УДК 347.965
DOI https://doi.org/10.51989/NUL.2021.5.15

КІБЕРБЕЗПЕКА АДВОКАТСЬКОЇ ДІЯЛЬНОСТІ В УКРАЇНІ ТА СВІТІ

Діордіца Ігор Володимирович,
доктор юридичних наук, доцент,
професор кафедри приватного та публічного права
Київського національного університету технологій та дизайну

У статті автор здійснив дослідження кібербезпеки адвокатської діяльності в Україні та світі в її теоретичному та практичному сенсі. Актуальність дослідження зумовлена значним збільшенням кібератак на юридичні фірми; хакери прагнуть отримати доступ до конфіденційних даних, які можуть бути будь-якими, від комерційної таємниці до інформації про майбутні злиття, доступ до фінансових рахунків. Запропоновано авторське розуміння «кібербезпеки діяльності адвоката» – стан захищеності інформації в кіберпросторі, що становить предмет адвокатської таємниці, за якого забезпечуються її конфіденційність, цілісність і доступність. Важливими аспектами дослідження стали акценти щодо значної маргіналізації кібербезпекової політики у сфері надання юридичних послуг в Україні, здійснено узагальнення кращих практик протидії кібератакам на юридичні фірми у провідних країнах світу. Проаналізовано способи кібератак на юридичні фірми: fishing (фішинг), ransomware (програма-вимагач), malware (шкідливе програмне забезпечення) та spyware (шпигунське програмне забезпечення), cryptojacking (криптоджекінг). Установлено причини, через які юридичні компанії є зручною мішенню для кіберзлочинців, запропоновано групування таких причин за такими блоками: one-stop shopping (універсальна покупка), particularly useful information (особливо корисна інформація), low hanging fruit (фрукти, що низько висять). Досліджено стандарти кібербезпеки адвокатської діяльності. Запропоновано заходи захисту та гарантування безпеки юридичної фірми та її клієнтів від кібератак. Висновується, що прийшов час зробити кібербезпеку пріоритетною і в адвокатській діяльності, що вимагає застосування професійних знань, сучасних стратегій та комплексних технологій.

Ключові слова: *кіберпростір, кібербезпека, кіберзлочинець, кібернетичний маргінал, адвокатська діяльність.*

Diorditsa Ihor. Cyber security of advocacy in Ukraine and the world

In the article the author conducted a research of cybersecurity of advocacy in Ukraine and the world in its theoretical and practical sense. The relevance of the study is due to a significant increase in cyberattacks on law firms; hackers seek access to confidential data, which can be anything from trade secrets to information about future mergers or access to financial accounts. The author's understanding of "cybersecurity of a lawyer's activity" is proposed – the state of information security in cyberspace, which is the subject of legal secrecy, which ensures its confidentiality, integrity and accessibility. At the same time, important aspects of the study focused on the significant marginalization of cybersecurity policy in the field of legal services in Ukraine and summarized the best practices to combat cyber-attacks on law firms in leading countries. Methods of cyber-attacks on law firms are analyzed: fishing, ransomware, malware and spyware, cryptojacking. The reasons why law firms are a convenient target for cybercriminals are identified and the grouping of such reasons into the following blocks is proposed: one-stop shopping, particularly useful information, low hanging fruit. The standards of cybersecurity of advocacy are studied. Measures to protect and ensure the security of the law firm and its clients from cyberattacks are proposed. The focus is on the fact that law firms need to regularly assess their risks, and therefore they should turn to the most qualified external experts. Technology is constantly changing, and so are security threats. Ensuring proper cybersecurity is an ongoing process, not a one-time or sporadic measure. It is concluded that the time has come to make cybersecurity a priority in advocacy, which requires the use of professional knowledge, modern strategies and integrated technologies.

Key words: *cyberspace, cyber security, cybercrime, cyber marginal, advocacy.*

Кібербезпека набуває обов'язкового характеру для юридичних фірм зі зростанням кількості кібератак у всьому світі. З метою гарантування власної безпеки та захисту своїх клієнтів юридичні компанії повинні усвідомити, що вони є серед основних цілей для кіберзлочинців. Кібератаки на юридичні фірми по всьому світу зростають разом з атаками на підприємства й урядові організації. Хакери прагнуть отримати доступ до конфіденційних даних, які можуть бути будь-якими – від комерційної таємниці до інформації про майбутні злиття, доступ до фінансових рахунків.

