ВІД РЕДАКЦІЙНОЇ КОЛЕГІЇ

ПРОГРАМА ІНФОРМАТИЗАЦІЇ ЗАКОНОТВОРЧОГО ПРОЦЕСУ У ВЕРХОВНІЙ РАДІ УКРАЇНИ НА 2010 - 2015 РОКИ

(проект Постанови Верховної Ради України від 01.07.10 р. № 6633*)

Загальна частина

Широке використання сучасних інформаційно-комунікаційних технологій з метою надання вільного доступу до інформації та знань є базовим принципом інформаційного суспільства, проголошеним Генеральною Асамблеєю Організації Об'єднаних Націй, визначеним Декларацією принципів та Планом дій Всесвітнього саміту інформаційного суспільства (Женева, грудень 2003 року; Туніс, листопад 2005 року) та Постановою Верховної Ради України від 1 грудня 2005 року № 3175 - IV “Про Рекомендації парламентських слухань з питань розвитку інформаційного суспільства в Україні”.

Згідно з рекомендаціями Міжпарламентського Союзу, членом якого є Верховна Рада України, застосування інформаційно-комунікаційних технологій у роботі національних парламентів має відбуватись відповідно до розробленої ними концепції задля:

- забезпечення ефективної роботи парламенту, її прозорості та відкритості;
- гарантування безпеки інформаційних ресурсів парламенту і конфіденційності інформації про особу;
- налагодження діалогу між парламентом, народними депутатами України та громадянами;
- поліпшення механізмів звітності парламенту, народних депутатів України перед виборцями;
- забезпечення повного доступу громадян до інформації про роботу парламенту;
- участі у глобальному інформаційному суспільстві.

Нагальність розроблення і виконання Програми зумовлена необхідність переходу на принципово новий рівень автоматизації технічних процедур, пов'язаних з діяльністю народних депутатів України, формування актуального парламентського електронного інформаційного ресурсу та ретроспективного оцифровування парламентської документації з метою більш ефективного використання наявних інформаційних ресурсів для реалізації повноважень. Верховної Ради України.

Програма розроблена з урахуванням відповідних положень законів України “Про інформацію”, “Про захист інформації в інформаційно-телекомунікаційних системах”, “Про Національну програму інформатизації”, “Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки”, “Про електронні документи та електронний документообіг”, “Про електронний цифровий підпис”, “Про телекомунікації”, “Про статус народного депутата України”, “Про комітети Верховної Ради України”, Постанови Верховної Ради України від 1 грудня 2005 року № 3175-IV “Про Рекомендації парламентських слухань з питань розвитку інформаційного суспільства в Україні” де, зокрема, встановлюються засади створення інформаційних електронних ресурсів та захисту інформації.

1. Мета і основні завдання Програми

Програма ґрунтується на засадах пріоритетності науково-технічного та інноваційного розвитку держави, у тому числі її інформаційної інфраструктури, що сприятиме збільшенню різноманітності та кількості електронних послуг, впровадженню інформаційно-комунікаційних

* Відповідно до статті 93 Конституції України в порядку законодавчої ініціативи внесено на розгляд Верховної Ради України народним депутатом України С.О. Довгим.

технологій в усі сфери суспільного життя та забезпечить максимальний доступ громадян до інформаційних ресурсів і телекомунікаційних послуг.

Метою Програми є: досягнення максимально можливої автоматизації інформаційно-організаційних процесів у діяльності депутатського корпусу загалом, у тому числі комітетів Верховної Ради України, депутатських фракцій а також Апарату Верховної Ради України шляхом створення сучасних систем управління законотворчим процесом та документообігом у парламенті; оперативне інформаційно-аналітичне забезпечення народних депутатів України, помічників-консультантів народних депутатів України, фахівців Апарату Верховної Ради України; створення нової автоматизованої системи обробки вхідних, вихідних, внутрішніх інформаційно-документальних потоків та контролю за виконанням доручень, оперативне формування аналітично-звітної та довідкової документації; технічне удосконалення систем зв'язку для забезпечення оперативності у роботі народних депутатів України, комітетів Верховної Ради України, Апарату Верховної Ради України, у тому числі щодо питань, пов'язаних з діяльністю органів виконавчої влади, органів місцевого самоврядування, інформуванням громадян.

Пріоритетним завданням Програми є створення інтегрованої електронної інформаційно-аналітичної системи “Електронний парламент” (далі - Система) та її центральних підсистем:

- “Електронний офіс народного депутата України”;
- “Електронний Комітет”;
- “Електронна погоджувальна рада”;
- “Електронна бібліотека і архів”;
- “Система електронного голосування та підрахунку голосів”. Створення Системи, у тому числі за визначенням Глобального центру з питань інформаційно-комунікаційних технологій у парламенті при Міжпарламентському Союзі, означає, що законодавчий орган набуде більшої ефективності, прозорості, доступності та звітності.

Так, створена Система забезпечить не лише повну автоматизацію етапів законотворчого процесу, а й інформаційну взаємодію Верховної Ради України з іншими органами державної влади та органами місцевого самоврядування, громадянами, юридичними особами за допомогою сучасних інформаційно-комунікаційних технологій із застосуванням високих стандартів доступу до інформаційних ресурсів парламенту.

2. Шляхи впровадження Програми

Розробка та впровадження Системи здійснюватиметься з урахуванням рекомендацій Глобального Центру з питань інформаційно-комунікаційних технологій у парламенті при Міжпарламентському Союзі, відповідно до світового досвіду зі створення та впровадження в експлуатацію аналогічних аналітично-інформаційних систем і систем підтримки прийняття рішень у галузі державного управління та законотворення.

Система буде створена шляхом модернізації діючих автоматизованих систем, програмно-технічних комплексів і баз даних законодавства та законопроектів, розширення їх можливостей з метою послідовного впровадження технічних систем підтримки прийняття рішень депутатським корпусом в залі пленарних засідань Верховної Ради України, комітетами Верховної Ради України, Погоджувальною радою депутатських фракцій у Верховній Раді України.

