УДК 004.056 **Бабенко Т.В., Третяк О.М., Мещеряков Л.І., Кручінін О.В. (НГУ)**

ОБРОБКА ПЕРСОНАЛЬНИХ ДАНИХ В УМОВАХ ДІЯЛЬНОСТІ ВИЩИХ НАВЧАЛЬНИХ ЗАКЛАДІВ

У статті розглянуто процес обробки персональних даних у вищих навчальних закладах, виконано аналіз законодавчих актів у сфері захисту інформації та висунуто ряд пропозицій щодо створення необхідних умов для реалізації вимог, зазначених у Законі України «Про захист персональних даних».

Прагнення інтеграції України до Євросоюзу та загальна інформатизація усіх сфер життя нашого суспільства сприяють реформуванню законодавчої бази України та її гармонізації з міжнародними стандартами. Останнім часом в Україні ратифіковано конвенцію Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» [1], прийнято створений на її основі Закон України «Про захист персональних даних» [2], внесено зміни та доповнення до Закону «Про інформацію» [3]. Під впливом нововведень змінюються і технології обробки інформації в освітній сфері, так, зокрема, в 2011 році Міністерство освіти і науки, молоді та спорту України запровадило експеримент «Електронний вступ» [4]. Його сутність полягає в тому, що абітурієнт зможе заповнювати свої вихідні (анкетні) дані в он-лайн режимі на інтернет-порталі «Єдине освітнє інформаційне вікно України», а вищі навчальні заклади – отримувати електронні заяви та контактувати з вступником засобами електронного зв'язку. З точки зору інформаційної безпеки перехід до електронної реєстрації ставить перед учасниками цього процесу багато питань як організаційного так і програмно-технічного характеру. Зокрема, це стосується обов'язкового впровадження і сертифікації комплексної системи захисту інформації, організації захищеного зберігання, обробки та знищення персональних даних абітурієнтів.

Метою даної статті є аналіз стану та заходів щодо забезпечення захищеності інформації в інформаційно-комунікаційних системах державних вищих навчальних закладів за умови набуття чинності закону «Про захист персональних даних».

Інформаційно-комунікаційна система вищого навчального закладу, як правило, представляє собою складну сукупність підсистем, призначених для автоматизації діяльності окремих адміністративних структур, бази даних яких можуть містити персональні дані.

Певні непорозуміння виникають вже на етапі визначення поняття «персональні дані». Згідно Закону України «Про захист персональних даних» це «відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована» [2], зокрема, у пункті 2 статті 5 закону зазначено, що «персональні дані, крім знеособлених персональних даних, за режимом доступу є інформацією з обмеженим доступом». Звернемося до закону «Про інформацію» [3], у статті 11 якого вказано, що обробка конфіденційної інформації про особу, а саме: даних про її «національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження» заборонена без її згоди. У законі «Про захист персональних даних» відсутня градація відповідно до ступеня вразливості персональних даних, отже будь-яку інформацію про фізичну особу, поєднану з її ім'ям, слід вважати конфіденційною і необхідно мати дозвіл суб'єкта персональних даних на її обробку. Відсутність чіткого поділу інформації може призвести до непорозумінь та конфліктних ситуацій з правової точки зору.

Закон «Про захист персональних даних» набув чинності 01.01.2011, але процедури збору та обробки персональних даних досі детально не визначені нормативними чи розпорядчими документами. Відповідно до Указу Президента №390 від 06.04.2011р. реалізацією державної політики у сфері захисту персональних даних повинна здійснювати Адміністрація державної служби України з питань захисту персональних даних [4]. До сфери її повноважень віднесено: створення методичних матеріалів і рекомендацій щодо визначення критеріїв і порядку оцінювання стану захищеності даних про фізичну особу, розробку

«Типового порядку обробки персональних даних у базах персональних даних» та ін. Якщо уважно прочитати Закон України «Про захист персональних даних», то можна виділити ще як мінімум три підзаконних нормативно-правових акти, які повинні бути прийняті Національним банком та Кабінетом міністрів України - це «Порядок обробки персональних даних, які належать до банківської таємниці» (п.10, ст. 6), «Положення про державний реєстр персональних даних» (п. 1, ст. 10) та «Порядок ведення Державного реєстру баз персональних даних» (п. 1, ст. 10).

