УДК 343.1:65.012.8
DOI https://doi.org/10.32782/2524-0374/2021-1/49

УДОСКОНАЛЕННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ, ТЕЛЕКОМУНІКАЦІЙНИХ ТА ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

IMPROVING THE INFORMATION PROTECTION SYSTEM IN INFORMATION, TELECOMMUNICATION AND INFORMATION-TELECOMMUNICATION SYSTEMS

Погорілецька А.В., старший викладач
кафедри кримінально-правових дисциплін
Криворізький факультет
Національного університету «Одеська юридична академія»

Бобошко О.М., старший викладач
кафедри кримінально-правових дисциплін
Криворізький факультет
Національного університету «Одеська юридична академія»

Стаття присвячена дослідженню проблеми захисту інформації в інформаційних, телекомунікаційних інформаційно-телекомунікаційних системах. Проведено аналіз понять «інформація», «інформаційна система», «телекомунікаційна система», «інформаційно-телекомунікаційна система». Визначено перелік інформації, яка охороняється відповідно до законодавства України в обов'язковому порядку.

Досліджено порядок функціонування інформаційної системи роботи державних органів влади і стан захисту інформації в цих інформаційних системах, що дає нам можливість визначити наявні проблеми, які потребують невідкладного вирішення. Визначено основні проблеми правового захисту інформації, що зберігається на електронних носіях і підписується за допомогою електронного підпису.

Обґрунтовано, що окремі положення чинного законодавства не забезпечують достатній рівень захищеності інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах.

Проаналізовано правозастосовну практику судів при вирішенні питання щодо заволодіння невідомими особами даних, що можуть бути використані при персоніфікації особи шляхом підтвердження засобами ідентифікатору (СМС повідомлення із кодом) електронного підпису або після автентифікації з використанням «кваліфікованого електронного цифрового підпису (ЕЦП), BankID, MobileID».

Досліджено національну правозастосовну практику в рамках оцінювання судом доказів винуватості особи, при підписанні договору після підтвердження засобами ідентифікатору (СМС повідомлення з кодом) електронного підпису. Визначено проблемні аспекти доказування підписання даних договорів.

Робиться висновок про необхідність удосконалення національного законодавства, з огляду на досліджені в статті проблемні аспекти регламентації вдосконалення системи захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах.

Акцентується увага, що забезпечення інформаційної безпеки – це комплексний засіб, який потребує постійного вдосконалення методів і способів захисту даних, підвищення рівня знань учасників процесу й розпорядників інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем.

Ключові слова: інформація, інформаційна система, телекомунікаційна система, інформаційно-телекомунікаційна система, електронний цифровий підпис, розпорядник системи, інформаційна безпека.

The article is devoted to the research of the problem of information protection in informative, telecommunicative information and telecommunication systems. The analysis of the concepts "information", "information system", "telecommunication system", "informative and telecommunicative system" is carried out. The list of information that is protected in accordance with the legislation of Ukraine in a mandatory manner is determined.

The order of functioning of the information system of the work of state authorities and the state of information protection in these information systems is studied, which gives us the opportunity to identify existing problems that need immediate solution. The main problems of legal protection of information stored on electronic media and signed with an electronic signature are identified.

It is substantiated that certain provisions of the existing legislation do not provide a sufficient level of information security in information, telecommunication and information-telecommunication systems.

The law enforcement practice of courts in resolving the issue of acquisition by unknown persons of data that can be used in personal identification by means of identification (SMS message with code) of electronic signature or after authentication using "qualified electronic digital signature" (EDS), BankID, MobileID is analyzed.

The national law enforcement practice in the framework of the court's assessment of the evidence of a person's guilt, when signing a contract after confirmation by means of an identifier (SMS message with a code) of an electronic signature, has been studied. The problem aspects of signing confirmation of these agreements are identified.

The conclusion is made about the need to improve the national legislation in view of the problematic aspects of the regulation of the improvement of the information protection system in information, telecommunication and information-telecommunication systems studied in the article.

Emphasis is placed on the fact that information security is a comprehensive tool that requires constant improvement of methods and ways of data protection, increasing the level of knowledge of process participants and managers of information, telecommunications and information and telecommunications systems.

