«Затверджую»
В.о. ректора Національного університету
«Львівська політехніка»
_____ проф. Ю.Я. Бобало
«___»_____ 2019 р.

ПОЛОЖЕННЯ ПРО ІНФОРМАЦІЙНУ СИСТЕМУ «ВІРТУАЛЬНЕ НАВЧАЛЬНЕ СЕРЕДОВИЩЕ ЛЬВІВСЬКОЇ ПОЛІТЕХНІКИ»

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Це Положення регламентує порядок функціонування Віртуального навчального середовища (надалі – **ВНС**) у Національному університеті «Львівська політехніка» (надалі – Університет).

1.2. Положення розроблено на підставі законів України «Про вищу освіту», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про доступ до публічної інформації», «Про авторське право і суміжні права», Статуту Університету, Політики інформаційної безпеки Національного університету «Львівська політехніка», Положення «Про єдине інформаційне середовище Національного університету «Львівська політехніка» та інших внутрішніх нормативних документів Університету.

1.3. У цьому Положенні терміни використовуються у таких значеннях:

- адміністратор Віртуального навчального середовища (Адміністратор ВНС) – структурний підрозділ Університету, який забезпечує процеси функціонування **ВНС** Університету та має повноваження, надані керівництвом Університету, щодо контролювання, впровадження, розвитку, підтримування, використання та захисту інформації;
- інформаційна культура – це способи поводження з інформацією під час її створення, збирання, зберігання, опрацювання, подання і використання, що забезпечують цілісне бачення інформаційної діяльності Університету та передбачення її результатів;

- інформаційна система/сервіс – сукупність організаційних і програмно-апаратних засобів для збору, збереження, пошуку, опрацювання та пересилання інформації з метою забезпечення інформаційних потреб користувачів;
- інформаційний актив – це сукупність інформації, яка має цінність для Університету, працівників, здобувачів освіти, інших зацікавлених фізичних та юридичних осіб, а також будь-яка система опрацювання, обміну або фізичного зберігання цієї інформації;
- інформаційний масив – множина однорідних сукупностей пов'язаної інформації (реквізитів), яка об'єднана спільним змістом і розглядається як єдине ціле;
- електронний освітній ресурс – навчальні, наукові, довідкові матеріали та засоби, розроблені в електронній формі та збережені на носіях будь-якого типу або розміщені у комп'ютерних мережах, що їх відтворюють за допомогою електронних цифрових технічних засобів і необхідні для ефективної організації освітнього процесу;
- ризик – це можливість негативного впливу на діяльність Університету внаслідок використання інформаційного активу.

1.4. У цьому Положенні використано такі скорочення:
- БД – база даних;
- ЕОР – електронний освітній ресурс;
- ЄІС – єдине інформаційне середовище;
- ІДН – Інститут дистанційного навчання;
- ІС – інформаційна система/сервіс;
- ОС – операційна система;
- СКБД – система керування базами даних;
- ЦІЗ – Центр інформаційного забезпечення.

1.5. **ВНС** – це Інтернет-орієнтована ІС ЄІС, призначена для інформаційного супроводу освітнього процесу в Університеті шляхом надання учасникам цього процесу доступу до ЕОР, оцінювання знань здобувачів освіти та реалізації таких завдань:
- забезпечення здобувачів освіти ЕОР та оцінювання їхнього рівня знань;
- створення, опрацювання та збереження веб-орієнтованих ЕОР Університету, а саме підручників, посібників, конспектів лекцій, методичних вказівок та інструкцій до лабораторних, практичних робіт тощо;
- каталогізації електронних освітніх ресурсів Університету та їх зв'язку із ЕОР у зовнішніх сервісах.

1.6. Користувачами **ВНС** є здобувачі освіти та працівники Університету.

1.7. Виключне майнове право на інформаційні активи, створені у **ВНС**, належить Університету.

1.8. Відповідальною особою за організацію та ефективне використання **ВНС** є проректор з науково-педагогічної роботи, який може частину своїх повноважень делегувати директору ІДН.

1.9. Адміністратором **ВНС** є ІДН.

1.10. Адміністратором системного програмного та апаратного забезпечення, необхідного для функціонування **ВНС**, є ЦІЗ.

2. ПРИНЦИПИ ТА ПРАВИЛА ПОБУДОВИ ВНС

2.1. Побудова **ВНС** базується на таких принципах:

- системності – **ВНС** є складовою ЄІС Університету;
- непублічності – основні інформаційні масиви **ВНС** не містять інформації у формі відкритих даних та файлів;
- цілісності інформації – стійкість інформації **ВНС** до спотворення і знищення (пов'язаних з помилками апаратних та програмних засобів, системними помилками та помилковими діями користувачів) підтримується усіма доступними засобами;
- логічної організації інформації – інформаційні масиви **ВНС** класифікуються згідно з типовими правилами опрацювання та інтерпретації даних.

