ЩОДО УДОСКОНАЛЕННЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ОРГАНАХ ДЕРЖАВНОЇ ВЛАДИ І МІСЦЕВОГО САМОВРЯДУВАННЯ ТА В ПРИВАТНОМУ СЕКТОРІ

Володимир Козак
Volodymyr.Kozak@gmail.com

Що ми маємо:

1. Застарілі принципи – захист інформації в інформаційних системах, а не забезпечення інформаційної безпеки в органах державної влади та місцевого самоврядування.
2. Держава визначає порядок захисту інформації в приватному секторі: втручання без відповідальності.

Важливо:

Реалізувати запровадження принципів забезпечення інформаційної безпеки в організаціях та установах публічного та приватного секторів, задекларовані керівними органами ЄС[1], зокрема:

- опрацювати мінімальні вимоги з інформаційної безпеки для публічного сектору;
- сприяти відповідальності у приватному секторі стосовно стану інформаційної безпеки;
- запроваджувати методи інформаційної безпеки, що базуються на оцінках ризиків;
- найширше використовувати міжнародні стандарти в сфері забезпечення інформаційної безпеки.

Пропозиції:

1. Стосовно забезпечення інформаційної безпеки в органах державної влади та місцевого самоврядування

Забезпечити реалізацію заходів з інформаційної безпеки в органах державної влади та їх контроль (аудит) з використанням сучасних підходів, визначених міжнародним стандартом ISO/IEC 27001[2], що включає:

[1] 1.JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 7.2.2013 JOIN(2013) 1 final http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf
2.Council Resolution of 28 January 2002 on a common approach and specific actions in the area of network and information security http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002G0216%2802%29
3.COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT. Accompanying the document Proposal for a Directive of the European Parliament and of the Council Concerning measures to ensure a high level of network and information security acrossthe Union https://netzpolitik.org/wp-upload/Cybersecurity-Impact-Assessment.pdf

[2] Див. наприклад Instructions on Implementing the Decree on Information Security in Central Government. Ministry of Finance. Finland. 2010
http://www.vm.fi/vm/en/04_publications_and_documents/01_publications/05_government_information_management/20101028Instru/vahti2b_2010netti.pdf

- організаційні заходи та заходи щодо адміністрування інформаційної безпеки,
- заходи щодо забезпечення безпеки інфраструктури інформаційних технологій (захист інформації в інформаційних системах) на основі визначення рівнів інформаційної безпеки:

Базовий рівень інформаційної безпеки – повинен бути реалізований в усіх без винятку органах державної влади та місцевого самоврядування. В усіх органах державної влади обробляється інформація та документи які належать до **публічної інформації** та/або **службової інформації** «що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень»[3].

Підвищений рівень інформаційної безпеки – повинен бути реалізований в органах державної влади та місцевого самоврядування або в підрозділах органів державної влади та місцевого самоврядування, де обробляється документи, інформація зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці[4], а також в підрозділах органів державної влади, на підприємствах та організаціях де використовуються великі обсяги інформаційних ресурсів, де необхідно забезпечити підвищені вимоги щодо цілісності, доступності та неспростовності.

Високий рівень інформаційної безпеки повинен бути реалізований в підрозділах, де обробляються документи та інформація, що містить державну таємницю.

2. Стосовно державно-приватного партнерства у сфері інформаційної безпеки в організаціях приватного сектору

На сьогодні відповідно до чинного законодавства приватні організації які здійснюють обробку *інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом*, повинні застосовувати комплексну систему захисту інформації, підтвердження відповідності якої здійснюється за результатами державної експертизи[5].

Оскільки законом встановлено надзвичайно широкий перелік інформації з обмеженим доступом, яка потребує захисту, але яка не відноситься до державних інформаційних ресурсів, вимога щодо створення комплексної системи захисту інформації та її державної експертизи стосується надзвичайно широкого переліку інформаційних систем організацій приватного сектору, що створює передумови для втручання державних органів у діяльність приватних підприємств та організацій.

---

[3] Див. пункт 1 частини 1 статті 9 Закону України «Про доступ до публічної інформації» http://zakon1.rada.gov.ua/laws/show/2939-17/print1390914525733723

[4] Див.пункт 2 частини 1 статті 9 Закону України «Про доступ до публічної інформації» http://zakon1.rada.gov.ua/laws/show/2939-17/print1390914525733723

[5] *«Державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством».* Стаття 8 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» http://zakon2.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80/print1383746845020769

На практиці організації приватного сектору, зокрема великі та середні організації, вже давно широко і цілком успішно використовують міжнародні стандарти забезпечення інформаційної безпеки в організаціях, ігноруючи положення застарілого за своїми принципами національного законодавства. Незалежна оцінка відповідності систем управління інформаційною безпекою (СУІБ) в Україні здійснюється лише органами, акредитованими в інших країнах[6]. При цьому базовий стандарт у сфері систем керування інформаційною безпекою ISO/IEC 27001 прийнято як національний у 2010 році[7].