Юридичні послуги значно залежать від знань та інформації. Окрім того, відносини «адвокат – клієнт» не можуть існувати без конфіденційності та зберігання таємниць. Тому захист конфіденційних комунікацій та інформації є першорядним для адвокатської професії [1].

Кібербезпека діяльності адвоката – це стан захищеності інформації в кіберпросторі, що становить предмет адвокатської таємниці, за якого забезпечуються її конфіденційність, цілісність і доступність.

Конфіденційність інформації – це забезпечення доступу до інформації тільки суб'єктів, які мають на це право. Цілісність інформації – стан, за якого її зміна здійснюється тільки навмисно і тільки суб'єктами (авторизованими користувачами), що мають на це право. Доступність інформації – стан, за якого суб'єкти, які мають право доступу до інформації, можуть реалізувати його безперешкодно, тобто безперешкодне забезпечення доступу до інформації авторизованих користувачів [2].

Відповідно до ч. 3 ст. 22 Закону «Про адвокатуру та адвокатську діяльність» адвокат, адвокатське бюро, адвокатське об'єднання зобов'язані забезпечити умови, що унеможливлюють доступ сторонніх осіб до адвокатської таємниці або її розголошення.

Однак навряд чи нині в Україні можна зустріти адвоката, який із метою дотримання принципу конфіденційності переймався б питаннями кібербезпеки й інформаційної безпеки. У результаті проведеного аналізу інформації про заходи з підвищення кваліфікації на сайті НААУ за 9 місяців 2021 р. висновуємо, що, окрім практично-прикладної правової проблематики, відсутні будь-які інші вектори вдосконалення професійної діяльності адвокатів, зокрема й у сфері гарантування кібербезпеки адвокатської діяльності.

Не можу залити поза увагою той факт, що в Законі «Про основні засади забезпечення кібербезпеки України», а саме у ст. 5, серед суб'єктів гарантування кібербезпеки не визначено, зокрема, адвокатуру (чи її органи). На моє переконання, нормативне закріплення адвокатури серед суб'єктів гарантування кібербезпеки безпосередньо посприяло б розвитку нової підгалузевої сфери кібернетичної деонтології – кібернетичної деонтології адвоката.

Згідно з результатами досліджень, майже всі юридичні фірми мають відкриті критичні прогалини на ПК і серверах, половина – на мережевому обладнанні. 65% юрфірм не мають навіть мінімальної системи захисту, 60% уразливі для дій інсайдерів, а 70% – не захищені від зовнішніх загроз. Причинами цього є відсутність шифрування даних, процесів гарантування безпеки і реагування на інциденти; відкриті права доступу; з усіх засобів захисту в основному наявні тільки антивірус і слабкі паролі [3].

Така недбалість юридичної компанії (у разі вчинення кібератаки) може призвести до втрати конфіденційної інформації та продуктів її інтелектуальної праці.

Навіть більше, таке безвідповідальне ставлення адвоката (чи об'єднання) до кіберзагроз та нормативне невизначення його як суб'єкта гарантування кібербезпеки характеризує його як ***кібернетичного маргінала*** – особу, яка перебуває поза контекстом регульованих нормами права кібервідносин (кібервідносини: не виникли, не змінилися і не припинилися), унаслідок чого вони не набули, або втратили, або не було юридично закріплено їхні положення (кібернетичний статус) у кіберпросторі через унікальність власної соціокультурної та кіберментальної ситуації, під час переходу до глобальної кібервзаємодії в рамках спільного функціонування та розвитку в кіберпросторі, відсутності правових можливостей та легітимної неспроможності протистояти нав'язуванню, пристосуватися до якісно

нової архітектури мережевих структур кіберсуспільства.

Послуговуючись наведеною вище статистикою [3], якщо динаміка заходів із гарантування кібербезпеки юридичних фірм залишиться без змін, можемо припустити, що разом з особами, що перебувають на маргінесі цивілізації і поза контекстом розвитку суспільства взагалі, сформується інтегрований змікшований маргінальний кластер у сфері адвокатури.

Цілком слушною є позиція Анни Кухар, членкині Ради Комітету АПУ з питань телекомунікацій, інформаційних технологій та інтернету, про те що юридичні компанії, зі своїм багажем «компроматів» та інформації про клієнтів, є привабливим об'єктом для кіберзлочинців. Під загрозою можуть бути як адвокати, які практикую індивідуально, так і великі юридичні компанії [4].