Основу Системи складуть діючі автоматизовані системи Верховної Ради України, перелік яких визначено Розпорядженням Голови Верховної Ради України від 1 липня 2003 р. № 663 “Про перелік автоматизованих систем інформаційно-технологічного забезпечення діяльності Верховної Ради України”; автоматизовані системи, програмно-технічні комплекси і парламентські веб-ресурси, розробка та впровадження яких передбачені Планом заходів щодо реалізації Програми (додаток до цієї Програми): інтегрована база даних законотворчого процесу, “Система електронного документообігу і контролю виконання доручень Верховної Ради України”, “Система електронного цифрового підпису”, “Комплексна система захисту інформації в автоматизованих системах Верховної Ради України”, “Електронний офіс

народного депутата України” (стаціонарний і мобільний), система підтримки прийняття рішень комітетом (“Електронний Комітет”), центр ситуативного аналізу (“Електронна погоджувальна рада”), “Електронна бібліотека і архів” (мережева збірка парламентської інформації, доступна депутатському корпусу, Апарату Верховної Ради України та суспільству), “Електронна система голосування і підрахунку голосів” (система “Рада” нового покоління), єдиний веб-портал Верховної Ради України та інтегровані до нього веб-сайти Голови Верховної Ради України, комітетів Верховної Ради України, депутатських фракцій, структурних підрозділів Апарату Верховної Ради України.

Інтеграція зазначених інформаційних ресурсів до Системи відбуватиметься шляхом максимального використання наявних інженерно-технічної інфраструктури та інформаційно-технологічних рішень, створення сучасних центрів обробки даних та електронних архівів з необхідною глибиною збереження інформації за рахунок:

- єдиної програмно-технічної платформи;
- єдиної серверної платформи;
- єдиної системи адміністрування, управління та моніторингу;
- моніторингу; єдиної пошукової системи та набору ефективних електронних сервісів; єдиної комплексної системи захисту інформації; широкого використання відкритих стандартів.

3. Перелік продукції (послуг)

Ядро інформаційно-комунікаційної системи електронного парламенту України у складі:

- інтегрованої бази даних законотворчого процесу Верховної Ради України (інтегрованої інформаційно-комунікаційної системи Верховної Ради України та моделі взаємодії між її складовими); моделі інтеграції сервісів БД законотворчого процесу з автоматизованими системами Верховної Ради України (програмно-технічним комплексом-системою “Рада”, єдиним веб-порталом Верховної Ради України, веб-сайтом Голови Верховної Ради України та веб-сайтами комітетів) по забезпеченню реалізації повноважень Верховної Ради України);
- “Система електронного документообігу та контролю виконання доручень Верховної Ради України” у складі підсистем:
  1) “Загальний електронний документообіг”;
  2) “Реєстрація та контроль проходження законопроектів”;
  3) “Листи та звернення громадян”;
  4) “Обробка депутатських запитів та доручень ВРУ”;
  5) Система “Рада”;
  6) “Кадри”;
  7) “Законодавство України”;
  8) “Міжпарламентські зв'язки”.
- Комплексна система захисту інформації;
- Система електронного цифрового підпису в органах Верховної Ради України та структурних підрозділах Апарату Верховної Ради України;
- Центр сертифікації ключів ВРУ;
- Центр реєстрації користувачів;
- Інтегрований інформаційний центр – центр обробки, резервування, копіювання та збереження інформації з системою комплексного безперервного моніторингу за станом захисту інформаційних ресурсів і оперативного реагування на потенційні загрози їх безпеці;
- Електронний офіс народного депутата України (у складі типових електронних сервісів по доступу до баз даних, звітів, статистики та аналітики) – 450 апаратно-програмних комплексів;
- Електронний Комітет – система підтримки прийняття рішень у залі засідань Комітету Верховної Ради України – 28 апаратно-програмних комплексів (1200 робочих місць);
- Електронна погоджувальна рада – центр ситуацій аналізу для потреб керівництва Верховної Ради України, голів депутатських фракцій і комітетів Верховної Ради України – апаратно-програмний комплекс з 50 робочих місць;
- Система електронного голосування та підрахунку голосів (“Рада-4”) – апаратно-

програмний комплекс з 450 робочих місць;

- Електронна бібліотека і архів – мережева збірка інформації по збору, управлінню і зберіганню цифрового вмісту законотворчого процесу – апаратно-програмний комплекс з 450 робочих місць;
- веб-портал Верховної Ради України;
- веб-сайт Голови Верховної Ради України;
- веб-сайти Комітетів – 28 одиниць;
- веб-сайти фракцій – 5 одиниць;
- інтеграція до веб-порталу ВРУ – 25 веб-сайтів облрад;
- системи комунікації між громадянами та парламентом у вигляді форумів, дискусійних он-лайн груп, інтернет-опитування та голосування і т.д.

4. Потенційні споживачі продукції (послуг)

Країна	Найменування організації
Україна	Верховна Рада України (Апарат ВРУ, Комітети ВРУ, народні депутати України), органи державної влади, громадяни України

5. Оцінка ефекту від впровадження продукції

Впровадження системи “Електронний парламент” України дозволить досягнули Парламенту Україні значних успіхів щодо використання широких можливостей ІКТ у провідних сферах законотворчого процесу, передусім таких, як системи планування, створення і управління базовими документами, систематизація документів відкритого стандарту, створення веб-сторінок, що надають інформацію за допомогою багатьох форматів і каналів, а також забезпечення доступу до широкого кола он-лайн інформації, яка дає посилання на законодавство ще на стадії розгляду. Також впровадження отриманих результатів дозволить розширити доступність даних нормативно-правової інформації “Законодавство України”, “Законодавство АР Крим”, “Київське регіональне законодавство” для населення України та закордонних країн, підвищити якість державного управління в Україні, здійснити широке залучення громадян України до законотворчого процесу, унеможливить нераціональне дублювання накопичувальних інформаційних ресурсів, сприятиме формуванню єдиного інформаційного простору та залученню до ефективного використання науково-технічного потенціалу України. Забезпечить поліпшення взаємодії між суспільством та ВРУ, сприятиме залученню громадянського суспільства до процесу формування та прийняття парламентських рішень.

6. Прогноз результатів

Створення сучасної системи “Електронний парламент” України у складі інтегрованої бази даних законотворчого процесу, “Системи електронного документообігу і контролю виконання доручень Верховної Ради України”, “Системи електронного цифрового підпису”, “Комплексної системи захисту інформації в автоматизованих системах Верховної Ради України”, “Електронного офісу народного депутата України” (стаціонарний і мобільний), системи підтримки прийняття рішень комітетом (“Електронний Комітет”), центру ситуативного аналізу (“Електронна погоджувальна рада”), “Електронної бібліотеки і архіву”, “Електронної системи голосування і підрахунку голосів” (система “Рада” нового покоління), єдиного веб-порталу Верховної Ради України та інтегрованих до нього веб-сайтів Голови Верховної Ради України, комітетів Верховної Ради України, і депутатських фракцій, структурних підрозділів Апарату Верховної Ради України.

