Основи інформаційної безпеки. Комплексна система захисту інформації:

СТРУКТУРА, ВСТАНОВЛЕННЯ ТА ПІДТРИМКА ФУНКЦІОНУВАННЯ. ПОРЯДОК ДОСТУПУ ДО АВТОМАТИЗОВАНОЇ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ «ДЕРЖАВНИЙ РЕЄСТР ВИБОРЦІВ»

Литвинюк А.А.,
заступник начальника управління технологічного та програмного забезпечення функціонування Реєстру Служби розпорядника Державного реєстру виборців

Основи інформаційної безпеки

Розвиток держави в сучасних умовах пов'язаний передусім із запровадженням інформаційних технологій. Саме розвиток інформаційної сфери, зокрема інформаційних технологій та телекомунікацій, створює сприятливі умови для суспільного прогресу. На сьогодні державна інформаційна політика спрямована на стимулювання поглиблення процесів інформатизації, оновлення і створення нових сучасних телекомунікацій.

Використання автоматизованих систем в управлінні підвищує якість і швидкість обробки та передачі інформації, потік якої постійно зростає. Інформатизація в органах державного управління забезпечує його раціональність і ефективність.

Проте розвиток інформаційної сфери супроводжується і появою принципово нових загроз інтересам особистості, суспільства, держави, її національній безпеці та зростанням рівня небезпеки вже відомих.

Широкі можливості інтеграції даних в автоматизованих системах органів державної влади забезпечують централізоване накопичення інформаційних даних з різних сфер життєдіяльності держави і суспільства. Але реалізація та використання таких можливостей пов'язана значною мірою із суттєвим зростанням ризику ураження, знищення, спотворення інформації та її несанкціонованого розповсюдження.

Серед загроз, що сформувалися у процесі інформаційної революції, варто виокремити розробку та вдосконалення засобів впливу на інформаційну інфраструктуру та пов'язане з цим падіння рівня захищеності державних інформаційних ресурсів. Інформаційно-телекомунікаційні системи вразливі для атак комп'ютерних вірусів, втручання сторонніх суб'єктів з метою підміни, спотворення, знищення інформації та інших видів комп'ютерної злочинності. Нейтралізація зазначених загроз потребує формування потужної системи протидії.

Існують такі джерела загроз:

- протизаконна діяльність політичних і економічних структур у сфері формування, поширення і використання інформації;
- неправомірні дії представників державних структур, що призводять до порушення законних прав громадян і організацій в інформаційній сфері;
- порушення встановлених регламентів збору, обробки і передачі інформації;
- навмисні дії і ненавмисні помилки персоналу інформаційних систем;
- відмови технічних засобів і збої програмного забезпечення в інформаційних і телекомунікаційних системах.

Одна з найважливіших проблем безпеки використання інформації пов'язана із забезпеченням управлінської діяльності органів державної влади. Більшість рішень, що приймаються державними структурами, мають інформаційну основу. З цих позицій інформаційно-аналітичне забезпечення органів державного управління доцільно розглядати як один із визначальних чинників ефективності і безпеки управління.

У зв'язку з високим державним статусом операцій з обміну, обробки та накопичення інформації інформаційна безпека та захист інформації в інформаційно-аналітичних системах набувають особливої ваги.

В Україні сформовано доволі потужну нормативно-правову базу щодо забезпечення інформаційної безпеки.

Загальні принципи функціонування інформаційної сфери, зокрема у сфері інформаційної безпеки, закріплені Законом України «Про інформацію». Відносини у сфері інформаційної безпеки регулюються Законами України «Про державну таємницю», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про Національну систему конфіденційного зв'язку» тощо.

Комплексна система захисту інформації

Державний реєстр виборців (далі – Реєстр) – автоматизована інформаційно-телекомунікаційна система (банк даних), призначена для зберігання, обробки даних, які містять передбачені Законом України «Про Державний реєстр виборців» (далі – Закон) відомості, та користування ними, створена для забезпечення державного обліку громадян України, які мають право голосу відповідно до статті 70 Конституції України.

Відповідно до статті 3 Закону однією з основних засад ведення Реєстру є його захищеність.

Захищеність Реєстру передбачає забезпечення захисту бази даних Реєстру від несанкціонованого доступу та зловживання доступом, від незаконного використання

персональних даних Реєстру, порушення цілісності бази даних Реєстру та його апаратного чи програмного забезпечення шляхом застосування засобів технічного захисту інформації, відповідних організаційно-правових заходів та встановлення юридичної відповідальності за порушення захищеності Реєстру.

Безпека інформаційної системи забезпечується відповідно до постанови Кабінету Міністрів України від 29 березня 2006 року № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах».

Правовою основою створення комплексної системи захисту інформації в автоматизованій інформаційно-телекомунікаційній системі «Державний реєстр виборців» є Закони України «Про захист інформації в інформаційно-телекомунікаційних системах» та «Про Державний реєстр виборців».

Таким чином, держава гарантує захист інформації про виборців шляхом встановлення Законом чітких вимог щодо її захисту.

