014 р..

Відповідно до **Угоди про Асоціацію з ЄС**, Україна зобов'язується поступово *наблизити своє законодавство до законодавства ЄС*, зокрема, вимог **Директиви 2006/43/ЄС Європейського Парламенту** та **Ради про обов'язковий аудит річної звітності консолідованої звітності**, зі змінами, внесеними **Директивою 2014/56/ЄС** Європейського Парламенту та Ради.

Термін виконання чітко зазначений: зміни мають бути впроваджені *протягом трьох років з дати набрання чинності цієї Угоди*.