Зі значною маргіналізацією кібербезпекової політики у сфері надання юридичних послуг в Україні, з метою узагальнення кращих практик протидії кібератакам на юридичні фірми було здійснено конвент-аналіз низки іноземних англомовних джерел із досліджуваної проблематики.

Приклади кібератак на юридичні фірми

Адвокати, як відомо, не завжди компетентні щодо кібербезпекових технологій, і це дозволяє хакерам легко отримати доступ до інформації про їхніх клієнтів. Дослідження, проведене консалтинговою компанією з кібербезпеки LOGICFORCE, показало, що хакери, які володіють шкідливим програмним забезпеченням, використовують вразливі місця, які є широко розповсюдженими в усій юридичній галузі. Юридичні компанії не повинні втішатися, уважаючи, що вони можуть бути занадто маленькими або віддаленими, щоб стати жертвою кіберзлочинця [5].

За даними Американської асоціації юристів, 22% з понад 4 000 респондентів, які взяли участь в опитуванні ABA 2017 Legal Technology Survey, заявили, що їхні фірми зіткнулися з витоком даних у 2017 р., порівняно із 14% у 2016 р. З усіх опитаних респондентів 25% повідомили про відсутність у їхній діяльності кібербезпекової політики, причому в цій категорії лідирують невеликі фірми, а 7% усіх респондентів заявили, що не знають про політику кібербезпеки [6].

У статті, опублікованій у The National Law Journal, одна вашингтонська фірма повідомила, що кількість щоденних спроб кібератак, свідком яких вона стала, збільшилася на 500% тільки за останні два роки [7].

Law 360 недавно повідомила, що «особисті дані до 1 500 американських власників полісів комерційного страхування могли бути скомпрометовані внаслідок злому неназваної спеціалізованої юридичної фірми» (за даними спеціалістів страхової компанії "Hiscox Ltd") [8].

Панамська юридична фірма "Mossack Fonseca" (четверта за величиною офшорна юридична фірма у світі) у 2015 р. зіткнулася з порушенням безпеки, унаслідок чого стався витік 2,5 терабайтів даних. Наслідки розлетілися по всьому світу, коли з'ясувалося, що фірма брала участь у створенні понад 200 000 підставних корпорацій для ухилення від сплати податків. У результаті у відставку пішли прем'єр-міністр Ісландії та міністр промисловості Іспанії. Якби дана фірма дбала про власну кібербезпеку і вжила необхідних заходів, вона б не постраждала від злому.

У 2016 р. китайський бізнесмен і політичний дисидент Венгуі найняв міжнародну юридичну фірму "Clark Hill", щоб отримати політичний притулок у США. Венгуі пояснив співробітникам Clark Hill, що китайський уряд зробив його об'єктом постійних кібератак і цілком імовірно, що вони піддадуться аналогічним атакам. Так, 12 вересня 2017 р. сервери Clark Hill були зламані, унаслідок чого були скомпрометовані паспортні дані Венгуі та його дружини, їхню заяву про надання політичного притулку, яка потім була поширена в інтернеті. На загальну думку, злом був організований китайським урядом. Після цієї події Clark Hill спробувала зняти із себе будь-яку відповідальність, відмовившись від послуг Венгуі як клієнта. Потім Венгуі подав позов проти Clark Hill на 50 мільйонів доларів за порушення фідуціарних обов'язків, порушення контракту і юридичну несумлінність. Справа триває, але суд постановив, що Венгуі пред'явив обґрунтовані претензії за недобросовісну роботу [9].

За останні кілька років почали з'являтися позови, засновані на загрозі

витоку даних, навіть до того, як будь-які дані були скомпрометовані.

Наприклад, чиказька юридична фірма "Johnson & Bell" є відповідачем у справі, де позивач стверджує, що їхній вебпортал вразливий для атак, тому продовжує піддавати ризику інформацію клієнтів.

Johnson & Bell стверджує, що їхня система безпечна, але їхні сервери працюють на застарілому програмному забезпеченні JBoss, яке має відомі вразливості.

Зазначу, що компанія "Johnson & Bell" має у своєму розпорядженні значний обсяг конфіденційної ділової інформації, як-от фінансові звіти, угоди зі злиття і поглинання та багато іншого.

Якщо суддя ухвалить рішення на користь позивача, буде створений новий прецедент щодо того, як юридичні фірми повинні управляти і зберігати дані клієнтів [10].

Кіберзлочинці можуть атакувати юридичну фірму різними способами.

Fishing (фішинг).

