СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ПРАВА
ЛІГА СТУДЕНТІВ АСОЦІАЦІЇ ПРАВНИКІВ УКРАЇНИ

РЕФОРМУВАННЯ ПРАВОВОЇ СИСТЕМИ В КОНТЕКСТІ ЄВРОІНТЕГРАЦІЙНИХ ПРОЦЕСІВ

МАТЕРІАЛИ
IV Міжнародної науково-практичної конференції
(Суми, 21–22 травня 2020 року)

У двох частинах

Частина 2

Суми
Сумський державний університет
2020

користувачів;

- головне правило корпоративної безпеки: один комп'ютер - тільки для роботи з банком, обслуговуючим організацію і більш ні для чого;
- не слід використовувати електронні носії інформації в невідомих пристроях і навпаки.

Якщо комп'ютерна система все-таки була атакована, не поспішати перераховувати грошові кошти зловмисникам, так як немає гарантії того, що шкідливе програмне забезпечення буде безповоротно видалено з комп'ютера і вимагання не повториться знову, а також не приховувати інцидент комп'ютерної безпеки, як від керівництва, так і від правоохоронних органів, не намагатися самостійно перевстановити систему. Необхідно негайно повідомити в правоохоронні органи і вжити всіх заходів для збереження і фіксації слідів здійсненої кібератаки.Дотримання представлених правил захистить комп'ютерну систему конкретного користувача, надасть значну роль у зміцненні інформаційної безпеки України в цілому, а також допоможе в фіксації слідів і в розслідуванні подібних інцидентів.

Незважаючи на всю масштабність кіберзагроз, при узгодженості дій, можливо їм успішно протидіяти. Якщо держава здійснює боротьбу з кіберзлочинцями законодавчими та організаційними заходами, то в силах кожного користувача внести свій неоціненний внесок у спільну справу – знати і дотримуватися елементарних правил кібербезпеки, своєчасно і грамотно реагуючи на неполадки в роботі комп'ютерної системи.

ЛІТЕРАТУРА:

1. Кибератака. URL: http://www.securitylab.ru/news/ (дата звернення: 10.04.2020).
2. Бехметьев А. Е. Кибератаки. *Административное право*. №1. 2017. С. 17.

МЕХАНІЗМ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В ЄВРОПЕЙСЬКОМУ СОЮЗІ ТА ЙОГО ВДОСКОНАЛЕННЯ В УКРАЇНІ

Костенко З. В.
Студент IV курсу ННІ права
Сумського державного університету
Науковий керівник: Думчиков М. О.
к. ю. н., асистент кафедри КПДС ННІ права
Сумського державного університету

У сучасному світі спостерігається широке поширення і застосування інформаційних технологій, методів автоматичної обробки даних, формування глобальних

інформаційних систем, доступ до яких може здійснюватися практично будь-якою особою з будь-якої точки земної кулі. Якщо раніше в це було важко повірити, то сьогодні це цифрова реальність. З однієї сторони, такі переваги вільного доступу до інформації безпосередньо забезпечують громадянам реалізацію одного з головних демократичних прав на свободу інформації. З іншої сторони, широке використання персональних даних органами державної влади, комерційними і суспільними організаціями істотно підсилює ризик несанкціонованого вторгнення сторонніх осіб в особисту сферу людини, що може порушити право на недоторканість приватного життя, гарантованого державою.

Найбільш активний розвиток норм про захист персональних даних спостерігається в європейському праві. До найбільш вагомих документів у цій сфері можна віднести Європейську конвенцію про захист прав і основних свобод, Конвенцію Ради Європи про захист прав фізичних осіб щодо автоматичної обробки персональних даних, Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних», та Хартію Європейського Союзу про основні права. Саме на цих нормативно-правових актах будується механізм захисту персональних даних на європейському просторі.

