Технічний захист інформації в Службі безпеки України

Богдан Ткач

головний судовий експерт, Центр судових і спеціальних експертиз
Українського науково-дослідного інституту спеціальної техніки та судових експертиз
Служби безпеки України, м. Київ, Україна, e-mail: tbogdan2010@gmail.com

Технічний захист інформації є невід'ємною складовою системи інформаційної безпеки в державних установах. Створення технічного захисту інформації в державних установах пов'язано із використанням та зберіганням критично важливої інформації, зокрема, державної таємниці, конфіденційних даних, стратегічних документів тощо.

Ключові слова: *технічний захист інформації; автентичність інформації; несанкціоноване втручання; контроль доступу.*

Technical protection of i formatio in the Security Service of Ukraine

Bohdan Tkach

Technical information protection is an integral part of the information security system in government institutions. The creation of technical information protection in government institutions is associated with the use and storage of critically important information, in particular, state secrets, confidential data, strategic documents, etc.

Keywords: *technical information protection; authenticity of information; unauthorized interference; access control.*

Технічний захист інформації (далі — *ТЗІ*) є невід'ємною складовою системи інформаційної безпеки, особливо в такій державній установі, як Служба безпеки України. Під час роботи установ, підрозділів та органів Служби безпеки України, під час розв'язання оперативно-службових завдань, використовується та зберігається критично важлива інформація, зокрема, державна таємниця, конфіденційні дані, стратегічні документи тощо. ТЗІ в інформаційних системах і мережах як Служби безпеки України, так і в інших державних установах, здійснюється через різноманітні методи та засоби, які забезпечують конфіденційність, цілісність, доступність і автентичність інформації. Особлива важливість організації та виконання вимог ТЗІ в державних установах пов'язана із можливістю витоку важливої конфіденційної інформації технічними каналами.

Основні напрями захисту містять захист інформаційних систем і мереж ТЗІ шляхом упровадження апаратних та програмних засобів, їх фізичного захисту, здійснення моніторингу й аудиту, резервного копіювання та відновлення інформації, проведення освітніх заходів та тренувань персоналу.

Захист інформаційних систем і мереж ТЗІ шляхом упровадження апаратних та програмних засобів дає змогу контролювати доступ до інформаційних ресурсів (системи аутентифікації та авторизації), забезпечувати

шифрування даних під час передачі через мережу та зберігання.

Під час створення та експлуатації систем оброблення даних, телекомунікаційних систем і мереж як шляхи досягнення технічного захисту можна визначити:

- ідентифікацію й авторизацію користувачів шляхом затосування паролів, карток доступу, біометричних даних, токенів тощо для аутентифікації користувачів;
- контроль доступу, який полягає в розмежуванні прав доступу до інформаційних ресурсів, реалізації політик доступу, таких як принцип мінімальних привілеїв, щоб користувачі мали доступ лише до необхідної для них інформації;
- захист від несанкціонованого втручання у вигляді моніторингу та реагування на інциденти;
- установлення ліцензованого та сертифікованого програмного забезпечення для виявлення та блокування шкідливого програмного забезпеченнями, постійне оновлювання баз даних вірусів для забезпечення захисту від нових загроз.

Фізичний захист досягається шляхом упровадження:

- забезпечення безпеки обладнання, серверів та інших пристроїв;
- застосування контрольно-пропускних систем для обмеження доступу до службових приміщень;
- захисту від природних катастроф та інших фізичних загроз (пожежі, затоплення тощо).

Моніторинг і аудит дає змогу виявляти підозрілу активність, вразливості або випадки інцидентів.

Резервне копіювання та відновлення важливої інформації передбачає наявність планів відновлення після катастроф, щоб мінімізувати наслідки атак або збоїв.

Освітні заходи та тренування мають на меті: навчання співробітників основам кібербезпеки та правильному поводженню з інформацією; проведення тренінгів з виявлення фішингових атак та інших соціальних інженерних загроз.