Фішингові атаки відбуваються постійно, але ось один із прикладів. У 2012 р. хакери отримали доступ до комп'ютера бухгалтера юридичної фірми в Торонто за допомогою фішингової атаки, імовірно, через вкладення в електронний лист або безкоштовну заставку (фірма й нині точно не знає). Потім хакери змогли записати паролі банківських рахунків, які набирав бухгалтер. Це дало їм повний доступ до трастового рахунку фірми, який вона використовувала для переказу коштів в інші країни. Фірма втратила шестизначну суму тільки за грудневі свята [11].

Ransomware (програма-вимагач).

Ransomware стає все більш небезпечною для юридичних фірм. Хакери шифрують дані фірми, а потім вимагають оплати в біткоїнах. Жертвою може стати фірма будь-якого розміру. Ransomware зазвичай проникає в системи юридичної фірми через фішинг. Вона шифрує дані, а злодії вимагають викуп в обмін на ключ для розшифровки.

У відомому інциденті 2017 р. глобальна юридична фірма "DLA Piper", яка позиціонує себе як експерт у сфері кібербезпеки, піддалася атаці програми-вимагача під назвою Petya. Фірма на деякий час втратила доступ до своїх даних і протягом трьох днів не мала телефонів та електронної пошти [12].

Malware (шкідливе програмне забезпечення) та spyware (шпигунське програмне забезпечення).

Хакери іноді заражають комп'ютерні системи юридичних фірм шкідливими програмами, які шпигують за юридичною фірмою. Серйозні наслідки зараження шкідливим ПЗ включають втрату даних і втрату конфіденційності даних. Звіт ABA Legal Technology Survey Report показав, що:

– 40% респондентів повідомили про зараження;

– 37% повідомили про відсутність заражень;

– 23% повідомили, що не знають про те, чи піддавалися вони шкідливому ПЗ.

Найбільш високий рівень зараження *malware* та *spyware* у фірмах із числом адвокатів від 10 до 49 (48%), найменше у фірмах із числом адвокатів більше 500 (20%) [6].

Cryptojacking (криптоджекінг).

Криптоджекінг є відносно новим видом кіберзлочинів. Злодії використовують програмне забезпечення для викрадення таких пристроїв, як ноутбуки та мобільні телефони, і перетворюють їх на пристрої для збирання криптовалют. Коли з'являються нові комунікаційні технології, вони часто відкривають хакерам нові можливості. Юридична фірма має бути в курсі технологій та захищатись від загроз.

Юридичні компанії є зручною мішенню для кіберзлочинців із деяких логічних причин.

One-stop shopping (універсальна покупка).

Якщо хакери зможуть проникнути в системи юридичної фірми, вони можуть отримати доступ до конфіденційних та інших цінних даних не однієї компанії, а багатьох – усіх клієнтів юридичної фірми.

Particularly useful information (особливо корисна інформація).

На серверах юридичних фірм може зберігатися цінна інформація – від інтелектуальної власності підприємств до медичних записів і державної таємниці. Якщо злочинець збираєтеся зламати сервер, то має сенс зламувати там, де винагорода буде коштувати таких зусиль.

Low hanging fruit (фрукти, що низько висять).

Багато юридичних фірм не захистили себе і своїх клієнтів від кібератак належним чином.

Стандарти кібербезпеки адвокатської діяльності (на прикладі США).

Американська асоціація адвокатів (ABA) дотримується Типових правил професійної поведінки з моменту їх затвердження в 1983 р. Ці правила є внутрішнім компасом для юристів, яким вони керуються в різних сценаріях і взаємодії із клієнтами.

Правило 1.6, що стосується конфіденційності інформації клієнта, говорить: «Адвокат повинен докладати розумних зусиль для запобігання ненавмисному або несанкціонованому розкриттю інформації, що належить до представництва клієнта, або несанкціонованому доступу до неї» [13].

По суті, це означає, що адвокати повинні докладати зусиль для захисту даних своїх клієнтів.

Однак адвокати зобов'язані захищати конфіденційні дані клієнтів уже досить давно. У цьому немає нічого нового. Змінилося те, як юридичні фірми повинні захищати своїх клієнтів у сучасних умовах кіберзагроз. Коментар до правила 1.1 Типових правил професійної поведінки зобов'язує адвокатів стежити не тільки за змінами в законодавстві та за судовою практикою, а й за перевагами і ризиками, пов'язаними з відповідними технологіями [14].

