Додаток А

ПРАВИЛА
використання ресурсів Українського Національного Гріда (УНГ)

1. Преамбула.

1.1. Цей документ встановлює загальні правила використання ресурсів національної грід-інфраструктури, обов'язкові для всіх користувачів Українського Національного гріда (УНГ), в тому числі, адміністраторів грід-сайтів і віртуальних організацій.

Мета цього документу полягає у визначенні правил для інформаційно-безпечного надійного обслуговування великої кількості користувачів у змінному, географічно і адміністративно розподіленому гетерогенному обчислювальному середовищі УНГ.

Вузли УНГ можуть висувати додаткові вимоги до користувачів віртуальних організацій, яким вони надають доступ до власних грід-сайтів, за умови, якщо ці вимоги не суперечать загальним правилам, викладеним в цьому документі.

Цей документ стосується усіх користувачів УНГ, в тому числі, іноземних, які використовують ресурси УНГ в рамках програм міжнародного співробітництва, незалежно від країни одержання сертифіката користувача грід, громадянства і країни постійного перебування.

1.2. Ресурси УНГ включають:

- комп'ютерні кластери, робочі станції, сервери, і персональні комп'ютери, що підключені до національної грід-інфраструктури;
- комунікаційні мережі, що об'єднують ці комп'ютери;
- системи збереження даних, підключені до національної грід-інфраструктури;
- інші активні компоненти і обладнання мережі, підключене до національної грід-інфраструктури;
- служби та сервіси, бібліотеки програм, прикладне і системне програмне забезпечення, бази даних і документів, інформаційні сховища і файлові архіви, встановлені на комп'ютерах і мережевому обладнанні національної грід-інфраструктури.

Поняття «ресурс УНГ» не передбачає жодної форми відчуження, часткової передачі права власності, або прав на управління чи безпосередній доступ до відповідних апаратних засобів і програмного забезпечення будь-яким іншим учасникам УНГ. Організації та установи, що надають (на добровільній основі і відповідно до їх внутрішньої політики) такі ресурси для часткового використання у межах УНГ, залишають за собою повний необмежений контроль над усіма складовими наданих ресурсів.

1.3. Терміни та визначення.

Грід-сайт (Grid Site) – сукупність ресурсів та сервісів грід-інфраструктури, що надається установою для колективного використання.

Адміністратор з безпеки грід-сайту, або представник з безпеки грід-сайту (Site Security Contact) – особа, яка відповідає за безпеку роботи сервісів грід-сайту, аналізує загрози безпеці грід-мережі і встановлених сервісів, проводить дослідження інцидентів безпеки та діє як контактна особа у випадках інцидентів, що стосуються питань комп'ютерної або мережевої безпеки грід-сайту.

Адміністратор грід-сайту (Site Administrator) – особа відповідальна за роботу грід-сайту і його сервісів. Як правило, цю функцію виконує адміністратор обчислювального кластера.

Менеджер віртуальної організації **(*Virtual Organization Manager*)** – уповноважена центром ВО особа, що відповідає за реєстрацію учасників ВО та слідкує за дотриманням ними правил користування УНГ і вимог інформаційної безпеки.

Адміністратор віртуальної організації **(*Virtual Organization Administrator*)** – уповноважена центром ВО особа, відповідальна за дотримання ліцензійних угод та відсутність інформаційної загрози програмного забезпечення, яке ВО розповсюджує на грід-сайти для проведення досліджень. Надає інформаційну підтримку або самостійно встановлює і налагоджує програмне забезпечення на грід-сайтах. Функції менеджера і адміністратора віртуальної організації можуть бути об’єднаними і закріпленими за одною особою.

Інцидент безпеки **(*Security Incident*)** – це акт порушення формально описаних, чи неявних умов інформаційної безпеки ресурсів УНГ, облікових записів користувачів УНГ, або конфіденційних даних користувачів УНГ.

2. Правила використання ресурсів УНГ.

2.1. Ресурси УНГ можуть використовуватися:

- тільки за умови дотримання вимог законодавства України, дотримання прийнятих в українському суспільстві моральних норм і законних інтересів третіх осіб;
- тільки в некомерційних цілях;
- тільки в інтересах і в рамках офіційної діяльності тієї організації чи установи, за чиєю заявою був наданий сертифікат користувача УНГ (Додаток Г);
- тільки за тематикою робіт, цілями і політикою, заявленою при реєстрації віртуальної організації, членом якої є користувач (Додаток Д);
- тільки з використанням дозволеного грід-сайтом легального програмного забезпечення.