2.2. Побудова **ВНС** базується на таких правилах:

- взаємодія **ВНС** із іншими ІС відбувається на основі загальновикористовуваних стандартів обміну даними;
- програмне забезпечення **ВНС** має модульну структуру;
- при обранні програмного забезпечення для **ВНС** перевага надається готовим програмним продуктам з відкритим кодом та можливістю адаптації до потреб Університету;
- **ВНС** не призначено для збереження приватної інформації користувачів, зокрема особистої переписки, фото(відео)матеріалів тощо;
- користувачі несуть відповідальність за зміст інформації, внесеної ними у **ВНС**.

3. СТРУКТУРА ВНС

3.1. **ВНС** складається з:

- основної частини – БД та інших інформаційних активів, які містять дані та файли про ЕОР Університету та їхнє використання;
- конфігураційної частини – інформаційних масивів, що містять налаштування (конфігурацію) **ВНС**;
- програмної частини – інформаційних масивів, які відображають алгоритми опрацювання даних;
- системного програмного та апаратного забезпечення.

3.2. Основна частина **ВНС** містить такі види інформаційних масивів: ЕОР; метадані та каталог ЕОР; тестові завдання; профілі користувачів; журнали оцінювання виконаних завдань; набір структурованих файлів з окремими компонентами ЕОР тощо.

3.3. Конфігураційна частина **ВНС** містить журнальні інформаційні масиви (журнали подій, помилок, імпорту/експорту даних тощо) та конфігураційні

інформаційні масиви (дані про налаштування, параметри, взаємозв'язки, розподіл прав користувачів тощо).

3.4. Програмна частина **ВНС** містить прикладне програмне забезпечення, збережені процедури, функції та тригери БД, необхідні для використання основної та конфігураційної частин **ВНС**.

3.5. Системне програмне та апаратне забезпечення **ВНС** містить серверні операційні системи, СКБД, сервери, засоби управління та моніторингу, мережеве обладнання та конфігураційні файли.

4. ПОВНОВАЖЕННЯ КОРИСТУВАЧІВ ВНС

4.1. Користувачі **ВНС** мають такі рівні повноважень:

- первинний – поширюється на користувачів, які створюють нові, змінюють наявні та знищують непотрібні елементи інформаційних масивів відповідно до наданих прав і повноважень;
- вторинний – поширюється на користувачів, які використовують інформаційні масиви для опрацювання, відображення, пошуку, передавання, розповсюдження, використання тощо відповідно до наданих прав і повноважень;
- адміністративний – поширюється на працівників Університету, які належать до Адміністратора ВНС і встановлюють права і повноваження інших користувачів.

4.2. Відповідальна особа за організацію та ефективне використання **ВНС**:

- здійснює загальне координування робіт щодо побудови **ВНС**;
- забезпечує впровадження та ефективне використання **ВНС**;
- бере участь у формуванні вимог до інформаційного та методичного забезпечення, необхідного для використання **ВНС**;
- здійснює управління ризиками, пов'язаними з використанням **ВНС**;
- має повноваження первинного чи вторинного рівня.

4.3. Користувач – працівник Адміністратора ВНС:

- виконує роботи, необхідні для побудови та забезпечення ефективного використання **ВНС**;
- відповідає за реалізацію Політики інформаційної безпеки щодо використання **ВНС** у межах ЄІС;
- реалізує заходи, пов'язані з управління ризиками, пов'язаними з використанням **ВНС**;
- бере участь у формуванні вимог до інформаційного, лінгвістичного, програмного, апаратного, метрологічного та методичного забезпечення, необхідного для використання **ВНС**;
- має повноваження адміністративного рівня.

4.4. Користувач, який не відноситься до Адміністратора ВНС:

- бере участь використанні **ВНС**, відповідно до наданих йому прав та повноважень;

- реалізує заходи щодо мінімізації ризиків, пов'язаними з використанням **ВНС**;
- може надавати пропозиції щодо вимог до інформаційного, лінгвістичного, програмного, апаратного, метрологічного та методичного забезпечення, необхідного для використання **ВНС**;
- користувачі мають повноваження первинного чи вторинного рівня.

5. УПРАВЛІННЯ РИЗИКАМИ ФУНКЦІОНУВАННЯ ВНС

5.1. Відповідальними за управління ризиками функціонування **ВНС** є Відповідальна особа та Адміністратор ВНС.