Вищий навчальний заклад є установою, де персональні дані складають значну частину інформації, що обробляється. Типовою є наявність баз персональних даних контингенту абітурієнтів, студентів, професорсько-викладацького складу і навчально-допоміжного персоналу, які включають: ПІБ, дату народження, стать, місце народження, громадянство, паспортні дані, ідентифікаційний код, дані про освіту, успішність у навчанні, відношення до військової служби, сімейний стан, сімейні умови, матеріальну забезпеченість, адресу тощо.

На всіх етапах обробки персональних даних виникають загрози порушення їх конфіденційності, цілісності, доступності як від зовнішніх зловмисників так і від внутрішніх порушників. Аналізуючи це питання звернемося до звіту Центру SECURIT Analytics щодо витоку конфіденційної інформації за підсумками 2010 року. [5]

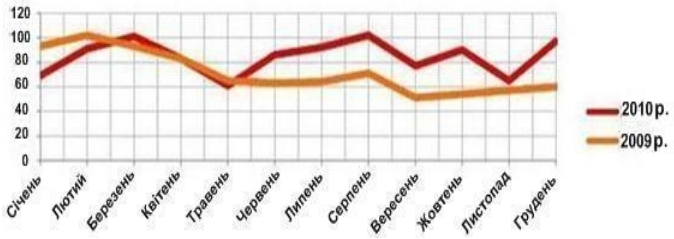

Рис. 1. Динаміка витоку конфіденційної інформації за даними SECURIT Analytics

З графіку (рис.1) видно, що кількість інцидентів, пов'язаних з витоком конфіденційної інформації, наприкінці 2010 року почала стрімко зростати і порівняно з 2009 роком підвищилася на 15, 6 %. Важливим фактом є те, що інциденти витоку саме персональних даних склали 63,6 % серед загального числа [5], що підтверджує необхідність приділити підвищену увагу цій проблемі. Графік (рис.2) з аналітичного звіту компанії Infowatch [6] також відображає тенденцію зростання, хоча і не таку значну.

Аналіз наведеної інформації свідчить, що у світі відбувається постійне зростання витоку конфіденційної інформації. Деякі розбіжності в отриманих результатах аналізу викликані тим, що Infowatch розглядає лише внутрішні інциденти, в той час як SECURIT Analytics аналізує всі типи атак. Враховуючи цей фактор, можна зробити висновок, що рівень внутрішніх атак є стабільно високим, а загальна динаміка викликана додатковим зростанням активності зовнішніх порушників.

Рис. 2. Динаміка витоку конфіденційної інформації за даними компанії Infowatch

Переважна більшість інцидентів витоку конфіденційної інформації (на думку аналітиків Infowatch вона складає близько 96%) стосується саме персональних даних через їх високу вартість на нелегальному ринку збуту та їх недостатню захищеність. Навчальні заклади не є виключенням – за результатами дослідження [6] у 12% випадків витік персональних даних відбувався з освітніх установ. Таким чином, перед керівництвом вищого навчального закладу постає досить складне питання щодо організації ефективного захисту інформації в тому числі і про фізичну особу.

На прикладі аналізу актуального на сьогодні для вищих навчальних закладів питання подачі заяв про вступ, розглянемо процедуру збору персональних даних. Абітурієнт має право зареєструватися в інтерактивному режимі [7], проте відсутні будь-які нормативно-правові акти, в яких визначено механізм одержання згоди на виконання дистанційних операцій з використанням персональних даних користувачів інтернет-сервісів. Виходячи з положень Закону України «Про захист персональних даних», згода суб'єкта персональних даних – це будь-яке документоване, зокрема письмове, добровільне волевиявлення фізичної особи щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки. Отже, таке волевиявлення не обов'язково має бути письмовим – це лише один з можливих варіантів, але воно має бути документованим. Уточнюючи поняття документу звернемося до Закону України «Про інформацію», згідно якого «документ – це матеріальний носій, що містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі», тобто, зафіксовану в електронному вигляді згоду, яка зберігається на жорсткому диску комп'ютера, можна вважати законною. Але складність полягає в доведенні факту, що саме ця особа, у конкретний час надала згоду на використання персональних даних з певною метою. Можливим рішенням є використання електронного цифрового підпису, адже стаття 3 Закону України «Про електронний цифровий підпис» говорить, що електронний цифровий підпис прирівнюється до власноручного, якщо його підтверджено з використанням посиленого сертифіката ключа. Цей спосіб безперечно є надійним, але реалізувати його в межах вищого навчального закладу складно.