2.2. Користувач зобов’язаний:

1) використовувати ресурси УНГ для виконання тільки робіт, розрахунків, передачі або зберігання даних, що відповідають п.2.1 даних Правил;
2) дотримуватися рекомендацій і правил безпеки грід-сайтів, віртуальної організації, центру сертифікації та інших служб УНГ;
3) зберігати особистий секретний ключ (private key), та завірений центром сертифікації сертифікат користувача УНГ тільки з додержанням правил захисту конфіденційності операційної системи;
4) зберігати пароль (секретне слово, необхідне для генерації проксі-сертифікату) в таємниці, використовувати складні безпечні паролі;
5) ні в якому разі не передавати свої ключі, паролі чи сертифікати, в тому числі, діючі проксі-сертифікати третім особам;
6) використовувати облікові записи користувача тільки для цілей, для яких вони були надані;
7) використовувати тільки власні облікові записи і не намагатися замаскувати реальну приналежність певних облікових записів;
8) не використовувати наданий доступ до ресурсів УНГ для надання непрямого доступу неавторизованих користувачів;
9) негайно повідомляти центр сертифікації або його філію про будь-які проблеми з безпекою свого особистого секретного ключа, сертифікатів, або паролю;
10) уникати використання ресурсів УНГ в такий спосіб, що може порушити їх нормальне функціонування або завдати їм збитку;
11) раціонально використовувати ресурси УНГ, враховувати інтереси інших користувачів, намагатися запобігати перевантаженню ресурсів і грід-служб УНГ;
12) не порушувати політику управління ресурсами, використовуючи механізми обходу засобів захисту чи адміністративного керування грід-сайту;
13) повідомляти адміністратора з безпеки грід-сайту про будь-який інцидент безпеки, відому чи підозрювану спробу несанкціонованого доступу до облікового запису або робочої станції користувача і, взагалі, про будь-яку аномалію поведінки користувачів чи функціонування програм, яка притягне їх увагу;
14) не намагатися використати чи самостійно виправити будь-які помилки захисту ресурсів УНГ. Негайно повідомити адміністратора з безпеки грід-сайту про виявлені помилки інформаційного захисту сайту;
15) зберігати конфіденційність будь-якої інформації, отриманої під час доступу до ресурсів УНГ, відносно якої можна припустити, що вона є конфіденційною або істотною для безпечного функціонування певних елементів УНГ. Повідомляти адміністратора з безпеки грід-сайту про наявність і розташування подібної інформації;
16) шанувати права власності, пов’язані з ресурсами УНГ, включаючи авторське право на програмне забезпечення і права власності на інформацію;
17) не намагатися дістати несанкціонований доступ до даних, що зберігаються або передаються по мережі ресурсу УНГ, зокрема, до облікових

записів користувачів, за винятком випадків передбачених п.2.3 даних Правил.

Користувачі повинні дозволити публікацію їх персональних відомостей в електронних каталогах і базах даних в тій мірі, в якій це необхідно для нормального функціонування УНГ.

Менеджери УНГ, базового чи регіонального координаційного центру, центрів сертифікації, центрів віртуальних організацій та грід-сайтів мають право регулювати і припиняти доступ до ресурсів з адміністративних чи операційних потреб, зокрема з ціллю усунення проблем безпеки, а також формувати додаткові інструкції, обов'язкові для подальшої роботи користувачів.

Користувачі, яким у зв'язку з їх професійними специфічними обов'язками був наданий обліковий запис з привілейованим доступом, повинні сповістити керівника віртуальної організації, адміністратора грід-сайту чи адміністратора з безпеки грід-сайту, як тільки необхідність в такому привілейованому доступі відпаде.

2.3. Адміністратори та адміністратори з безпеки грід-сайтів УНГ мають особливий привілейований доступ до інформації, що зберігається на ресурсах УНГ.

Використання вказаної інформації обмежується наступними умовами:

1) адміністраторам та адміністраторам з безпеки грід-сайтів УНГ дозволено обмінюватися інформацією, отриманою завдяки привілейованому доступу тільки між собою, за винятком випадків, коли більше поширення інформації необхідне для виконання їх службових обов'язків;
2) привілейований доступ до інформації повинен здійснюватися виключно в рамках професійних обов'язків і тільки для наступних цілей:
   - щоб вирішити проблеми пов'язані з функціонуванням обчислювальних ресурсів УНГ, включаючи оптимізацію існуючих або інсталяцію нових ресурсів;
   - для виявлення вразливих місць або порушень комп'ютерного захисту ресурсів;
   - для моніторингу ресурсів;
   - для проведення розслідувань, коли є підозра в порушенні правил використання ресурсів УНГ (за розпорядженням відповідального за безпеку сайту або іншого уповноваженого на те керівника);
   - для зміни прав доступу або для анулювання облікових записів після закінчення контракту користувача з організацією, за чиєю заявкою йому був наданий сертифікат користувача УНГ, після закінчення членства користувача у віртуальній організації, у разі закінчення надання ресурсів грід-сайту віртуальній організації, або якщо дії користувача виявилися не сумісні з даними Правилами чи правилами використання ресурсів грід-сайту;
   - для відновлення нормального функціонування елементу УНГ, якщо його робота була серйозно порушена внаслідок неумисних або умисних дій користувача.

3. Відповідальність.

3.1. Відповідальність користувача за порушення Правил.