Додаток

до Програми інформатизації законотворчого процесу **у** Верховній Раді України на 2010-2015 роки

План заходів щодо реалізації Програми інформатизації законотворчого процесу у Верховній Раді України на 2010-2015 роки

Автоматизація етапів законотворчого процесу (розробка систем планування, створення та управління законопроектами і всіма законодавчими ініціативами)			
№ п/п	**Назва заходу**	**Термін виконання**	**Очікуваний результат**
1	Створення інтегрованої бази даних законотворчого процесу Верховної Ради України (інтегрованої інформаційно-комунікаційної системи Верховної Ради України та моделі взаємодії між її складовими, моделі інтеграції сервісів баз даних законотворчого процесу з автоматизованими системами Верховної Ради України, програмно-технічним комплексом-системою “Рада”, електронним офісом народного депутата, електронним комітетом, електронною погоджувальною радою, електронною бібліотекою, єдиним веб-порталом Верховної Ради України, веб-сайтом Голови Верховної Ради України та веб-сайтами комітетів) по забезпеченню реалізації повноважень Верховної Ради України.	2010-2015 рр.	Створення ядра інформаційно-телекомунікаційної системи електронного парламенту України у складі: електронний офіс народного депутата України; електронний комітет Верховної Ради України; електронна погоджувальна рада; система електронного голосування та підрахунку голосів; електронна бібліотека та архів; система електронного документообігу електронного парламенту України; система електронного цифрового підпису електронного парламенту України; система центру сертифікації ключів; захищені канали зв'язку; системи підтримки електронного парламенту України: єдина точка доступу; система інформаційно-аналітичного забезпечення; система внутрішньої взаємодії. Забезпечення усунення дублюючої інформації в різних базах; більш стабільного процесу обробки та збереження інформації на централізованій основі; послідовна нормалізація та створення систем підтримки прийняття рішень у комітетах на основі існуючих комплексів баз даних законодавства та законопроектів.
2	Розробка та впровадження на сучасних апаратно-програмних засадах “Системи електронного документо-обігу та контролю виконання доручень Верховної Ради України” у складі	2010-2014 рр.	Поетапне впровадження безпаперової технології обробки вхідних, внутрішніх і вихідних інформаційно-документальних потоків. Оснащення

	таких підсистем: 1) “Загальний електронний документообіг”; 2) “Реєстрація та контроль проходження законопроектів”; 3) “Листи та звернення громадян“”; 4) “Обробка депутатських запитів та доручень Верховної Ради України”; 5) Система “Рада”; 6) “Кадри”; 7) “Законодавство України”; 8) “Міжпарламентські зв'язки”.		комп'ютеризованих робочих місць народних депутатів України системами планування, створення та збереження законопроектів.
3	Розробка та впровадження системи електронного цифрового підпису в органах Верховної Ради України та структурних підрозділах Апарату Верховної Ради України.	2010-2014 рр.	Поетапне впровадження електронного цифрового підпису у Верховній Раді України.
4	Розробка технічних регламентів впровадження та функціонування “Системи електронного документообігу та контролю виконання доручень Верховної Ради України” і “Системи електронного цифрового підпису” у органах Верховної Ради України та структурних підрозділах Апарату Верховної Ради України.		Прийняття типових положень, інструкцій, правил, настанов адміністраторам і користувачам; затвердження технологічної схеми роботи з інформаційно-документальними потоками; створення в Апараті Верховної Ради України підрозділів з реєстрації користувачів і сертифікації електронних ключів.
5	Сприяння впровадженню та функціонуванню у Верховній Раді Автономної Республіки Крим, в обласних, міських і районних радах систем електронного документообігу та електронного цифрового підпису на засадах і стандартах, розроблених у Верховній Раді України.	2010-2015 рр.	Поетапна інтеграція інформаційно-комунікаційних систем Верховної Ради України з аналогічними системами місцевих органів державної влади і органів місцевого самоврядування.
6	Створення інтелектуального інструментарію для інформаційно-комп'ютерного супроводу законотворчого процесу - системи оптимізації законотворчого процесу у Верховній Раді України.	2010-2015 рр.	Концептуальна модель системи оптимізації законотворчого процесу у Верховній Раді України; системи аналізу, лінгвістичні підсистеми та природномовні інтерфейси.
6.1.	Системна декомпозиція законотворчого процесу.	2010-2012 рр.	Концептуальна модель системної декомпозиції законотворчого процесу.
6.2.	Розробка інтелектуальної “надбудови” над діючими та проектованими автоматизованими системами Верховної Ради України. 1) Розробка системи статистичного аналізу інформаційно-лінгвістичного корпусу законодавчих документів з метою ретроспективного дослідження,	2010-2014 рр.	1. Концептуальна модель комплексу інтелектуальних інструментів для інформаційно-комп'ютерного супроводу законотворчого процесу. 2. Технічне завдання на розробку систем аналізу, лінгвістичних підсистем та природномовних інтерфейсів. 3. Макет програмного забезпечення