Законом передбачено використання лише засобів захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за результатами **державної експертизи**[8].

Оскільки незалежна оцінка відповідності засобів захисту інформації шляхом сертифікації розвинута вкрай слабо[9], використання в інформаційних системах засобів захисту інформації, навіть вже сертифікованих в інших країнах, вимагає проведення **державної** експертизи цих засобів в Україні.

Напрямки розвитку:

Чітко законодавчо визначити, що приватні організації самостійно визначають заходи щодо забезпечення інформаційної безпеки виходячи з характеристик бізнесу та організації, її розташування, оцінених ризиків, наявних ресурсів та технологій.

В разі укладання договору з органами державної влади чи місцевого самоврядування, які передбачають обробку документів та інформації, необхідність захисту якої визначена законодавством приватними організаціями, умови обробки інформації в інформаційній системі визначаються органами державної влади та місцевого самоврядування (володільцем інформації) відповідно до договору з приватною організацією.

З метою забезпечення розвитку незалежної оцінки заходів щодо забезпечення інформаційної безпеки, відповідності систем управління інформаційною безпекою (СУІБ) в Україні необхідно:

---

[6] Станом на 06.10.2014 року в Україні немає жодного акредитованого у Національному агентстві з акредитації України органу з сертифікації систем менеджменту інформаційної безпеки (див. веб-сайт Національного агентства акредитації України http://naau.org.ua/reyestr-akreditovanix-oov/). Водночас протягом 2013 року понад десяток приватних організацій в Україні було сертифіковано органами з сертифікації систем управління інформаційною безпекою акредитованими закордонними органами з акредитації (див. Evolution of ISO/IEC 27001 certificates in Ukraine http://www.iso.org/iso/home/standards/certification/iso-survey.htm?certificate=ISO/IEC%2027001&countrycode=UA#countrypick)

[7] ДСТУ ISO/IEC 27001:2010 Інформаційні технології. Методи та засоби досягнення інформаційної безпеки. Системи керування інформаційною безпекою. Вимоги (ISOIEC 27001:2005, IDT)

[8] *«Для створення комплексної системи захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, використовуються засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації. Підтвердження відповідності та проведення державної експертизи цих засобів здійснюються в порядку, встановленому законодавством».* Стаття 8 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» http://zakon2.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80/print1383746845020769

[9] У 2014 році призупинено акредитацію останньої випробувальної лабораторії засобів технічного захисту інформації http://naau.org.ua/reyestr-akreditovanix-oov/

Запропонувати приватному сектору здійснювати інвестиції у розвиток інформаційної безпеки та співпрацю з органами державної влади, зокрема в рамках державно-приватного партнерства[10] стосовно:

- прийняття як національних міжнародних стандартів у сфері інформаційної безпеки, необхідних для розвитку механізмів самостійного забезпечення інформаційної безпеки в організаціях приватного сектору, зокрема незалежної оцінки систем управління інформаційної безпеки[11];
- створення незалежних органів з сертифікації систем керування інформаційною безпекою;
- прийняття як національних міжнародних стандартів у сфері інформаційної безпеки необхідних для незалежної оцінки засобів безпеки інформаційних технологій (засобів захисту інформації) та визнання незалежної оцінки таких засобів, вже проведеної відповідно до міжнародних стандартів органами сертифікації інших країн[12];
- створення незалежних органів із сертифікації засобів безпеки інформаційних технологій (засобів захисту інформації) та відповідних випробувальних лабораторій.

Здійснити заходи щодо приєднання спеціально уповноваженого центрального органу виконавчої влади з питань організації спеціального зв'язку та захисту інформації до Договору про визнання сертифікатів Загальних Критеріїв в сфері безпеки інформаційних технологій (Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security, July 2, 2014)[13].

---

[10] Закон України «Про державно-приватне партнерство» http://zakon2.rada.gov.ua/laws/show/2404-17/print1383746845020769

[11] ISO/IEC 27000:2014 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary
ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements
ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controlsISO/IEC 27003:2010 Information technology -- Security techniques -- Information security management system implementation guidance
Інші стандарти цієї серії див.
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_tc_browse.htm?commid=45306

[12] ISO/IEC 15408-1:2009 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model
ISO/IEC 15408-2:2008 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional components
ISO/IEC 15408-3:2008 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance components
ISO/IEC TR 15443-1:2012 Information technology -- Security techniques -- Security assurance framework -- Part 1: Introduction and concepts
ISO/IEC TR 15443-2:2012 Information technology -- Security techniques -- Security assurance framework -- Part 2: Analysis
ISO/IEC TR 15446:2009 Information technology -- Security techniques -- Guide for the production of Protection Profiles and Security Targets

[13] Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security https://www.commoncriteriaportal.org/files/CCRA%20-%20July%202,%202014%20-%20Ratified%20September%208%202014.pdf