Залежно від різних чинників юридичні компанії повинні «контролювати мережеву діяльність, переглядати IT-звіти і, можливо, найняти керівника відділу з питань IT-безпеки (CISO) для розробки, упровадження та підтримки відповідних програм кібербезпеки». Якщо цього не зробити, це може призвести до судових позовів про порушення службових повноважень.

У 2018 р. ABA випустила Formal Opinion 483 (Офіційна думка 483) [15], де йдеться про важливість захисту даних і те, як впоратися з неминучим порушенням безпеки. У висновку говориться, що ризик того, що юридичні фірми зіткнуться з витоком даних, залежить не від того, якщо, а від того, коли. У висновку викладені вимоги до дій до, під час і після кібератаки, спрямованої на юридичні фірми.

Аналітики Atlant Security, компанії, що спеціалізується на гарантуванні інформаційної та кібербезпеки в усьому світі, рекомендують такі ***заходи захисту та гарантування безпеки юридичної фірми та її клієнтів від кібератак*** у 2021 р.

Створіть усвідомлену культуру (кіберосвіти та кіберграмотності – І. Д.) фірми.

Старші партнери фірми повинні переконатися, що всі її співробітники зацікавлені в безпеці даних. Вони повинні організувати постійне навчання з питань гарантування безпеки даних на всіх пристроях.

Тримайте свою фірму напоготові.

Не досить просто навчити всіх співробітників вашої фірми і забути про це. Необхідно регулярно проводити перепідготовку і тестувати людей. Можливо, ви навіть захочете відправити підроблені «фішингові» листи, щоб подивитися, хто на них натисне. Звичайно, за цим послідує ще одне навчання. Постійне навчання – важливий ключ до гарантування кібербезпеки.

Призначте відповідального.

Якщо розмір вашої компанії дозволяє, ви захочете, щоб ваш керівник відділу з питань IT-безпеки контролював кібербезпеку вашої компанії. Інакше керівник фірми може контролювати її за допомогою кращих експертів із кібербезпеки, яких він може і має знайти.

Створіть резервні копії.

Тільки 40% адвокатів, які взяли участь у звіті ABA Legal Technology Survey Report 2018, повідомили, що їхні фірми мають план аварійного відновлення/безперервності бізнесу. Якісне резервне копіювання даних може захистити вас від програм-вимагачів та інших шкідливих програм, які їх знищують.

Використовуйте якісне антивірусне програмне забезпечення.

Не досить просто використовувати антивірусне програмне забезпечення. Переконайтеся, що ваше антивірусне програмне забезпечення ефективне, постійно оновлюйте його.

Підтримуйте програмне забезпечення в актуальному стані.

Використовуйте найсучасніші операційні системи і програмне забезпечення, своєчасно встановлюйте програмні виправлення.

Обмежте доступ.

Надавайте доступ до даних тільки тим, кому він справді необхідний. Іноді співробітники самі можуть становити загрозу, і навіть якщо це не так, вони є ще однією позицію, через яку може проникнути хакер.

Будьте обережні під час передачі файлів.

Правильна обробка файлів має бути частиною вашого навчання. Наприклад, ви не хочете, щоб люди завантажували їх на флешку і виходили з ними за межі офісу. Якщо файли потрібно передати, їх треба зашифрувати та захистити паролем. Ви також можете використовувати інфраструктуру віртуального робочого столу (VDI), щоб файли не зберігалися на ноутбуках, а лише на сервері VDI.

Захистіть свою електронну пошту.

Наполягайте, щоб вся електронна пошта надсилалася лише з фірмових облікових записів, які можна зашифрувати. Вам потрібно буде дотримуватись цієї політики, оскільки адвокати легко можуть надсилати важливу інформацію зі своїх особистих акаунтів, коли вони будуть удома у вихідні. Окрім того, запровадьте політику збереження електронної пошти, щоб зберігалась тільки та пошта, яка справді необхідна.

Подумайте про передачу функції з гарантування кібербезпеки на аутсорсинг експертам.

Якщо ваша компанія не є великою, то дуже сумнівно, що у вас у штаті є фахівці з кібербезпеки, здатні забезпечити максимально ефективний постійний захист ваших даних. Щоб ефективно захистити свої дані самостійно, вам необхідно створити операційний центр безпеки, який буде перевіряти весь ваш трафік, класифікувати його за ступенем ризику, зупиняти підозрілий трафік на його шляху і негайно усувати порушення. Зрозуміло, що необхідно також розробити надійний план антикризового управління на випадок злому ваших систем [16].