Ефективний захист персональних даних в ЄС забезпечується завдяки комплексному механізму, що складається з наступних елементів:

• загальноєвропейська нормативна база, національні законодавчі акти, що регулюють питання захисту персональних даних, межі їх захисту, що визначають умови передачі персональних даних третім країнам;

• основні принципи права щодо захисту персональних даних, що володіють правовою чіткістю;

• європейські консультативні та наглядові органи щодо захисту персональних даних;

• особливий правовий статус, основні права, свободи та обов’язки суб’єктів даних, контролерів, операторів та третіх осіб.

Звичайно, що в Україні в базах даних різних органах державної влади, установах та підприємствах знаходиться величезний обсяг персональних даних, які з кожним днем стають дуже популярним об’єктом господарського обороту, при тому, що українське законодавство щодо захисту персональних даних знаходиться на етапі формування. В Європейському Союзі і багатьох інших країнах спеціальне законодавство про захист персональних даних існує вже більше десяти років. Однак, в цих країнах йде активний розвиток і вдосконалення інформаційних технологій, і з кожним роком інститут захисту персональних даних вдосконалюється набагато інтенсивніше, ніж у нас.

Інститут захисту персональних даних являє собою сукупність правових норм, що регулюють суспільні відносини, що виникають при зборі, використанні, зберіганні, обробці, видаленні, передачі і розкритті персональних даних, а саме будь-якої інформації, пов'язаної з ідентифікованою особою. Як елемент системи права він представлений сукупністю правових норм, що регулюють однорідну групу суспільних відносин, що характеризуються однорідністю фактичного змісту, що базуються на загальних принципах захисту персональних даних і включають специфічні правові поняття. Інститут захисту персональних даних включає в себе весь спектр норм, необхідних для повноти правового регулювання, в тому числі норми-дефініції, уповноважуючі норми, наприклад, норми про права суб'єкта даних, забороняючі норми, наприклад, норми про заборону обробки даних без згоди суб'єкта даних [1].

Використання персональних даних в політичній діяльності також набуває особливий інтерес серед європейських вчених і практиків. Право свободи політичної мови є одним з основних прав громадян ЄС. В європейських країнах з метою підвищення відкритості діяльності органів державної влади активно використовуються системи електронного уряду, які, для авторизації доступу громадян, де міститься інформація, вимагають обробки їх персональних даних. В результаті ведення подібних баз даних, а також збору інформації політичними організаціями, в останніх накопичується великий обсяг персональних даних про членів партій, членів груп підтримки, а саме електронні адреси, телефонні номери, дані про сімейний стан і місце роботи, а також про приналежність до політичних партій і політичних поглядах, які відносяться до категорії персональних даних, які потребують особливого захисту.

Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» закріпила вісім основних принципів захисту персональних даних, відповідно до яких повинні діяти «контролери даних». Таким чином, країни-учасниці ЄС повинні забезпечити реалізацію наступних основних принципів:

1. Персональні дані обробляються сумлінно та законно (принцип «законності»);

2. Персональні дані збираються для певних, чітких і легітимних цілей і не можуть бути надалі оброблені способом, несумісним з даними цілями (принцип «цільової визначеності»);

3. Персональні дані повинні відповідати цілям, для яких вони збираються і обробляються, (принцип «мінімальності»);

4. Персональні дані повинні бути точними і в разі необхідності оновлюватися (принцип «якості інформації»);

5. Контролери даних або їх представники повинні надати суб'єкту даних, про який або від якого збираються персональні дані, певну інформацію і забезпечити доступ суб'єкта даних до його персональних даних (принцип «участі суб'єкта даних і здійснення ним контролю»);

6. Розкриття персональних даних контролерами даних третім особам обмежується і може здійснюватися тільки при дотриманні певних умов (принцип «обмеження розкриття персональних даних»);

7. Контролер повинен вжити всіх необхідних технічних та організаційних заходів для захисту персональних даних від випадкового або незаконного знищення або випадкової втрати, зміни, несанкціонованого розголошення або доступу, в разі передачі даних по мережах, а також від будь-яких інших форм незаконної обробки даних (принцип «інформаційної безпеки»);

8. Обробка особливих персональних даних повинна здійснюватися при більш строгому контролі, ніж інших персональних даних (принцип «чутливості») [2].