Комплексна система захисту інформації в автоматизованій інформаційно-телекомунікаційній системі «Державний реєстр виборців» (далі – КСЗІ) призначена для захисту даних (інформаційних ресурсів) автоматизованої інформаційно-телекомунікаційної системи «Державний реєстр виборців» (далі – Система) від знищення, підміни, спотворення, спроб несанкціонованого доступу і копіювання та забезпечення доступу користувачів, а саме:

– захисту конфіденційності, цілісності, доступності конфіденційної інформації (в тому числі персональних даних), що циркулює в Системі, розпорядником якої є державний орган;

– захисту конфіденційності, цілісності та доступності технологічної інформації щодо функціонування Системи, яка повинна бути доступна тільки уповноваженому персоналу, що забезпечує управління програмними та технічними засобами Системи;

– захисту цілісності та доступності відкритої інформації, що циркулює в Системі.

Метою створення КСЗІ є забезпечення захисту інформації, що обробляється, передається та зберігається в межах автоматизованої інформаційно-телекомунікаційної системи «Державний реєстр виборців», від несанкціонованого доступу, порушення конфіденційності, несанкціонованої модифікації та знищення, а також забезпечення доступності зазначеної інформації для авторизованих користувачів, а саме:

– забезпечення захисту при веденні загальнодержавного обліку виборців відповідно до Закону;

– забезпечення захищеності бази даних Реєстру від несанкціонованого доступу та від незаконного використання персональних даних Реєстру;

– забезпечення цілісності відомостей Реєстру шляхом захисту бази даних Реєстру з повним обсягом відомостей про виборця, їх коректності;

– забезпечення доступності відомостей Реєстру, що містяться в базі даних Реєстру;

– забезпечення захисту при веденні та зберіганні персональних даних Реєстру;

– забезпечення захисту при поновленні відомостей Реєстру під час періодичної або ініціативної актуалізації бази даних Реєстру;

– забезпечення захисту від порушень цілісності апаратного чи програмного забезпечення Реєстру шляхом застосування засобів технічного захисту інформації, відповідних організаційно-правових заходів.

До складу корпоративної телекомунікаційної мережі системи та системи захисту інформації входять:

- технічні елементи корпоративної мережі, розміщені у Службі розпорядника Реєстру та органах ведення Реєстру;
- канали передачі даних відповідного оператора зв'язку;
- локальні мережі Служби розпорядника Реєстру та органів ведення Реєстру;
- програмно-технічні засоби захисту інформації, що розміщуються у Службі розпорядника Реєстру та органах ведення Реєстру. Частково засоби захисту інтегровані в телекомунікаційне обладнання, частково являють собою окремі елементи.

Комплексна система захисту інформації Системи має дворівневу архітектуру і об'єднує комплекси засобів захисту рівня розпорядника Реєстру та 755 місцевих органів ведення Реєстру.

Створення КСЗІ АІТС «Державний реєстр виборців» передбачає застосування засобів технічного та криптографічного захисту інформації, що виконують функції:

1) захисту інформації при передаванні каналами зв'язку;
2) автентифікації;
3) керування захистом;
4) моніторингу загроз безпеки;
5) міжмережних екранів та систем виявлення вторгнень;
6) антивірусного програмного забезпечення;
7) програмно-апаратних засобів ідентифікації (носіїв ключової інформації) із системою централізованого керування ними.

З метою забезпечення цілісності та достовірності електронних копій баз даних Реєстру, що передаються політичним партіям (стаття 24 Закону України «Про Державний реєстр виборців»), використовується процедура засвідчення їх цифровим підписом.

Система забезпечує збереження інформації або можливість її відновлення (станом на момент створення останньої резервної копії бази даних або на момент створення останнього архівного журналу) у разі:

- відключення живлення комп'ютера, на якому працює користувач;
- відключення струму серверної компоненти.

Захист інформації реалізується з використанням апаратних та програмних засобів, а також організаційних

заходів, спрямованих на керування засобами захисту, регламентацію дій користувачів і контроль за цими діями.

Організаційні заходи, що здійснюються відділами ведення Реєстру, повинні включати:

- обладнання приміщень, якими забезпечуються відділи ведення Реєстру, системою автоматичної пожежної сигналізації та охоронною системою сигналізації;
- застосування до приміщень, якими забезпечуються відділи ведення Реєстру, правил, встановлених для приміщень з обмеженим доступом. Статус таких приміщень встановлюється органом, що утворив відділ ведення Реєстру;
- визначення керівником відділу ведення Реєстру переліку осіб, які мають право доступу до цих приміщень;
- виконання інших вимог до приміщень, встановлених постановою Комісії від 20 грудня 2007 року № 572;
- визначення керівником відділу ведення Реєстру особи, яка здійснює обов'язки адміністратора безпеки;
- організацію обліку та збереження інформаційних матеріалів, що містять персональні дані як на паперових, так і на електронних носіях;
- регламентування надання інформації, яка містить персональні дані, особам, що не є працівниками відділів ведення Реєстру;
- проведення інструктажу працівників відділів ведення Реєстру з питань захисту інформації;
- встановлення контролю за програмним і технічним забезпеченням, що використовується працівниками відділів ведення Реєстру, його ліцензійною чистотою.