5.2. Управління ризиками функціонування **ВНС** здійснюється під час роботи прикладного програмного забезпечення **ВНС**, СКБД, веб-сервера та ОС (яка керує файловою системою та забезпечує функціонування СКБД, веб-сервера тощо).

5.3. Ризиками функціонування **ВНС** є порушення конфіденційності, цілісності та доступності інформації БД та збережених у **ВНС** файлів.

5.4. Можливими загрозами функціонування **ВНС** є:
- загрози впливу неякісної (недостовірної, неповної, свідомо чи несвідомо спотвореної тощо) інформації на користувача **ВНС**, підрозділ Університету чи Університет загалом;
- загрози несанкціонованого і неправомірного впливу на БД та файли, що зберігаються у **ВНС**, а також на засоби їхнього зберігання, формування і використання;
- загрози інформаційним правам і свободам осіб (працівників, здобувачів освіти, випускників) щодо створення, пошуку, одержання і використання інформації, дотримання особистої таємниці, захисту честі і гідності тощо.

5.5. Основними чинниками та обставинами, наслідком прояву яких може бути виникнення ризиків функціонування **ВНС** є:
- порушення зв'язків з зовнішніми джерелами формування інформаційних масивів;
- помилки у даних, імпортованих з інших ІС Університету;
- низький рівень інформаційної культури користувачів **ВНС**;
- навмисні шкідливі дії користувачів **ВНС** чи анонімних відвідувачів сайту **ВНС**;
- порушення законодавства про захист авторських та суміжних прав при розміщенні матеріалів у **ВНС**;
- низька якість апаратного та програмного забезпечення, а також інформаційної інфраструктури Університету;
- неналежне регулювання Університетом процесів функціонування підсистем ЄІС;
- проникнення шкідливого програмного забезпечення у **ВНС** чи інші ІС ЄІС;
- впровадження нових програмних засобів та інформаційних технологій;

- втрата зв'язку з інформаційними ресурсами сторонніх сервісів;
- використання недосконалих методів та засобів захисту інформації;
- відсутність ефективної системи резервного копіювання та відновлення **ВНС**;
- викрадення чи несанкціоноване копіювання інформації;
- несанкціоноване підключення до апаратного забезпечення та каналів зв'язку.

5.6. Типовими несанкціонованими (навмисними або випадковими) діями користувачів **ВНС** без отриманих на це прав і повноважень є:

- зміна, знищення або блокування даних **ВНС** та їхніх резервних копій;
- перехоплення або копіювання даних **ВНС**, які не є публічною інформацією, що призвело до їхнього витоку;
- розсилання спаму користувачам **ВНС**, інших ІС ЄІС чи зовнішніх систем;
- створення умов, що привели до проникнення шкідливого програмного забезпечення в ІС ЄІС.

5.7. Заходи щодо зменшення вразливості **ВНС** реалізуються пропорційно та адекватно до наявних та потенційних ризиків та загроз.

5.8. Основними заходами для зменшення вразливості **ВНС** є:

- налагодження контролю за дотриманням принципів та правил побудови **ВНС**;
- проведення заходів щодо підвищення рівня інформаційної культури користувачів;
- налагодження функціонування системи моніторингу працездатності та продуктивності апаратного і програмного забезпечення **ВНС** та зовнішніх систем і сервісів тощо;
- узгодження процесів функціонування **ВНС** та нормативних документів Університету;
- розподіл прав і повноважень користувачів;
- своєчасне оновлення програмного забезпечення, зокрема антивірусного;
- побудова систем взаємодії **ВНС** з іншими ІС ЄІС чи зовнішніми системами і сервісами, які використовують інформацію **ВНС**;
- побудова системи резервного копіювання та відновлення інформації, що забезпечує територіальну відокремленість резервних копій;
- налагодження контролю доступу до інформації, яка не є публічною;
- проведення аудиту даних;
- облік проблем під час функціонування та адміністрування **ВНС**;
- побудова системи життєзабезпечення технічних засобів та каналів зв'язку (відеоспостереження, сигналізації, протипожежної безпеки, резервного електроживлення, клімат-контролю тощо);
- посилення фізичного захисту будівель та приміщень для протидії незаконному підключенню до апаратного забезпечення та каналів зв'язку.

5.9. У разі зміни переліку ризиків, їхніх чинників чи можливих загроз Адміністратор ВНС погоджує з Відповідальною особою зміну моделей несанкціонованих дій користувачів та вживає заходи щодо зменшення вразливості **ВНС**.

5.10. Кожен користувач повинен вживати заходи щодо мінімізації ризиків використання **ВНС**, а у разі виявлення нових видів ризиків та загроз – негайно повідомити про це Відповідальну особу чи Адміністратора ВНС.

Проректор Д.В. Федасюк

Директор ІДН Д.О. Тарасов