Висновки. Отже, юридичні фірми повинні регулярно оцінювати свої ризики. Більшість із них не володіють достатнім досвідом для цього, тому їм варто звернутися до найбільш кваліфікованих зовнішніх експертів. Технології постійно змінюються, загрози безпеки теж. Гарантування належної кібербезпеки – це постійний процес, а не разовий або епізодичний захід.

Просто подумайте про одного із провідних адвокатів юридичної фірми та про те, як він розподіляє свій час у період роботи та повсякденного життя. Можливо, він починає день із перевірки електронної пошти, оновлення свого статусу у Facebook, здійснення дзвінка клієнту та надсилання подальшого електронного листа із вкладеною конфіденційною інформацією. Не одна, а кожна окрема із цих дій відкриває інформацію, яку хакери можуть використовувати для проникнення в юридичну фірму.

Прийшов час зробити кібербезпеку пріоритетною і в адвокатській діяльності. Вона вимагає застосування професійних знань, сучасних стратегій та комплексних технологій.

ЛІТЕРАТУРА:

1. Важливість кібербезпеки для юридичних фірм. 2021. Протокол. URL: https://protocol.ua/ru/vaglivist_kiberbezpeki_dlya_yuridichnih_firm/

2. Завадський А. Інформаційна та кібербезпека адвокатської діяльності: теоретичні та практичні аспекти (досвід США). *Порівняльно-аналітичне право.* 2020. № 1. URL: https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/35837/1/%D0%86%D0%9D%D0%%D0%A2%D0%90%20%D0%9A%D0%86%D0%91%D0%95%D0%A0%D0%91%D0%95%D0%97%D0%9F%D0%95%D0%9A%D0%90.pdf

3. Новикова А. Питання кібербезпеки у світі юриспруденції. *Судово-юридична газета.* 2019. URL: https://sud.ua/ru/news/publication/138379-pitannya-kiberbezpeki-u-sviti-yurisprudentsiyi

4. Кухар А. «Вас хакнули», ч 1 : про кіберзлочини на теренах юрринку. *Асоціація правників України*. 2020. URL: https://uba.ua/ukr/news/7764/

5. Vivian Hood Law Firms and Cyber Attacks – What's a Law Firm to Do? Part One. The National Law Review. 2018. URL: https://www.natlawreview.com/article/law-firms-and-cyber-attacks-what-s-law-firm-to-do-part-one

6. David G. Ries. 2017 Security. *The American Bar Association.* 2017. URL: https://www.americanbar.org/groups/law_practice/publications/techreport/2017/security/

7. Ryan Lovelace. Fearing DLA Piper-Style Breach, DC Firms Ramp Up Cyber Defenses. *The National Law Journal.* 2018. URL: https://www.law.com/nationallawjournal/sites/nationallawjournal/2018/02/22/fearing-dla-piper-style-breach-dc-firms-ramp-up-cyber-defenses/?slreturn=20210717042011

8. Law360. Hiscox Says Hack of US Law Firm Exposed Policyholders. 2018. URL: https://www.law360.com/articles/1033532/hiscox-says-hack-of-us-law-firm-exposed-policyholders

9. Hope A. Comisky. Wengui v. Clark Hill – Lessons Learned to Protect Privilege in the Investigation of a Cyber Breach. 2021. URL: https://www.americanbar.org/groups/business_law/publications/blt/2021/03/wengui-v-clark-hill/

10. Jason Shore and Coinabul, Llc v. Jonson & Bell, Ltd, an Illinois corporation *United States District court for the Northern District of Illinois, Eastern Division.* 2016. URL: https://www.datasecuritylawjournal.com/files/2016/12/Johnson-and-Bell-Complaint.pdf

11. Adam Adler. Encrygma About How Cyber Attacks Damage Law Firms and Their Clients. *Digital Bank Vault Limited.* 2020. URL: https://www.digitalbankvault.com/post/how-cyber-attacks-damage-law-firms-and-their-clients

12. Malwarebytes All about ransomware attacks. 2021. URL: https://www.malwarebytes.com/ransomware

13. The American Bar Association. Rule 1.6 : Confidentiality of Information. URL: https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/

14. The American Bar Association. Rule 1.1 Competence – Comment. URL: https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence/comment_on_rule_1_1/

15. The American Bar Association. Formal Opinion 483. URL: https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_op_483.pdf

16. Atlant Security. Cyber Security For Law Firms – 7 Critical Objectives for 2021. URL: https://atlantsecurity.com/cybersecurity-for-law-firms/