Формування державної політики у сфері кібербезпеки, реалізація Стратегії кібербезпеки України

Актуальні аспекти захисту інформації в державних ІТС

Формування державної політики у сфері кібербезпеки, реалізація Стратегії кібербезпеки України

Указом Президента України від 06.05.2015 № 287 затверджено нову редакцію Стратегії національної безпеки України

Указом Президента України від 15.03.2016 № 96 затверджено Стратегію кібербезпеки України

Формування державної політики у сфері кібербезпеки, реалізація Стратегії кібербезпеки України

Розпорядження КМ України 440-р від 24.06.2016 “Про затвердження плану заходів на 2016 рік із реалізації Стратегії кібербезпеки України

Передбачає 24 завдання за такими напрямами:

нормативно-правове забезпечення діяльності у сфері кібербезпеки (гармонізації законодавства із захисту державних інформаційних ресурсів, впровадження системи аудиту інформаційної безпеки об’єктів критичної інфраструктури тощо);

створення технологічної складової національної системи кібербезпеки;

налагодження більш тісного співробітництва з міжнародними партнерами України у сфері кібербезпеки;

налагодження процесу підготовки кадрів у сфері кібербезпеки.

Проект Закону України “Про кібербезпеку України”

Доопрацьовано з урахуванням конструктивних пропозицій від наступних міжнародних організацій:

- НАТО
- Європейської служби зовнішньої діяльності Європейської комісії
- Генерального директорату комунікаційних мереж, контенту та технологій Європейської комісії
- МЗС Німеччини
- Держдепартамент США

Проект Закону України “Про основні засади забезпечення кібербезпеки України”

Основні статті законопроекту передбачають визначення:

- Базових термінів таких як кібератака, кібербезпека, кіберзахист, кіберпростір
- Об’єктів кібербезпеки та кіберзахисту
- Суб’єктів забезпечення кібербезпеки
- Забезпечення кіберзахисту об’єктів кібербезпеки (в тому числі критичної)
- Критичної інформаційної інфраструктури
- Національної системи кібербезпеки
- Повноважень державних органів – основних суб’єктів забезпечення кібербезпеки
- Завдань та статусу Урядової команди реагування на комп’ютерні надзвичайні події України CERT-UA
- Державно-приватної взаємодії у сфері кібербезпеки

Національна система кібербезпеки

Рада національної безпеки і оборони України
(Національний координаційний центр кібербезпеки)

- Державна служба спеціального зв'язку та захисту інформації України (Урядовий CERT-UA)
- Служба безпеки України
- Міністерство внутрішніх справ України (Національна поліція)
- Міністерство оборони України
- Розвідувальні органи України

Інші суб'єкти забезпечення кібербезпеки:

- ✔ інші державні органи (зокрема Національний банк України)
- ✔ розпорядники інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури та інших об'єктів кібербезпеки, які провадять діяльність із надання інформаційних та/або телекомунікаційних послуг
- ✔ незалежні організації та експерти

Урядова команда реагування на надзвичайні комп’ютерні події (CERT-UA)

http://www.cert.gov.ua

Законопроектом визначаються наступні завдання для CERT-UA:

- сприяння державним органам, підприємствам, установам і організаціям незалежно від форми власності, а також громадянам України у вирішенні питань кіберзахисту та протидії кіберзагрозам;
- надання власникам об’єктів кіберзахисту практичної допомоги з питань запобігання, виявлення та усунення наслідків кіберінцидентів стосовно цих об’єктів ;
- накопичення та аналіз даних про кіберінциденти, здійснення ведення реєстру кіберінцидентів ;
- підготовка та висвітлення через власний веб-сайт рекомендацій щодо протидії сучасним видам кібератак та кіберзагроз ;
- взаємодія з українськими командами реагування на комп’ютерні надзвичайні події (CERT або CSIRT), а також іншими підприємствами, установами та організаціями незалежно від форми власності, які провадять діяльність, пов’язану із забезпеченням безпеки кіберпростору ;
- опрацювання отриманої від громадян інформації про кіберінциденти ;
- взаємодія з іноземними та міжнародними організаціями з питань реагування на кіберінциденти ;
- організація та проведення практичних семінарів з питань кібербезпеки та кіберзахисту для державних суб’єктів забезпечення кібербезпеки, а також власників об’єктів кіберзахисту.

