АНАЛІЗ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В ЕЛЕКТРОННОМУ УРЯДУВАННІ

Марія Мандрона, Олександр Поліщук

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

In the paper considers features of e-government system. There are analyzes the essence and content of information security at various levels of government. It was found the main remedies that do are used to create mechanism of ensuring safety in the system of e-governance.

Keywords: e-government, information, information security system.

Використання технологій електронного урядування (ЕУ) є важливим фактором, що дає змогу забезпечити вирішенню проблем української держави, таких як: непрозорість, закритість, високий рівень корумпованості органів влади; формування механізмів децентралізації, демократичного контролю та участі громадян у розробці та реалізації державної політики; повернення довіри громадян до інститутів та посадовців органів державної влади та місцевого самоврядування.

Основними цілями ЕУ є [1-3]:

• підвищення якості та доступності державних послуг для громадян та бізнесу, спрощення процедур і скорочення адміністративних витрат;

• підвищення якості управлінських процесів, контроль за результативністю та ефективністю діяльності органів державної влади та органів місцевого самоврядування;

• забезпечення відкритості інформації про діяльність органів державної влади й місцевого самоврядування, розширення доступу до неї та надання можливості безпосередньої участі людини та інститутів громадянського суспільства в процесах підготовки й експертизи проектів політико-адміністративних рішень.

Впровадження ЕУ робить систему державного управління більш уразливою з боку різного роду загроз: кіберзлочинності, кібертероризму, кібервійн, проведення спеціальних інформаційних операцій, розповсюдження недостовірної інформації, маніпулювання свідомістю громадян тощо. Тому обов'язковою підсистемою сучасних інформаційно-телекомунікаційних систем є підсистеми захисту інформації, що застосовуються в електронному урядуванні.

Мета роботи полягає в аналізі систем захисту електронного урядування.

Аналізуючи напрями та сутність забезпечення інформаційної безпеки у внутрішньо системному функціонуванні органів виконавчої влади можна сказати, що їх характеризує сама компетенція, котра пов'язана із виконанням покладених на них державою, функцій і завдань. До характеристик, що дають змогу описати дану систему належать такі [4]:

✓ доступність – можливість за прийнятний час отримати необхідну інформаційну послугу будь-яким суб'єктом виконавчої влади;

✓ цілісність – актуальність і несуперечливість інформації, її захищеність від руйнування та несанкціонованої зміни;

✓ конфіденційність – захист від несанкціонованого ознайомлення.

Коли ж розглядати сутність та зміст інформаційної безпеки, то вони проявляються по-особливому на кожному з рівнів системи органів влади, зокрема на [2]:

– стратегічному (загальнодержавному);

– тактичному (органів влади, установ тощо);

– оперативному (структурних підрозділів органів державної влади, місцеві органи виконавчої влади, провідне місце серед яких посідають місцеві державні адміністрації).

Таким чином, можна говорити і про прояви інформаційної безпеки у самому процесі її забезпечення. У зв'язку з цим слід виділити такі її рівні:

▪ *законодавчий та нормативно-правовий* – закони, нормативно-правові акти, тощо;

- *адміністративний* – дії загального характеру, що вживаються органами виконавчої влади;
- *процедурний* – конкретні процедури забезпечення інформаційної безпеки;
- *програмно-технічний* – конкретні технічні заходи забезпечення інформаційної безпеки.

Нижче зазначені основні засоби захисту [4, 5], які використовуються для створення механізму забезпечення безпеки.

Технічні засоби реалізуються у вигляді електричних, електромеханічних та електронних пристроїв. Уся сукупність технічних засобів поділяється на апаратні й фізичні.

Програмні засоби являють собою програмне забезпечення, спеціально призначене для виконання функцій захисту інформації.

Організаційні засоби – це організаційно-технічні й організаційно-правові заходи, які здійснюються в процесі створення та експлуатації обчислювальної техніки, апаратури телекомунікацій для забезпечення захисту інформації. Організаційні заходи охоплюють усі структурні елементи апаратури на всіх етапах їх життєвого циклу.

Морально-етичні засоби реалізуються у вигляді різних норм, які склалися традиційно або складаються в міру поширення обчислювальної техніки й засобів зв'язку в суспільстві. Ці норми здебільшого не є обов'язковими, як законодавчі заходи.

Законодавчі засоби захисту визначаються нормативно-правовими актами, якими регламентуються норми та правила користування, обробки й передачі інформації обмеженого доступу. За порушення цих правил встановлюються відповідальність.

Технології захисту інформації передбачають впровадження технічних рішень та технічних засобів захисту складових інформаційної інфраструктури. До них належить:
антивірусне програмне забезпечення; системи управління доступом; міжмережеві екрани; системи аутентифікації (смарт-карти, біометрічні системи тощо); системи виявлення вторгнення; управління політиками; сканування на наявність уразливих місць; системи криптографічного захисту; механізми фізичного захисту.

Що стосується боротьби з кіберзлочинами, то сюди відносяться системи ідентифікації та аутентифікації користувачів, криптографічного перетворення інформації, антивірусного захисту, аудиту та моніторингу подій в мережі.

У сукупності отримані результати аналізу дали змогу з'ясувати механізми забезпечення захисту інформації в електронному урядуванні, а також визначити напрями удосконалення систем електронного урядування в цілому.

Література

1. Державна програма інформатизації та комп'ютеризації вищих навчальних закладів I – II рівня акредитації на 2005 – 2008 роки [Текст] : Постанова Кабінету Міністрів України від 8 вересня 2004 р. N 1182 // Офіційний вісник України. – 2004. – № 36. – С. 40.
2. Державна програма інформатизації та комп'ютеризації вищих навчальних закладів I – II рівня акредитації на 2005 – 2008 роки [Текст] : Постанова Кабінету Міністрів України від 8 вересня 2004 р. N 1182 // Офіційний вісник України. – 2004. – № 36. – С. 40.
3. Порядок застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності [Текст]: Постанова Кабінету Міністрів України від 28 жовтня 2004 р. №1452 // Офіційний вісник України.– 2004. – № 44. – С. 123
4. Кукарін О.Б. Електронний документообіг та захист інформації: навч.посібн. / О.Б. Кукарін. – К: НАДУ, 2015. – 84 С.
5. Опорний конспект лекцій. [Дзюба С.В., Жиляєв І.Б., Полумієнко С.К, Рубан І.А., Семенченко А.І.] /За ред. А.І. Семенченка. – Київ, 2012. – 264 с.