Key words: information, information system, telecommunication system, information and telecommunication system, electronic digital signature, system administrator, information security.

Сучасні інформаційні технології впроваджуються сьогодні в усі сфери суспільного життя, що, у свою чергу, спрощує доступ до певних сервісів чи інформаційних ресурсів, прискорюючи отримання необхідної інформації учасниками інформаційних процесів. Поступово інформаційні технології впроваджуються в правовий сектор нашого життя. Так, електронні сервіси отримання довідки та послуги призводять до спрощення отримання сервісу адміністративних послуг для громадян, прискорюючи отримання чіткого результату за персональною, банківською чи адміністративною послугою в більш короткі строки.

Українською державою вибрано чіткий вектор на створення нового формату інформаційних державних послуг, які можливо отримати, користуючись створеними державою

інформаційними платформами, вхід до яких можливий за допомогою ідентифікації користувача. При цьому створюється значний комплекс баз даних інформації користувачів, що стосується персональних даних, пов'язаних із медичною, технічною, освітньою, банківською та іншими сферами. При цьому сервіси створюються, використовуючи спрямований вид інформації, робота з якою вимагає певного правового врегулювання й захисту.

Правовими питаннями понять «інформація», «інформаційна система», «телекомунікаційна система», «інформаційно-телекомунікаційна система» займалася велика кількість авторів, доробки яких висвітлено в працях І. Арістової, П. Біленчука, Р. Калюжного, Т. Костецької, Б. Кормича, А. Марущака та ін.

Поняття «інформація» висвітлюється в українському законодавстві в Законі України «Про інформацію» в статті 1, у якій визначено інформацію через поняття даних чи відомостей, що можуть бути збережені на матеріальному чи електронному носії. Ця стаття під захистом інформації розуміє певний комплекс правових, технічних, організаційних методів і засобів, які забезпечують непорушність, цілісність і збереження інформації [1].

Сьогодні інформаційні ресурси зберігаються в банках певних даних, при цьому від утримувача інформації вимагають відповідного рівня захищеності інформації, що створює певні правові гарантії як права на інформацію, так і права на захист інформації, що зберігається в розпорядника. Державою створено правовий механізм отримання інформації. Так, залежно від виду інформації виникає відповідний механізм права на цю інформацію або права на доступ до інформації. Правові норми Закону України «Про інформацію» не дозволяють обмежувати право особи щодо застосування не заборонених законом джерел і форм збирання інформації.

Загалом інформація, що створена або зібрана за певною ознакою, може утворювати інформаційну систему, яка являє собою сукупність методів збирання, передачі, перетворення й упорядкування інформації за певною ознакою. Вочевидь, застосування певних програмних і технічних засобів будуть перетворювати інформаційну систему на телекомунікаційну систему, поняття якої визначено в статті 1 Законі України «Про захист інформації в інформаційно-телекомунікаційних системах» як синтез програмних і технічних засобів, що застосовуються для передавання або приймання певної системи у формі звуків, зображень, що застосовуються для обміну інформацією.

Український законодавець визначає види інформації, використовуючи прийом поділу інформації, виходячи з її змісту. Ці види інформації визначено в статті 10 Закону України «Про інформацію», однак варто звернути увагу, що перелік інформації, наведений у цій статті, не є вичерпним, залежно від виду інформації існують правові режими й механізми захисту інформації. Так, наприклад, інформація про фізичну особу, яка визначена в статті 11 вищезазначеного Закону, регулюється й Законом України «Про захист персональних даних», який визначає механізми, спрямовані на захист прав особи, пов'язаних із його персональними даними. У Законі чітко визначено об'єкти захисту, перераховано особливі вимоги до обробки персональних даних, надано роз'яснення щодо порядку доступу до персональних даних [2]. Отже, правові механізми захисту видів інформації за змістом певною мірою врегульовані законодавчо, однак у користувачів інформаційно-телекомунікаційних систем виникають певні проблеми щодо функціонування електронних кабінетів певних систем.