Наведені вище заходи мають бути враховані під час створення комплексної стратегії захисту, що відповідає специфічним вимогам і загрозам для конкретної інформаційної системи або мережі установ, підрозділів та органів Служби безпеки України.

Під час організації ТЗІ необхідно дотримуватись вимог Українського законодавства щодо захисту інформації (наприклад, Закону «Про інформацію», Закону «Про захист інформації в інформаційно-телекомунікаційних мережах» та інші нормативні акти, зокрема внутрішньовідомчі).

Упровадження ТЗІ дає змогу установам, підрозділам та органам Служби безпеки України, а також державним установам відповідати вимогам законодавства; забезпечувати конфіденційність, цілісність та доступність інформації; підтримувати стандарти безпеки, затверджені державними органами.

Якщо більш ретельно розглядати питання законодавчого регулювання в Україні щодо ТЗІ, під час службової

діяльності в органах, установах та закладах Служби безпеки України необхідно спиратись на низку законів, підзаконних актів і державних стандартів, які визначають порядок захисту інформації від несанкціонованого доступу, витоку інформації, модифікації та інших загроз:

- гарантування права на захист персональних даних відповідно до ст. 32 Конституції України [1];
- гарантування права на збирання та захист інформації відповідно до ст. 34 Конституції України [1];
- визначення основних принципів державної політики у сфері інформації відповідно до ст. 3 Закону України «Про інформацію» [2];
- визначення порядку доступу до інформації відповідно до ст. 20 Закону України «Про інформацію» [2];
- регулювання питання забезпечення захисту інформації в інформаційних системах, визначаючи вимоги до технічних і організаційних засобів захисту, а також до контролю за безпекою інформаційних систем відповідно до ст. 8, 9 Закону України «Про захист інформації в інформаційно-комунікаційних системах» [3];
- визначення порядку охорони державної таємниці, класифікація інформації здійснюється згідно зі ст. 18 Закону України «Про державну таємницю» [4];
- визначення технічного захисту інформації як складової національної безпеки згідно зі ст. 7 Закону України «Про основи національної безпеки України» [5].

Технічний захист інформації в Україні регламентується підзаконними актами та нормативними документами у сфері ТЗІ, а саме:

- постановою Кабінету Міністрів України від 29.03.2006 р. № 373 «Про затвердження Порядку проведення державної експертизи у сфері технічного захисту інформації» [6];
- Національними стандартами та нормативними документами, а саме — ДСТУ 3396.1-96, визначаються загальні вимоги до ТЗІ.

Технічний захист інформації у Службі безпеки України, а також в інших державних установах України є важливою складовою інформаційної безпеки, що регулюється на державному рівні та відповідає міжнародним стандартам.

Роль ТЗІ в Службі безпеки України та інших державних установах України є надзвичайно важливою для забезпечення безпеки критично важливої інформації, підтримки стабільності та безперервності роботи державного апарату, а також для протидії сучасним кіберзагрозам. Ураховуючи постійний розвиток технологій та зростання кіберризиків, інвестування в сучасні технології захисту інформації та постійне вдосконалення систем безпеки є обов'язковими умовами для ефективної діяльності Служби безпеки України та інших державних установ.

Перелік джерел посилання

1. Конституція України : Закон України від 28.06.1996 р. № 254к/96-ВР (зі змін. та допов.). URL: https://constitution.in.ua/articles/32/ (дата звернення 03.04.2025).
2. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 03.04.2025).
3. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 03.04.2025).
4. Про державну таємницю : Закон України від 21.01.1994 р. № 3855-XII (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text/ (дата звернення: 03.04.2025).
5. Про основи національної безпеки України : Закон України від 19.06.2003 р. № 964-IV (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/964-15#Text/ (дата звернення: 04.04.2025).
6. Про затвердження Порядку проведення державної експертизи у сфері технічного захисту інформації : постанова КМУ від 29.03.2006 р. № 373. URL: https://zakon.rada.gov.ua/laws/show/373-2006-п#Text/ (дата звернення: 04.04.2025).