	поточного програмно-аналітичного моделювання та стратегічного планування законотворчої роботи. 2) Розробка лінгвістичних підсистем та природно-мовних інтерфейсів “Системи електронного документообігу та контролю виконання доручень Верховної Ради України”. 3) Розробка системи інформаційно-технологічної підтримки законотворчого процесу на робочому місці народного депутата в службовому кабінеті, в залі комітету, в залі засідань погоджувальної ради, в залі сесійних засідань Верховної Ради України з розширеними інтелектуальними властивостями та ергономікою.		систем аналізу, лінгвістичних підсистем та природномовних інтерфейсів.
7	Розробка, впровадження та удосконалення комплексної системи захисту інформації в автоматизованих системах Верховної Ради України, у т.ч. політики безпеки інформації, концепції захисту інформаційних ресурсів, порядку виявлення, попередження, оцінювання та прогнозування загроз безпеці державних інформаційних ресурсів, визначення рівня захисту інформації від несанкціонованих дій в інформаційно-телекомунікаційній системі Верховної Ради України.	2010-2014 рр.	Реалізація функцій управління: інцидентами, проблемами, конфігураціями, змінами, релізами, потужностями, рівнем IT-сервісів та їх безперервністю, доступністю, інформаційною безпекою.
8	Розробка та погодження з уповноваженими органами виконавчої влади порядку створення та експлуатації сучасних комплексів та засобів захисту інформації у Верховній Раді України, вимога щодо захисту якої встановлена законом.	2010-2015 рр.	Забезпечення функціонування комплексу оперативних методів автентифікації, контролю доступу та засобів захисту при використанні інформаційних ресурсів.
9	Розробка та затвердження нормативно-правової бази, що регламентує питання функціонування і розвитку системи “Електронний парламент” та підсистем “Електронний офіс народного депутата”, “Електронний Комітет”, “Електронна погоджувальна рада”, “Електронна бібліотека і архів”, “Система електронного голосування та підрахунку голосів”, їх апаратно-програмної платформи, політики та системи захисту інформації.	2015 р.	Пакет нормативно-правових актів (у т.ч. пропозиції щодо внесення змін до Регламенту Верховної Ради України та Положення про Апарат Верховної Ради України і навчально-методичних матеріалів, що забезпечують перехід на безпаперову технологію законотворчого, процесу.

Автоматизація формування баз даних чинного законодавства України			
1	Розвиток систем управління чинними законами (бази даних “Законодавство України в Інтернет” та “Законодавство України в Інтранет”).	2010-2014 рр.	Інтеграція бази даних “Законодавство України” до “Системи електронного документообігу і контролю виконання доручень Верховної Ради України”; підвищення рівня інформаційно-аналітичного забезпечення суб'єкта законотворчого процесу.
2	Створення технологічної бази даних нормативно-правової інформації “Законодавство-4” та “Законодавство-4 (Документообіг)” у складі баз даних: “Законодавство України”; “Законодавство АР Крим”; “Київське регіональне законодавство”.	2010-2014 рр.	Розширення функціональних можливостей бази даних “Законодавство України”.
3	Розробка систем семантичного аналізу: 1) Розробка фундаментальної лексикографічної системи “Великий державний тезаурус України”. 2) Розвиток програмного, інформаційного та лінгвістичного забезпечення української версії тезаурусу EUROVOC. 3) Розробка та впровадження експериментальної зони віртуальної, юридичної лабораторії законодавства України.	2010-2015 рр.	1.Концептуальні моделі лексикографічної системи «Великий державний тезаурус України», лінгвістичного забезпечення та віртуальної юридичної лабораторії законодавства України. 2. Технічне завдання на розробку систем лінгвістичного забезпечення та віртуальної юридичної лабораторії законодавства України. 3. Макет програмно-інформаційного та лінгвістичного забезпечення фундаментальної лексикографічної системи “Великий державний тезаурус України”, української версії тезаурусу EUROVOC, експериментальної зони віртуальної юридичної лабораторії законодавства України.
Розширення програмно-технічної, мережевої та інженерно-будівельної інфраструктури законотворчого процесу			
1	Створення системи електронного голосування та підрахунку голосів (програмно-технічний комплекс-система “Рада-4”).	2010-2012 рр.	Впровадження програмно-технічного комплексу нового покоління, який повною мірою відповідатиме Регламенту Верховної Ради України (забезпечення функції персонального голосування), чинним нормативним документам з технічного захисту інформації, стандартам Єдиної системи програмної документації та Єдиної системи конструкторської документації. Виконання будівельно-монтажних і оздоблювальних робіт у залі пленарних засідань.
2	Створення інтегрованого	2010-2014 рр.	Введення в промислову експлуатацію

	інформаційного центру (вул. Садова, 3, добудова, - центр обробки, резервування, копіювання та збереження інформації з системою комплексного безперервного моніторингу за станом захисту інформаційних ресурсів і оперативного реагування на потенційні загрози їх безпеці).		сертифікованого центру безпеки інформаційних ресурсів Верховної Ради України; забезпечення 100 % відмовостійкості та катастрофостійкості автоматизованих систем і мереж.
3	Створення електронного офісу народного депутата України: розробка набору однотипних електронних сервісів, які надають доступ до баз даних, звітів, статистики та аналітики.	2010-2014 рр.	Облаштування в службовому кабінеті народного депутата України електронного офісу та забезпечення мобільним електронним офісом.
4	Створення “Електронного Комітету” - системи підтримки прийняття рішень у залі засідань Комітету Верховної Ради України (у тому числі з можливістю впровадження підсистеми дистанційного голосування при прийнятті рішень на засіданнях Комітету та депутатських фракції).	2010-2014 рр.	Впровадження систем підтримки прийняття рішень комітетом Верховної Ради України. Виконання будівельно-монтажних і оздоблювальних робіт у залах засідань комітетів.
5	Створення “Електронної погоджувальної ради” - Центру ситуативного аналізу для потреб керівництва Верховної Ради України, голів депутатських фракцій і комітетів Верховної Ради України.	2010-2014 рр.	Впровадження програмно-технічного комплексу в залі засідань погоджувальної ради з метою надання допомоги членам погоджувальної ради у прийнятті рішень за складних умов для повного та об'єктивного аналізу предметної галузі законотворчого процесу. Виконання будівельно-монтажних і оздоблювальних робіт у залі засідань погоджувальної ради.
6	Створення “Електронної бібліотеки і архіву” - мережевої збірки інформації, яка збирає, управляє і зберігає для довгострокового використання весь цифровий вміст законотворчого процесу.	2010-2014 рр.	Впровадження першої черги програмно-технічного комплексу збору, управління і зберігання всього цифрового вмісту законотворчого процесу. Виконання будівельно-монтажних і оздоблювальних робіт у бібліотечних залах.
7	Модернізація інженерно-технічної та мережевої інфраструктури Верховної Ради України.	2010-2015 рр.	Розширення можливостей резервування, копіювання інформації.
7.1	Розширення можливостей діючого центру обробки даних (в. Садова 3-А).	2010-2015 рр.	Розширення можливостей резервування, копіювання інформації.
7.2	Модернізація комп'ютерної мережі в адмінбудинках вул. Грушевського, 18/2, Садова, 3, Несторівський пр., 4, В.Житомирська, 11 до швидкості передачі даних 1 Gbit/s з підтримкою протоколу Dot1x.	2010-2014 рр.	Заміна морально застарілого обладнання, досягнення сучасних параметрів обробки та передачі інформації (швидкість, надійність, захист).