Зберігання одержаних персональних даних згідно статті 13 закону «Про захист персональних даних» передбачає дії щодо «забезпечення їх цілісності та відповідного режиму доступу до них» [2]. Після закінчення строку зберігання персональні дані повинні бути знищені, а власник повідомлений про факт знищення. Адміністрація вищого навчального закладу відповідно до вимог Закону України «Про інформацію» [3] за невиконання правил обробки інформації, зокрема, про персональні дані, може бути притягнута до дисциплінарної цивільно-правової, адміністративної або кримінальної відповідальності (ст.182 Кримінального кодексу України). Нещодавно Кодекс України про адміністративні правопорушення також було доповнено статтями 188-39 і 188-40, які передбачають накладання штрафу у разі недодержання встановленого законодавством порядку захисту персональних даних у базі персональних даних.

З урахуванням нових організаційних особливостей обробки персональних даних в рамках висунутих законодавством вимог, суттєво ускладнюється технічна сторона забезпечення цього процесу. Закон України «Про захист персональних даних» регламентує, що володілець (розпорядник) бази персональних даних повинен забезпечити певний рівень гарантій захисту даних про фізичну особу, так як це інформація з обмеженим доступом, і оброблятися вона повинна, відповідно до статті 8 закону «Про захист інформації в інформаційно-телекомунікаційних системах» [8] із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю.

Загалом, результати проведеного аналізу дозволяють зробити висновок, що станом на червень 2011 року нормативно-правове забезпечення суспільних відносин в Україні щодо захисту персональних даних вимагає термінового прийняття ряду підзаконних нормативно-правових актів, що регламентують процедури обробки персональних даних в інформаційно-телекомунікаційних системах. Відповідно складність та багатоплановість поставленої задачі

потребує тісної співпраці різних законодавчих та виконавчих органів влади країни. У свою чергу, адміністрація вищого навчального закладу має вирішити низку складних, матеріально витратних організаційних і програмно-технічних заходів щодо приведення процесів функціонування інформаційно-комунікаційної системи у відповідність вимогам чинного законодавства.

Література

1. Конвенція ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» [Електронний ресурс]. Режим доступу до статті: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=994_326
2. Закон України «Про захист персональних даних» [Електронний ресурс]. Режим доступу до статті: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2297-17
3. Закон «Про інформацію» [Електронний ресурс]. Режим доступу до статті: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2657-12
4. Указ Президента України №390/2011 «Про Положення про Державну службу України з питань захисту персональних даних» [Електронний ресурс]. Режим доступу до статті: http://www.president.gov.ua/documents/13358.html
5. «Отчет Securit Analytics об утечках корпоративной информации и персональных данных за 2010 год» [Електронний ресурс]. Режим доступу до статті: http://www.securit.ru/press/news/?id=120
6. «Глобальное исследование утечек конфиденциальной информации 2010» [Електронний ресурс]. Режим доступу до статті: http://www.infowatch.ru/report/462
7. Наказ МОНмолодьспорт №291 «Про запровадження у 2011 році у вищих навчальних закладах експерименту «Електронний вступ 2011» від 28.03.11 року [Електронний ресурс]. Режим доступу до статті: http://osvita.ua/legislation/Vishya_osvita/17719
8. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [Електронний ресурс]. Режим доступу до статті: http://www.ucrf.gov.ua/uk/doc/laws/1147239096/

Надійшла: 13.06.2011 р.

Рецензент: д.т.н., проф. Литвиненко О.Є.