Інші нормативно-правові акти з врегулювання питань забезпечення кібербезпеки держави

Проект Указу Президента України «Про деякі заходи щодо захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах»:

- **забезпечення захищеного підключення до Інтернету інформаційно-телекомунікаційних систем державних органів, а також підприємств, установ та організацій, які обробляють державні інформаційні ресурси;**
- **створення захищеного центру обробки даних та затвердження порядку зберігання резервних копій державних інформаційних ресурсів з метою забезпечення можливості відновлення працездатності веб-сторінок, баз даних, реєстрів та інших інформаційних ресурсів державних органів у разі їх втрати або порушення цілісності;**
- **впровадження захищеної електронної пошти із застосуванням засобів криптографічного та технічного захисту інформації в інтересах державних органів;**
- **припинення використання в інформаційно-телекомунікаційних системах програмних засобів захисту інформації російського виробництва;**
- **використання посадовими особами для організації службового електронного листування до впровадження захищеної електронної пошти виключно офіційних електронних поштових скриньок, розміщених на серверах власних інформаційно-телекомунікаційних систем або ресурсах операторів, провайдерів телекомунікацій на території України в доменних зонах GOV.UA або .УКР сегменту Інтернету.**

Інші нормативно-правові акти з врегулювання питань забезпечення кібербезпеки держави

Проект постанови Кабінету Міністрів України «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави»

Порядок визначає механізм формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави.

Наказ Адміністрації Держспецзв'язку від 15.01.2016 № 20 «Про затвердження Порядку сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті», зареєстрований в Мін’юсті за № 196/28326 від 05.02.2016

Метою наказу є підвищення рівня захищеності державних інформаційних ресурсів, розміщених в Інтернеті, шляхом запровадження процедури сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті.
За результатами сканування державним органам надаються конкретні рекомендації щодо усунення виявлених уразливостей, які викладаються у відповідному акті.

Перелік основних нормативних документів системи ТЗІ

Закон України «Про інформацію» від 2 жовтня 1992р. № 2657-XII (зі змінами);
Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 31.05.2005р. № 2594-IV (зі змінами);
Закон України «Про захист персональних даних» від 01.06.2010р. №2297-VI (зі змінами);
Указ Президента України від 27 вересня 1999р. № 1229/99 «Про Положення про технічний захист інформації в Україні»;
Указ Президента України від 14 липня 2000р. № 887/2000 «Про вдосконалення інформаційно-аналітичного забезпечення Президента України та органів державної влади»;
«Правила захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» затверджені постановою Кабінету Міністрів України від 29 березня 2006 року № 373;

ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення.
сприяння державним органам, підприємствам, установам і організаціям незалежно від форми власності, а також громадянам України у вирішенні питань кіберзахисту та протидії кіберзагрозам;
ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.
ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.
ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення.
ДБН А.2.2-2-96 Проектування. Технічний захист інформації. Загальні вимоги до організації проектування та проектної документації для будівництва.

Перелік основних нормативних документів системи ТЗІ

ДБН 2.2-3-2004 Склад, порядок розроблення, погодження та затвердження проектної документації для будівництва.
ГОСТ 34.201 - 89 Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем.
ГОСТ 34.601 - 90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания.
ГОСТ 34.602 - 89 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.
РД 50 - 34.698 - 90 Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Требования к содержанию документов.
Комплекс стандартов Единая система программной документации (ЕСПД).
Комплекс стандартов Единая система конструкторской документации (ЕСКД).
«Положення про державну експертизу в сфері технічного захисту інформації», затверджене наказом Адміністрації Держспецзв'язку України від 16 травня 2007р. № 93 (зі змінами);
НД ТЗІ 1.6-005-2013 «Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної експертизи державної експертизи», затверджене наказом Адміністрації Держспецзв'язку від 15 квітня 2013 р. № 215.

Перелік основних нормативних документів системи ТЗІ

НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.
НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.
НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі. Затверджено наказом ДСТСЗІ СБ України від 04.12.2000 № 53.
НД ТЗІ 1.6-003-2004
НД ТЗІ 2.1-001-2001 Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення. Затверджено наказом ДСТСЗІ СБ України від 09.02.2001 №2.
НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.
НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.
НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 20.12.2000 № 60.

Перелік основних нормативних документів системи ТЗІ

НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.

НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. Затверджено наказом ДСТСЗІ СБ України від 08.11.2005 р. №125

«Порядок оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи сфері технічного захисту інформації», затверджений наказом Адміністрації Держспецзв'язку від 26 березня 2007р. № 45.

Дякую за увагу!