7.3	Заміна активного мережевого обладнання в будівлях Верховної Ради України, де не передбачено проведення реконструкції для підтримки протоколу передачі даних Dot1x.	2010-2014 рр.	Заміна морально застарілого обладнання, досягнення сучасних параметрів обробки інформації.
7.4	Створення міжбудинкового швидкісного (10 Gbit/s) оптоволоконного кільця передачі даних.	2010-2014 рр.	Забезпечення сучасних параметрів обробки та передачі інформації (швидкість, надійність, захист).
8	Закупівля ліцензійного системного та прикладного програмного забезпечення і стандартної технічної підтримки до нього.	2010-2015 рр.	Досягнення відповідності апаратних засобів їх програмному забезпеченню; впровадження новітніх технологій у програмному забезпеченні АС Верховної Ради України.
Впровадження парламентських веб-технологій і створення систем підтримки взаємодії Верховної Ради України з громадянами			
1	Впровадження в промислову експлуатацію та супроводження програмного забезпечення веб-порталу Верховної Ради України, веб-сайту Голови Верховної Ради України та веб-сайту Комітету.	2010 р.	Вирішення питань структури, дизайну, навігації, пошукових сервісів та мультимедійних параметрів відповідно до рекомендацій Міжпарламентського Союзу. Впровадження комплексної системи захисту інформації єдиного веб-порталу Верховної Ради України як складової системи “Електронний парламент”.
2	Створення парламентського веб-порталу “Інтернет-мовлення”.	2011-2013 рр.	Складова системи “Електронний парламент”.
3	Розробка методичних рекомендацій щодо використання Інтернету під час проведення опитувань населення.	2011-2013 рр.	Забезпечення народних депутатів України інструментарієм роботи з виборцями у рамках системи “Електронний парламент”.
4	Розробка системи оперативного ознайомлення з нормативними актами України через супутниковий канал “Рада” обласних, міських, районних та сільських органів місцевого самоврядування.	2011-2013 рр.	Інформаційно-просвітницька складова системи “Електронний парламент”.
5	Розробка підсистеми комунікації між громадянами та парламентом у вигляді форумів, дискусійних он-лайн груп, інтернет-опитування та голосування і т.п.	2011-2014 рр.	Забезпечення методами комунікації зворотного зв'язку між громадянами та парламентом для поглиблення діалогу.
Організаційно-правові заходи інформатизації законотворчого процесу			
1	Проведення серії “круглих столів”, семінарів, відео-конференцій за участю Голови Верховної Ради України, голів комітетів Верховної Ради України, лідерів депутатських фракцій, народних депутатів України та керівництва Апарату з питань інформатизації	2011-2014 рр.	Забезпечення регулярного обговорення питань розвитку інформатизації законотворчого процесу та прийняття відповідних рішень і рекомендацій.

	законотворчого процесу.		
2	Уточнення структури та штатного розкладу Управління комп'ютеризованих систем Апарату Верховної Ради України.	2010 р.	Розробка та затвердження уточненої структури та штатного розкладу Управління комп'ютеризованих систем Апарату Верховної Ради України.
3	Створення організаційної структури управління та підтримки електронного парламенту України.	2014 р.	Розробка правової та нормативної бази функціонування електронного парламенту України; створення структурних підрозділів підтримки та безпеки електронного парламенту України.
4	Організація участі представників комітетів Верховної Ради України і Апарату Верховної Ради України у розробці пропозицій до проектів Інформаційного кодексу України та нормативно-правових актів з питань впровадження механізмів та регламентів надання Верховною Радою України та органами місцевого самоврядування інформаційних послуг юридичним та фізичним особам через Інтернет, зокрема у частині опрацювання звернень громадян, які подаються з використанням Інтернет та електронного цифрового підпису.	2011-2014 рр.	Розробка та створення належної нормативно-правової бази для розвитку інформаційного суспільства та функціонування системи “Електронний парламент”.
5	Підготовка методичних рекомендацій щодо розроблення програм інформатизації обласних, районних, міських, селищних і сільських рад.	2011-2014 рр.	Забезпечення місцевих органів державної влади і органів місцевого самоврядування інструментарієм роботи у рамках системи “Електронний парламент”.
6	Забезпечення співпраці з Міжпарламентським Союзом, Генеральним Директоратом Європейської комісії з питань інформаційного суспільства, Форумом ООН з управління Інтернетом, Глобальним центром з питань інформаційно-комунікаційних технологій у парламенті, дослідними комісіями, центрами і робочими групами з питань розвитку інформаційного суспільства.	2011-2014 рр.	Організація участі представників від Верховної Ради України в роботі зазначених структур, у підготовці та проведенні міжнародних заходів, обмін досвідом, навчання фахівців.
7	Аналіз стану виконання міжнародних договорів та зобов'язань України з питань розвитку інформаційного суспільства.	2011-2015 рр.	Моніторинг виконання міжнародних договорів з питань розвитку інформаційного суспільства.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

Неофіційний переклад

РЕКОМЕНДАЦІЇ
Ради Організації економічного співробітництва та розвитку
від 27 липня 2002 року

“ДИРЕКТИВИ З ПРОБЛЕМ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ І МЕРЕЖ: ФОРМУВАННЯ КУЛЬТУРИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ”

Рада Організації економічного співробітництва та розвитку,

беручи до уваги Конвенцію про створення Організації економічного співробітництва та розвитку (далі – ОЕСР) від 14 грудня 1960 р. і, зокрема, статей 1 b), 1 c) і 5 b) вказаного документа,

беручи до уваги Рекомендації Ради, що регламентують забезпечення недоторканності приватного життя та захисту транскордонних потоків персональних даних від 23 вересня 1980 р.,

беручи до уваги Декларацію про транскордонні потоки даних, прийняту урядами держав-членів ОЕСР від 11 квітня 1985 р.,

беручи до уваги Рекомендації Ради, що регламентують політику в сфері криптографії від 27 березня 1997 р.,

беручи до уваги Декларацію про аутентифікацію у сфері електронній комерції, прийняту на рівні міністрів держав-членів ОЕСР 7 – 9 грудня 1998 р.,

