УДК 004.056

О.О. Будік, В.Ф. Чекурін
Національний університет «Львівська політехніка»,
кафедра «Захист інформації»
79013, м. Львів, вул. С. Бандери, 12

СПЕЦИФІЧНІ ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ СИСТЕМ ЕЛЕКТРОННОГО НАВЧАННЯ

In the paper specific information security problems and threats of e-learning systems were considered. The threats were classified and analyzed.

Keywords – e-learning system, information security, threats, threat analysis, impersonation threat

У статті розглянуто специфічні проблеми та загрози інформаційній безпеці систем електронного навчання. Проведено класифікацію та аналіз виявлених загроз.

Ключові слова: система електронного навчання, інформаційна безпека, загрози, аналіз загроз, загроза підміни особи

Вступ

Системи електронного навчання (СЕН) являють собою відкриті інформаційно-комунікаційні системи, які за допомогою сукупності спеціалізованих програмних, комп'ютерних, телекомунікаційних засобів та педагогічних технологій реалізують якісно нову форму навчання. СЕН все більше використовують як в закладах освіти, так і в інших галузях – державних, комерційних, громадських структурах тощо. Хоч в СЕН, призначених для освітньої галузі, циркулюють документи переважно без грифів секретності, інформаційні потоки містять дані, що потребують захисту з огляду на їх комерційну, службову чи персональну конфіденційність [1]. До того ж забезпечення цілісності та доступності інформації в таких системах потребують застосування як спеціальних технічних засобів, так і організаційних заходів захисту.

У СЕН можуть виникати специфічні загрози, невластиві для інших інформаційних систем. Їх виявлення, аналіз і розроблення методів і засобів для нейтралізації є актуальним науково-технічним завданням. У статті розглядаються підхід до їх виявлення та деякі специфічні загрози інформаційній безпеці СЕН.

1. Аналіз публікацій

Останнім часом інтерес науковців до питань інформаційної безпеки СЕН істотно зріс. Основними напрямками досліджень у цій галузі є аналіз загроз, розроблення підходів до їх нейтралізації, процедур управління інформаційною безпекою СЕН тощо.

У праці [2] запропонована методологія аналізу загроз СЕН, що базується на побудові дерева відмов. На цій основі розглянуті деякі загрози в конкретних системах (Moodle і ILIAS) і запропоновані рекомендації для їх усунення. Проте проведений аналіз не враховує імовірності появи загроз та ступеня їх деструктивного впливу на СЕН. Це не дозволяє кількісно їх оцінювати і порівнювати. До того ж запропонована методологія не дозволяє здійснювати ранжирування загроз.

У роботі [3] звертається увага на проблеми автентифікації користувачів у системах дистанційного навчання. Подальше дослідження у цьому напрямку виявило, що системи автентифікації сучасних СЕН є незадовільними з точки зору інформаційної безпеки і потребують інноваційних підходів. Запропоноване рішення – використання смарт-карт – дає деякі переваги, проте не вирішує проблеми добровільної передачі носія з автентифікаційними даними іншій особі.

Автори статті [4] звертають увагу на виникнення загроз при дистанційному оцінюванні студентів. Тут розглядаються деякі загальні технічні аспекти, властиві не лише СЕН, зокрема, такі загрози як XSS (міжсайтовий скриптінг), SQL-ін'єкція, атаки на сесії, переповнення буферу, підміна стеку. На конкретних прикладах позані можливості реалізації цих загроз в системі Moodle.

У статті [5] акцентується увага на необхідності розроблення адекватних підходів до управління інформаційною безпекою СЕН. Стверджується, що більшість сучасних СЕН розроблялися без урахування вимог інформаційної безпеки. Автори наголошують на важливості управління безпекою для створення захищеного навчального середовища. Проте конкретні рішення не пропонуються.