Сьогодні громадяни України можуть отримати доступ до електронних баз даних, на яких зберігається певного роду інформація. Класичним прикладом у цьому випадку може бути користування дуже зручним сервісом системи BankID Національного банку України, яка створена для надання певного сервісу щодо отримання громадянами України чітких послуг від державних, фінансових, банківських, освітніх установ шляхом дистанційної персоніфікації запитувача послуги. З одного боку, ми отримали сервіс швидкої послуги, яка не потребує відвідування певної установи для отримання, наприклад, довідки, але, з іншого боку, виникли проблеми незахищеності цього сервісу й відсутності системи знань осіб щодо власних механізмів захисту своїх електронних даних від шахраїв і зловмисників, які виникають через технічну необізнаність особи щодо вжиття заходів власної безпеки.

Значних успіхів з питань надання певних інформаційних сервісів досягнуто за рахунок реалізації державного проекту «Дія», за допомогою якого розширено перелік послуг, що можна отримати онлайн від органів державної влади й органів місцевого самоврядування. Цей сервіс надає послуги за відповідними тематичними напрямами, створюючи діалог між державою та громадянином, державою та бізнесом. При цьому розробники «Дії» стверджують, що збирання даних про суб'єкта відбувається на низькому рівні, застосовуючи сервіси шифрування для передачі даних, що створює високий рівень захищеності від кібератаки.

Сучасний рівень захищеності інформаційних систем та інформаційно-технологічних систем досяг значного рівня захищеності, однак вразливим залишається технічний засіб і режими захищеності технічних засобів користувача, за допомогою яких відбувається персоніфікація особи у відповідних сервісах держави чи установи.

Під час аналізу правозастосовної практики українських судів при вирішенні питання щодо визнання недійсними договорів, які укладені при заволодінні невідомими особами даними, що використовувалися при персоніфікації особи шляхом підтвердження засобами ідентифікатора (СМС повідомлення із кодом) електронного підпису або після автентифікації з використанням «кваліфікованого електронного цифрового підпису (ЕЦП), BankID, MobileID», ми дійшли висновку, що відсутній механізм надійного захисту технічного засобу, яким можуть заволодіти зловмисники з метою отримання доступу до персональних даних власника, наприклад, смартфона.

На жаль, аналіз наявних правопорушень щодо шахрайських дій із картковими рахунками осіб сьогодні говорить про відсутність механізму власної безпеки з боку особи, яка визнається потерпілою, наприклад, за правовими кваліфікаціями ст. ст. 185, 186, 190 Кримінального кодексу України. Так, при заволодінні злочинцем відкрито із застосуванням насильства смартфона потерпілого, із сім-карткою певного мобільного оператора з номером абонента, який є фінансовим для банківської картки, при отриманні доступу до мережі Інтернет зловмисники можуть, використовуючи викрадений мобільний телефон із зазначеною сім-картою на ім'я особи, отримати кредити в різних мікрофінансових установах.

При відновленні сім-картки за абонентським номером викраденого мобільного оператора з певним номером абонента, активувавши нову сім-картку за номером, потерпілі згодом отримують СМС-повідомлення щодо інформації про здійснення заявки для оформлення кредиту, які було погоджено фінансовою установою, і кошти особі перераховано на невідомі потерпілому рахунки, які зловмисники надали після погодження надати кредит особі. При цьому сама особа, що є потерпілою, не вжила належних заходів власного захисту своїх даних, які містяться в електронному кабінеті.

Вочевидь, велика кількість випадків, коли потерпілий уважає, що якщо ним не укладався кредитний договір у письмовій формі, то цей договір є таким, що не укладений. Однак це хибна думка, так як будь-який договір може бути укладеним в електронній формі за допомогою технічних і програмних засобів.

Стаття 11 Закону України «Про електронну комерцію» визначає порядок підписання електронного договору,

серед основних моментів якого є умови, за яких укладається цей договір в електронній формі, які визначені законодавством і можуть містити процедуру укладення цього договору, послідовність створення й підписання договору електронним підписом та інші умови цього договору. При цьому варто відзначити, що одна зі сторін надає пропозицію укласти договір (оферта), а друга сторона приймає цю пропозицію (акцепт) [3].