визнаючи, що інформаційні системи і мережі використовуються урядами, комерційними підприємствами, іншими організаціями і приватними користувачами у все більш широких масштабах і що важливість та значимість цих систем і мереж постійно зростає,

визнаючи, що постійно зростаюча значимість і роль інформаційних систем і мереж, а також зростаюча залежність від них у справі забезпечення стабільного і ефективного функціонування національної економіки різних держав і міжнародної торгівлі, а також в соціальному, культурному та політичному житті потребують особливих заходів по захисту таких систем і мереж і по закріпленню довіри до них,

визнаючи, що впровадження інформаційних систем і мереж та їх розповсюдження по всьому світу пов’язані з появою нових і зростаючих факторів ризику,

визнаючи, що існує загроза безпеці даних і інформації, що зберігається в системах і мережах, або даним і інформації, що передаються про них, яка зумовлена можливістю різного роду несанкціонованого доступу, використання, неправомірного присвоєння, зміни, пересилки шкідливих програм, відмови в обслуговуванні або знищення вищезгаданих даних і інформації, і що необхідні належні міри захисту,

визнаючи, що існує необхідність підвищення обізнаності про фактори ризику для інформаційних систем і мереж та існуючу політику, практику, засоби і процедури, що спрямовані на протидію факторам ризику, а також на необхідність стимулювання належної поведінки як найважливіший крок, що спрямований на формування культури забезпечення безпеки,

визнаючи, що існує загальна зацікавленість в забезпеченні безпеки інформаційних систем і мереж шляхом формування культури забезпечення безпеки, причому ця зацікавленість сприяє координації дій і співробітництву в міжнародних масштабах для того, щоб успішно вирішувати проблеми, що виникають у зв’язку зі збитком, який може бути завданий економіці різних держав, міжнародній торгівлі і участі громадян у соціальному, культурному та політичному житті через збої в системі безпеки,

визнаючи, що “Директиви з проблеми безпеки інформаційних систем і мереж: формування культури забезпечення безпеки”, які приведені у Додатку до цих Рекомендацій, підлягають виконанню на добровільних засадах та не зачіпають суверенних прав держав,

визнаючи, що ці Рекомендації не є основою для припущень про вищевказане так, як для забезпечення безпеки існує одне конкретне рішення, і про те, яка саме політика, практика, засоби і процедури придатні для будь-якої конкретної ситуації; навпаки, в цих рекомендаціях

викладена сукупність принципів, що покликані сприяти формуванню більш чіткому представленню про те, як сторони-учасники можуть винести для себе вигоду від розвитку і удосконалення культури безпеки та зробити свій внесок в її розвиток і вдосконалення,

р е к о м е н д у є держава-членам ОЕСР для застосування документ, що називається “Директиви з проблем безпеки інформаційних систем і мереж: формування культури забезпечення безпеки”, шляхом:

заохочення розвитку культури забезпечення безпеки у відповідності до положень Директив,

проведення консультацій та координації дій держав-членів ОЕСР та здійснення співпраці на національному та міжнародному рівні з метою реалізації положень Директив,

прийняття державами-членами ОЕСР нових положень та внесення змін до чинної політики, практики, заходів і процедур в сфері безпеки з тим, щоб врахувати положення Директив в державному та приватному секторах, в тому числі, серед урядів, комерційних підприємств, інших організацій і приватних користувачів для того, щоб сприяти формуванню і закріпленню культури забезпечення безпеки і підтримати всі зацікавлені сторони і їх намагання проявляти відповідальне відношення до даної проблеми та прийняття необхідних заходів для реалізації вказаних у Директивах положень,

надання державами-членами ОЕСР Директив у розпорядження держав, що не є членами ОЕСР,

перегляду Директив кожні п’ять років для того, щоб сприяти розвитку міжнародного співробітництва з питань, що стосуються безпеки інформаційних систем та мереж.

Ці Рекомендації прийняті на заміну Рекомендацій Ради з проблеми безпеки інформаційних систем від 26 листопада 1992 р.

Додаток

ДИРЕКТИВИ З ПРОБЛЕМ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ І МЕРЕЖ: ФОРМУВАННЯ КУЛЬТУРИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ

Передмова

За період, що минув з 1992 р., коли ОЕСР вперше представила “Директиви з проблеми безпеки інформаційних систем”, у сфері застосування інформаційних систем та мереж, так само як і інформаційних технологій в цілому, відбулися корінні зміни. Ці зміни, що тривають і до цього дня, принесли суттєву вигоду, однак при цьому вони вимагали і набагато більш серйозної уваги до сфери безпеки з боку урядів, комерційних підприємств, інших організацій та приватних користувачів, які розробляють інформаційні системи і мережі, володіють ними, надають їх у користування, керують ними, обслуговують або використовують їх (“сторони-учасники”).

На зміну досить скромним за можливостями автономним системам, що працювали, як правило, в ізольованих мережах, прийшли значно більш високопродуктивні персональні комп'ютери, розробки на стику різних наукових напрямів, повсюдне розповсюдження отримав Інтернет. Сьогодні сторони-учасники стають все в більшій мірі пов’язаними один з одним, причому ці зв’язки перетинають кордони держав. Крім того, Інтернет забезпечує функціонування таких важливих компонентів інфраструктури, як енергетика, транспорт і фінансовий сектор, та значно суттєвою мірою визначає те, яким чином компанії ведуть свій бізнес, як уряди і органи державного управління надають послуги громадянам та підприємствам і як громадяни спілкуються між собою та обмінюються інформацією один з одним. Характер і тип технологій, що утворюють інформаційну інфраструктуру та інфраструктуру зв’язку, також істотно змінилися. Кількість та різноманіття пристроїв для доступу до цих видів інфраструктури зросли в багато раз, і тепер до їх складу входять фіксовані, бездротові та мобільні пристрої, причому постійно збільшується відсоток пристроїв, доступ через які здійснюється у безперервному режимі через постійно працюючі канали

зв’язку. Як наслідок усього цього, значно зросли різноманітність, обсяг і ступінь секретності інформації, що надсилається.