Стосовно України, то до 2010 року в Україні здебільшого окремі питання захисту персональних даних було врегульовано у межах конституційного, частково – інформаційного та міжнародного права. Конституцією України гарантовані основні права та свободи людини і громадянина. Прийняття 1 червня 2010 року Закону України «Про захист персональних даних», що набув чинності 1 січня 2011 року, ратифікація Верховною Радою України у липні 2010 року Конвенції Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до неї щодо органів нагляду та транскордонних потоків даних стали важливим етапом становлення системи захисту персональних даних в Україні як у правовому, так і в інституційному значенні [3, с. 100].

Незважаючи на те, що за останній час Україні в цілому вдалося сформувати сучасну та адекватну нормативно-правову основу для подальшого формування вітчизняної системи захисту персональних даних, наразі в Україні закладені лише основи вітчизняного законодавства у сфері захисту персональних даних, яке у цілому відповідає міжнародним стандартам. Однак потрібна подальша робота з його систематизації, розробки підзаконних актів, відповідних національних стандартів, чіткого визначення термінів, понять та категорій [4, с. 81]. Таким чином, механізм захисту персональних даних ЄС може бути використаний в якості моделі при подальшому вдосконаленні національної системи правового захисту персональних даних в Україні.

ЛІТЕРАТУРА:

1. Головченко В. Правові основи захисту персональних даних. *Юридична газета online.* № 36 (638). 2018.
2. Директива 95/46/ЄС Європейського парламенту та Ради Європейського Союзу «Про захист осіб у зв'язку з обробкою персональних даних та вільним обігом цих даних» від 24.10.1995 р. URL: www.evropa.eu.int/ISPO/legal/en/dataprot /directiv/directiv.html.
3. Мельник К. С. Іноземний та вітчизняний досвід становлення інституту захисту персональних даних. *Інформаційна безпека людини, суспільства, держави*. 2013. № 2. С. 97–103.
4. Теремецький В. І. Застосування зарубіжного досвіду правового захисту персональних даних в Україні. *Часопис Академії адвокатури України*. 2014. Т. 7. № 2. С. 73–82.

ОСОБЛИВОСТІ БАНКІВСЬКОЇ ТАЄМНИЦІ ТА ПОРЯДКУ ЇЇ РОЗКРИТТЯ

Неверова С. А.
Студентка IV курсу ННІ права
Сумського державного університету
Науковий керівник: Думчиков М. О.
к .ю. н., асистент кафедри КПДС ННІ права
Сумського державного університету

Банківська система України включає в себе Національний банк України, інші банки, фінансові установи та представництва іноземних банків. Їх завданнями є здійснення банківських операцій, операцій з клієнтами і організація міжбанківських кредитно-фінансових відносин. Банківська діяльність нерозривно пов'язана з отриманням та передачею певної інформації, значну частину якої становлять відомості, що є банківською таємницею. Тим паче, нещодавно до порядку розкриття банківської таємниці були внесені певні зміни.

Ще з XVIII століття, з моменту прийняття Женевських банковсьвких правил кантональною радою, і до кінця минулого століття, банківська таємниця вважалася показником стабільної фінансової системи держави. Більш за все це виражалося у прагненні захистити інформацію про вклади та переведення особи від можливого доступу з боку держави. Сьогодні ж держави намагаються збільшити доступ до банківської таємниці, але з поважних причин, насамперед, національної безпеки. Наприклад, з 1 серпня 2010 року за укладеним між ЄС і США угодою, будь-яка інформація приватного особи-громадянина Євросоюзу потрапляє до спецслужб, якщо є підстави вважати, що ця особа підозрюється в тероризмі.