Класичним у цьому випадку є заповнення невідомими особами анкетних даних до кредитного договору, які містять часткові відповідності персональних даних особи, у якої викрадено технічний засіб комунікації з активованим додатком Приват24. Дані з приводу проведеної персоніфікації банком виявляються частково актуальними, якщо власником карткового рахунку АТ «Приватбанк» надано останні актуальні відомості щодо себе, однак у більшості випадків в особистому кабінеті користувачів банківських послуг інформація міститься застаріла й не відповідає актуальним персональним даним особи, доступ до карткового рахунку якої отримано невідомими особами. Також варто звернути увагу на те, що відповідь особі, яка бажає укласти договір, у цьому випадку надається різними способами, серед яких – СМС-повідомлення або повідомлення на електронну пошту; заповнена заява про прийняття пропозиції, що підписується в електронній формі.

При цьому варто звернути увагу на те, що для доказової бази винуватості чи невинуватості особи, яка уклала чи не укладала договір в електронній формі, варто витребувати від керівника фінансової установи такі копії документів:

- роздруківку послідовності дій при заповненні й реєстрації особи на сайті надання послуг з розшифровкою та часом послідовних дій особи на сайті;
- роздруківку анкети, яка заповнювалася потерпілим чи невідомою особою при отриманні кредиту;
- роздруківку кредитного договору;
- інформацію щодо перерахунку фінансовою установою коштів на зазначений розрахунковий рахунок, отриманих за кредитним договором коштів;
- інформацію, на чиє ім'я відкрито рахунок, на який фінансова установа здійснила перерахування коштів, отриманих за кредитним договором.

При отриманні цієї інформації від мікрофінансової установи варто звернути увагу на аналіз документів і чітку невідповідність щодо місця знаходження потерпілої особи й IP-адреси місця знаходження технічного засобу при заповненні заявок для отримання кредитних коштів, номера рахунку, на який перераховано кошти кредитною установою.

Але є певні обставини, про які весь час забувають користувачі банківських карток та електронних додатків Приват24, а саме: при відкритті рахунку в банківській установі особу повідомляють про дотримання заходів безпеки при роботі з карткою чи електронним додатком. Так, у разі викрадення картки власник останньої зобов'язаний негайно повідомити установу про крадіжку або зникнення картки, при цьому ризик щодо дій, які будуть відбуватися до повідомлення власника картки установи банку, несе власник картки. На жаль, цей пункт договору наявний у багатьох договорах банків з користувачами карток. Однак не завжди власник підозрює про вибуття з його володіння картки чи технічного засобу (смартфона), у якому активовано роботу електронного сервісу розпорядження рахунком, що не дає можливості з боку власника картки вчасно повідомити банківську установу щодо ймовірності шахрайських дій стосовно карткового рахунку власника картки.

У свою чергу, відділи безпеки банку після проведення аналізу дій з картковим рахунком у певний проміжок часу можуть дійти висновку щодо шахрайських договорів, які здійснені невідомою особою від імені власника картки, використовуючи його персональні дані. При цьому варто зауважити, що тільки після отримання низки доказів за шахрайським договорами, укладеними в електронній формі, ми можемо говорити про розмір збитків, завданих потерпілому чи фінансовій установі.

У зв'язку з проблемами, які існують при роботі з електронними сервісами під час отримання кредитних коштів, укладаючи електронні договори на відстані, шляхом використання персональної інформації власника карткового рахунку, яка міститися в електронних кабінеті банківської установи, виникає необхідність удосконалення національного законодавства з огляду на проблемні аспекти системи захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах.

При цьому вважаємо, що забезпечення інформаційної безпеки – це комплексний засіб, який потребує постійного вдосконалення методів і способів захисту даних, підвищення рівня знань учасників процесу й розпорядників інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем. Тому перспективні напрямки дослідження системи захисту інформаційно-телекомунікаційних систем варто продовжити в наступних дослідженнях авторів.

ЛІТЕРАТУРА

1. Про інформацію : Закон України № 2658-XII / *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 28.01.2021).
2. Про захист персональних даних : Закон України № 2297-VI / *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 28.01.2021).
3. Про електронну комерцію : Закон України № 675-VIII / *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/675-19#Text (дата звернення: 28.01.2021).