Як наслідок, збільшення числа зв’язків та обсягів обміну даними між інформаційними системами та мережами, даним системам та мережам зараз загрожують зростаюча кількість і більш широке різноманіття загроз і факторів ризику. У зв’язку з цим, у сфері забезпечення безпеки виникають нові проблеми. З цих причин дані Директиви поширюються на всі сторони-учасники інформаційного суспільства і дають підстави вважати, що існує необхідність розширення обізнаності про існування проблем у сфері забезпечення безпеки та досягнення кращого розуміння суті цих проблем, а також необхідність формування так званої “культури забезпечення безпеки”.

Стаття 1. Формування культури забезпечення безпеки

Ці Директиви покликані допомогти впоратися з проблемами, що виникають в мінливій сфері безпеки, шляхом заохочення формування культури забезпечення безпеки. Іншими словами, акцент робиться на необхідність забезпечення безпеки при розробці інформаційних систем і мереж та прийняття нової моделі мислення і поведінки при використанні інформаційних систем та мереж і при взаємодії з ними. Прийняття цих Директив знаменує собою принципову зміну в самому ставленні до забезпечення захищеної структури і безпечної експлуатації мереж і систем у порівнянні з тим, що було раніше (в минулому, дуже в багатьох випадках проблеми безпеки намагалися вирішувати “заднім числом”, тобто тоді, коли було вже надто пізно). Сторони-учасники все більшою мірою залежать від інформаційних систем, мереж та пов'язаних з ними послуг, і всі ці системи, мережі й послуги повинні стати більш надійними і захищеними. Безпека може бути надійно забезпечена тільки при прийнятті такого підходу, при якому в належній мірі враховуються інтереси всіх сторін-учасників і основні властивості систем, мереж та пов’язаних з ними послуг.

Діяльність кожної сторони-учасника має важливе значення для забезпечення безпеки. Сторони-учасники у відповідності зі своїми ролями та функціями повинні бути проінформовані про відповідні ризики у сфері безпеки і превентивні заходи, вони повинні брати на себе відповідальність і вживати заходів, спрямованих на підвищення безпеки інформаційних систем та мереж.

Для того щоб стимулювати формування і вдосконалення культури забезпечення безпеки, будуть потрібні як керівництво, так і широка участь зацікавлених сторін, і це має призвести до підвищення пріоритетності питань планування та керівництва забезпеченням безпеки, а також до усвідомлення всіма сторонами-учасниками необхідності забезпечення безпеки. Проблемами забезпечення безпеки повинні займатися на всіх рівнях державного управління та комерційних підприємств, так само як і всі сторони-учасники. Справжні Директиви утворюють основу, на якій має будуватися робота по формуванню культури забезпечення безпеки в суспільстві.

Це дозволить сторонам-учасникам враховувати фактор безпеки при проектуванні та експлуатації всіх інформаційних систем та мереж. У Директивах пропонується, щоб усі сторони-учасники сформували у себе і розвивали культуру забезпечення безпеки як спосіб мислення, оцінки та прийняття заходів, що стосуються функціонування інформаційних систем та мереж.

Стаття 2. Цілі та завдання

Метою і завданням цих Директив є:

а) сприяти вдосконаленню у всіх сторін-учасників культури забезпечення безпеки як засобу захисту інформаційних систем і мереж;

б) підвищити обізнаність про фактори ризику для інформаційних систем та мереж, про існуючу політику, практику, заходи та процедури, спрямовані на захист від цих ризиків, і про необхідність прийняття та реалізація даної політики, практики, заходів і процедур;

в) заохочувати формування у всіх сторін-учасників більшої довіри до інформаційних систем та мереж і до того способу, яким вони надаються в користування і використовуються;

г) створити спільну концептуальну основу, яка допоможе сторонам-учасникам зрозуміти суть проблем у сфері безпеки і поставитися з увагою до етичних цінностей при розробці та реалізації логічно послідовної політики, практики, заходів і процедур забезпечення безпеки інформаційних систем і мереж;

д) сприяти співпраці та обміну інформацією, наскільки це буде доречним, між усіма сторонами-учасниками при виробленні та реалізації політики, практики, заходів і процедур у галузі безпеки;

е) сприяти тому, щоб всі сторони-учасники, залучені в розробку і реалізацію стандартів і норм, визнавали важливість завдання забезпечення безпеки.

Стаття 3. Основні принципи

Наступні дев’ять принципів є взаємодоповнюючими, і їх слід розглядати як єдине ціле. Вони відносяться до сторін-учасників на всіх рівнях, включаючи політичний і оперативний. Згідно з цими Директивами обов’язки сторін-учасників будуть залежати від виконуваних ними функцій та ролей. Всі сторони-учасники тільки виграють від покращення рівня своєї поінформованості, їм піде на користь прищеплення відповідних навичок, спільне використання інформації і навчання, а це дозволить їм глибше зрозуміти суть проблем безпеки й удосконалювати практичні дії в цій сфері. Заходи і зусилля по підвищенню безпеки інформаційних систем та мереж не повинні суперечити цінностям демократичного суспільства і, зокрема, необхідності існування вільних і відкритих інформаційних потоків і такому основоположному тезису, як необхідність забезпечення недоторканності приватного життя.

1) Поінформованість

Сторони-учасники повинні усвідомлювати необхідність забезпечення безпеки інформаційних систем та мереж і розуміти, що вони можуть зробити для підвищення безпеки.

Поінформованість про фактори ризику та існуючі заходи безпеки можна розглядати як перший “рубіж оборони” при забезпеченні безпеки інформаційних систем та мереж. На інформаційні системи і мережі можуть впливати як внутрішні, так і зовнішні ризики. Сторони-учасники повинні віддавати собі звіт в тому, що збої в системі безпеки можуть призвести до заподіяння істотної шкоди системам та мережам, які знаходяться під їх контролем. Вони також повинні бути інформовані про можливий збиток, який може бути завданий іншим внаслідок взаємного підключення та взаємної залежності між системами та мережами. Сторони-учасники повинні знати конфігурацію своєї системи, і в їх розпорядженні має бути інформація про існуючі оновлення до неї, про місце системи в мережах, про належні прийоми роботи, які вони можуть впровадити для підвищення безпеки, а також про потреби та потреби інших сторін-учасників.

2) Відповідальність

За безпеку інформаційних систем та мереж відповідають всі сторони-учасники.