Технічні заходи забезпечують збереження інформації на зовнішніх носіях, використання джерел безперебійного живлення, можливість резервування інформації, що зберігається на жорстких дисках робочих станцій, організацію та підтримку захищеності телекомунікаційної мережі Реєстру. Технічні засоби використовуються для здійснення доступу до бази даних Реєстру.

Програмними засобами захисту інформації вважаються налаштування політики безпеки операційних систем робочих станцій, встановлення антивірусного захисту, розподіл повноважень користувачів комп'ютерної мережі відділу ведення Реєстру на рівні системного програмного забезпечення.

Доступ до бази даних Державного реєстру виборців

Закон України «Про Державний реєстр виборців» визначає чітке розмежування доступу органів Реєстру до відомостей про виборців у базі даних автоматизованої інформаційно-телекомунікаційної системи «Державний реєстр виборців». Відповідно до статті 14 Закону орган адміністрування Реєстру не має права доступу до бази даних Реєстру. Проте ці органи для виконання своїх повноважень мають доступ до інших елементів системи, таких як електронна пошта та інформаційно-довідкові веб-ресурси.

Стаття 15 Закону встановлює межі доступу органу ведення Реєстру до бази даних Реєстру. Так, орган ведення Реєстру має доступ до всіх записів Реєстру в режимі читання.

Орган ведення Реєстру має доступ в режимі записування до персональних даних Реєстру стосовно виборців, виборча адреса яких знаходиться в межах території, на яку поширюються повноваження цього органу. Орган ведення Реєстру в Міністерстві закордонних справ України має доступ у режимі записування до персональних даних Реєстру стосовно виборців, які проживають чи перебувають за межами території України.

Стосовно повноважень і прав доступу до інформації, що зберігається та циркулює на рівні органу ведення Реєстру, визначають такі ролі:

Адміністратор безпеки здійснює адміністрування операційних систем та іншого програмного забезпечення, що функціонує на автоматизованих робочих місцях відділів ведення Реєстру, контролює відповідність настроювань програмних та технічних засобів прийнятій політиці безпеки, здійснює загальний контроль за станом безпеки у відділі ведення Реєстру (контролює дотримання користувачами вимог інструкцій та нормативних документів, здійснює аналіз системних журналів).

Оператори – користувачі рівня відділу ведення Реєстру. Права доступу цих користувачів повинні дозволяти читання та модифікацію записів бази даних, які містять персональні дані в межах власного району, та обмежений доступ (читання) до всіх інших записів.

Обслуговуючий персонал. Має фізичний доступ до обладнання Системи у супроводі відповідних осіб.

Для забезпечення процедур ідентифікації/автентифікації користувачів Системи і подальшої авторизації їх у Системі використовуються програмно-апаратні засоби ідентифікації, які повинні зберігати атрибути доступу користувачів у захищеному вигляді.

Програмні та інші засоби доступу надаються персонально працівникам органу ведення Реєстру розпорядником Реєстру.

Для отримання доступу до бази даних Реєстру керівник органу ведення Реєстру невідкладно після призначення працівника цього органу подає розпоряднику Реєстру документи, визначені порядком доступу.

Після первинного формування бази даних Реєстру на етапі введення автоматизованої інформаційно-телекомунікаційної системи Реєстру розпорядник Реєстру забезпечує доступ органів ведення Реєстру до бази даних Реєстру.

На підставі поданих органами ведення Реєстру документів розпорядник Реєстру приймає рішення про надання доступу користувачам Реєстру до бази даних Реєстру.

Служба розпорядника Реєстру на підставі рішення розпорядника Реєстру та згідно з відомостями, зазначеними в поданій анкеті, створює обліковий запис користувача Реєстру та проводить його авторизацію в Системі.

При створенні облікового запису користувача Реєстру формуються його системні ідентифікатори: індивідуальні Ім'я користувача в Системі та Пароль – PIN-код. Зміст

Пароля та Ім'я користувача є конфіденційними і не можуть бути передані іншим особам.

Служба розпорядника Реєстру здійснює підготовку програмно-апаратного засобу ідентифікації – USB-ключа працівника органу ведення Реєстру та прив'язує його до відповідного облікового запису користувача Реєстру.

Працівники органів ведення Реєстру особисто отримують індивідуальний пакет доступу до бази даних Реєстру: PIN-код та USB-ключ, і несуть особисту відповідальність за їх використання і схоронність.

Програмно-апаратний засіб ідентифікації здійснює авторизацію користувачів у Системі шляхом під'єднання до комп'ютера через USB-порт та введення PIN-коду. Проте користувач отримує доступ до бази даних Реєстру, а відтак і можливість вчиняти дії щодо внесення до бази даних Реєстру нових записів, змін до персональних даних Реєстру, знищення записів бази даних Реєстру тільки за умови наявності авторизованого в системі іншого користувача цього ж відділу ведення Реєстру.