Користувачі несуть персональну відповідають за збиток, нанесений ресурсам УНГ внаслідок будь-якого порушення даних Правил.

У разі отримання повідомлення від адміністратора з безпеки грід-сайту, адміністратора чи менеджера віртуальної організації, або безпосереднього керівника користувач повинен прийняти негайні заходи для усунення виявлених порушень протягом призначеного терміну.

Якщо порушення не було усунуте протягом призначеного терміну, було пов'язане з суттєвою загрозою безпеці, або мало негативні наслідки, надання користувачу доступу до ресурсів УНГ припиняється.

За результатами розслідування користувач може бути притягнутий до адміністративної, а у випадку виявлення фактів порушення законодавства України – до кримінальної відповідальності.

3.2. Взаємна відповідальність елементів УНГ

Постійні елементи національної грід-інфраструктури (базовий та регіональні координаційні центри, ресурсні центри, центри сертифікації) несуть відповідальність перед державою відповідно до договорів, заключених в рамках Державної цільової науково-технічної програми впровадження і застосування грід-технологій на 2009-2013 роки.

Відповідальні особи вузлів УНГ несуть відповідальність перед державою відповідно до зобов'язань взятих на себе під час реєстрації та підключення до національної грід-інфраструктури (Додаток В). Зокрема, вони зобов'язані дотримуватися правил обслуговування й інформаційного захисту ресурсів власних грід-сайтів.

Відповідальні особи центрів віртуальних організацій несуть відповідальність перед державою та іншими елементами національної грід-інфраструктури відповідно до зобов'язань взятих на себе під час реєстрації та підключення до національної грід-інфраструктури (Додаток Д), а також перед вузлами УНГ відповідно до двосторонніх угод про надання віртуальній організації ресурсів певного грід-сайту.

3.3. Відповідальність елементів УНГ перед користувачем.

Жоден елемент національної грід-інфраструктури, так само як УНГ в цілому, не гарантує надання ресурсів УНГ, безвідмовного функціонування ресурсів УНГ, чи збереження конфіденційності інформації, що передається чи зберігається в грід.

Жоден елемент національної грід-інфраструктури, УНГ в цілому, держава не несуть ніякої відповідальності у випадку фінансових чи моральних втрат користувачів, організацій чи установ, що надають ресурси чи використовують УНГ, або третіх осіб (фізичних чи юридичних) внаслідок чи у зв'язку з:

- використанням ресурсів УНГ;
- отриманням, збереженням у центрі сертифікації чи його філії, або оновленням сертифікатів користувача;
- реєстрацією віртуальної організації чи грід-сайту, тощо.

Користувач отримує сертифікат, підключається до віртуальних організацій та використовує ресурси УНГ тільки під свою власну відповідальність.

4. Реагування на інциденти безпеки

У разі виявлення порушень Правил використання ресурсів УНГ, адміністратор з безпеки грід-сайту, адміністратор чи менеджер віртуальної організації, або безпосередній керівник користувача повинні терміново повідомити користувача про суть виявленої проблеми і її наслідки.

Якщо порушення незначне, не мало наслідків і може бути швидко усунутим, після усного попередження користувач повинен прийняти негайні заходи для усунення виявлених порушень.

Якщо порушення не було усунуте протягом призначеного терміну, або пов'язане з невеликою загрозою безпеці окремого грід-сайту, але не мало негативних наслідків, і не вплинуло на інші елементи УНГ адміністратор з безпеки грід-сайту повинен у письмовій формі сповістити менеджера віртуальної організації користувача про факт порушення і правила, які були порушені, визначити спосіб і остаточний термін виправлення порушення.

У разі порушення, що являє собою суттєву загрозу безпеці сайту чи загрозу конфіденційності інформації, або якщо порушення не було усунуте протягом письмово вказаного терміну виправлення, або в разі повторного порушення менеджер віртуальної організації за зверненням адміністратора з безпеки грід-сайту має терміново анулювати членство користувача у віртуальній організації, а адміністратор з безпеки грід-сайту – надійно позбавити такого користувача доступу до ресурсів УНГ.

Якщо терміново анулювати право доступу користувача до ресурсів УНГ не вдається, адміністратор з безпеки грід-сайту має право повністю відключити віртуальну організацію та повідомити центр реєстрації віртуальних організацій про необхідність анулювання реєстрації відповідної віртуальної організації.

Адміністратор з безпеки грід-сайту, адміністратор і менеджер віртуальної організації зобов'язані терміново інформувати базовий координаційний центр про кожний інцидент з безпеки, щодо якого прийнято рішення про обмеження доступу користувача або віртуальної організації. Базовий координаційний центр повинен сповістити адміністраторів з безпеки усіх інших сайтів, яких може торкатися ця проблема, і організувати їх співробітництво для її усунення в масштабі УНГ.

5. Термін дії.

Ці правила затверджуються та можуть бути змінені рішенням Координаційного Комітета Програми «Державної цільової науково-технічної програми впровадження і застосування грід-технологій на 2009-2013 роки».