Взаємозалежні локальні та глобальні інформаційні системи і мережі відіграють важливу роль у забезпеченні нормальної роботи сторони-учасника, і ці сторони повинні усвідомлювати свою відповідальність за забезпечення безпеки цих інформаційних систем та мереж. Вони повинні відповідати за свої дії відповідно до виконуваних ними функцій і ролей. Сторони-учасники повинні регулярно аналізувати свою власну політику, практику, заходи та процедури, і оцінювати, наскільки вони відповідають ситуації, що склалася. Ті, хто розробляє, проектує і постачає продукти та послуги, повинні в процесі своєї роботи приділяти увагу питанням забезпечення безпеки систем і мереж та своєчасно розсилати відповідну інформацію, включаючи оновлення, з тим, щоб читачі могли краще зрозуміти функціональні можливості продуктів і послуг, що відносяться до забезпечення безпеки, і свої обов’язки щодо забезпечення безпеки.

3) Вжиття заходів у відповідь

Сторони-учасники повинні, у співробітництві з іншими, робити своєчасні дії для запобігання, виявлення та реагування на інциденти, пов’язані з порушеннями безпеки.

Усвідомлюючи взаємозв’язок і взаємозалежність інформаційних систем і мереж та потенційну можливість того, що цим системам, в принципі, можуть бути протягом короткого часу завдані масштабні ушкодження, сторони-учасники повинні своєчасно, виявляючи готовність до співпраці один з одним, реагувати на інциденти, пов’язані з порушеннями безпеки. Вони повинні ділитися один з одним – залежно від конкретної ситуації – відомостями про погрози та вразливі місця, а також реалізовувати процедури, що передбачають швидке і дієве налагодження співробітництва для запобігання та виявлення інцидентів, пов’язаних з порушенням безпеки, і реагування на них. У тих випадках, коли це буде допустимим, можуть передбачатися транскордонне спільне використання інформації та міжнародне співробітництво.

4) Етика

Сторони-учасники повинні враховувати законні інтереси інших осіб і організацій.

Враховуючи широке поширення інформаційних систем та мереж в суспільстві, сторони-учасники повинні усвідомити, що їх дія або бездіяльність може завдати шкоди іншим особам і організаціям. Тому вкрай важлива етична поведінка, і сторони-учасники повинні докласти зусиль для розробки та впровадження найбільш оптимальних методів роботи та стимулювання такої поведінки, при якій усвідомлюється необхідність забезпечення безпеки і повазі до законних інтересів інших.

5) Демократія

Забезпечення безпеки інформаційних систем та мереж не повинно вступати в протиріччя з основними цінностями демократичного суспільства.

Безпека повинна реалізовуватися таким чином, щоб це поєднувалося з цінностями, визнаними в демократичному суспільстві, такими, зокрема, як свобода обміну думками та ідеями, вільний обмін інформацією, конфіденційність інформації та зв’язку, належний захист особистої інформації, інформаційна відкритість та прозорість.

6) Оцінка ризиків

Сторони-учасники повинні проводити оцінку ризиків.

У ході оцінки ризиків виявляються загрози та вразливі місця, причому така оцінка повинна бути достатньою мірою всеосяжною, щоб врахувати найважливіші внутрішні та зовнішні фактори, до числа яких відносяться технологічні, фізичні і людські фактори, політика і послуги третіх сторін, що впливають на забезпечення безпеки. Оцінка ризиків дозволить визначити прийнятний рівень ризику і допомогти у виборі належних засобів і методів управління в ситуації, коли існує ризик завдання збитку інформаційним системам та мережам, при цьому повинні братися до уваги характер і важливість інформації, що захищається. З огляду на зростаючий взаємозв’язок і взаємозалежність між інформаційними системами, оцінка ризиків повинна включати в себе аналіз потенційного збитку, що може виходити від інших осіб і організацій або може бути завданий їм.

7) Розробка та реалізація систем і мереж з урахуванням необхідності забезпечення безпеки

Сторони-учасники повинні розглядати безпеку як один з найбільш важливих елементів інформаційних систем та мереж.

Для забезпечення оптимального рівня безпеки необхідна належна розробка, реалізація та координування систем, мереж і політики. Головним, але не єдиним напрямом цієї діяльності є розробка та впровадження належних заходів безпеки і рішень, покликаних усунути або обмежити потенційний збиток, обумовлений існуванням виявлених загроз і вразливих місць. Для цього потрібні заходи безпеки і рішення як технічного, так і нетехнічного характеру, і вони повинні відповідати цінності інформації, що зберігається в системах та мережах відповідної організації. Забезпечення безпеки повинно бути основоположною властивістю всіх продуктів, послуг, систем і мереж, так само як і невід’ємною складовою частиною проектів і архітектури

систем. Для кінцевих користувачів проектування і реалізація з урахуванням фактору безпеки значною мірою зводиться до вибору і конфігурації продуктів і послуг для своєї системи.

8) Керівництво забезпеченням безпеки

Сторони-учасники повинні прийняти комплексний підхід до керівництва забезпеченням безпеки.

Керівництво забезпеченням безпеки повинно ґрунтуватися на оцінці ризиків. Воно має бути динамічним, таким, що охоплює всі рівні діяльності сторін-учасників і всі аспекти їхньої роботи. Воно має включати в себе завчасне реагування на загрози, що з’являються, і має передбачати вжиття заходів, спрямованих на запобігання та виявлення інцидентів та реагування на них, заходів з відновлення систем після збоїв, безперервне технічне обслуговування, аналіз і аудит. Політика, практика, заходи і процедури в галузі забезпечення безпеки інформаційних систем та мереж повинні бути скоординованими та інтегрованими для того, щоб утворювати логічно послідовну систему забезпечення безпеки. Вимоги до керівництва забезпеченням безпеки залежать від рівня участі, ролі та функцій сторін-учасників, існуючого ризику та вимог до системи.

9) Повторна оцінка

Сторони-учасники повинні аналізувати і проводити повторну оцінку безпеки інформаційних систем і мереж, а також вносити відповідні зміни в політику, практику, заходи і процедури в сфері безпеки.

Постійно виявляються нові, постійно-змінні загрожуючи фактори і вразливі місця. Сторони-учасники повинні безперервно аналізувати, повторно оцінювати і вносити зміни в усі елементи комплексу заходів по забезпеченню безпеки, для того щоб протидіяти цим можливим факторам ризику.

Переклад з англ. – Віри Брижко.
Режим доступу: *//www.oecd.org/dataoecd/16/22/155 82260.pdf*

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~