2. Взаємодії об'єктів та суб'єктів в СЕН

Загрози СЕН можна поділити на загальні і специфічні. До загальних відносимо загрози, що є властивими для будь-яких автоматизованих інформаційних систем, наприклад, загрози доступності (DoS-атаки), підбір паролей, атаки переповнення буфера, SQL-ін'єкції та ін. Виходитимемо із того, що ефективне убезпечення від загроз такого типу в СЕН можливе з використанням методів та засобів захисту інформації загального призначення.. Тому їх тут не розглядатимемо.

Серед специфічних можна виділити ті, які залежні від реалізації СЕН, та ті, які зумовлені взаємодією суб'єктів та об'єктів СЕН [6]. Перші необхідно розглядати при побудові СЕН за конкретно вибраними технологіями. У цій статті звернемо увагу на специфічні загрози другого типу. Вони є більш загальними, виявляються через особливості навчального процесу і проявляються в СЕН незалежно від того, яким чином вона спроектована.

Виділяємо множини суб'єктів $\mathbf{S}$ та об'єктів $\mathbf{O}$ СЕН. Суб'єктами взаємодії в СЕН можуть виступати зареєстровані в ній користувачі, зокрема, студенти, викладачі, адміністратори освіти, автори навчального контенту, системні адміністратори тощо.

Кожен суб'єкт $s \in \mathbf{S}$ володіє певною множиною прав і обов'язків R, тобто існує відповідність

$$\forall s \in S \quad s \mapsto R, \; R \in \mathbf{R} \tag{1}$$

де $\mathbf{R}$ — множина усіх прав і обов'язків суб'єктів, можливих в СЕН.

Якщо суб'єкти $s_1 \in \mathbf{S}$ і $s_2 \in \mathbf{S}$ мають одну і ту ж множину прав і обов'язків R, то вони належать до одного класу S_R суб'єктів: $s_1, s_2 \in S_R$. В такий спосіб усі суб'єкти поділяються на класи еквівалентності, які називатимемо класами суб'єктів СЕН.

Кожен об'єкт $o \in O$ характризується певною множиною правил доступу до нього P, тобто існує відповідність:

$$\forall o \in O \quad o \mapsto P, P \subset \mathbf{P} \tag{2}$$

де $\mathbf{P}$ — множина усіх правил, які діють в СЕН.

При цьому суб'єкти та об'єкти СЕН взаємодіють між собою. Множина таких взаємодій встановлює зв'язки між S та O:

$$\mathrm{I}_{SO} : S \mapsto O \tag{3}$$

Для кожного конкретного суб'єкта та об'єкта існує певна своя множина взаємодій I_{so}, яка є підмножиною I_{SO}:

$$\forall s : s \in S \wedge \forall o : o \in O \exists I_{so} : I_{so} \subset \mathrm{I}_{SO} \quad (4)$$

Кожна взаємодія встановлює зв'язок між суб'єктами та об'єктами:

$$i_{so} : s \mapsto o, i_{so} \in I_{so} \quad (5)$$

Тоді політику безпеки СЕН можна визначити як дозволену сукупність елементів множин R_S та P_O, поставлених у відповідність до $s \in S$ та $o \in O$ в рамках конкретної взаємодії.

Формуємо множину суб'єктів S. Згідно узагальненої структурної моделі СЕН [7], є пять суб'єктів: студент – s_1, викладач – s_2, автор контенту – s_3, адміністратор освіти – s_4, системний адміністратор – s_5. Тоді $S = \{s_1, s_2, s_3, s_4, s_5\}$ – дискретна множина суб'єктів СЕН.

Формуємо множину об'єктів O. Вона включає репозиторій навчального контенту – o_1, бази даних навчальної інформації – o_2, адміністративну систему СУНК (системи управління навчальним контентом) – o_3, авторингову систему СУНК – o_4, адміністративну систему СУН (системи управління навчанням) – o_5, систему доставки СУН – o_6, систему оцінювання СУН – o_7, комунікаційний модуль – o_8. Тоді $O = \{o_1, o_2, o_3, o_4, o_5, o_6, o_7, o_8\}$ - дискретна множина об'єктів СЕН.

3. Модель взаємодії «студент-викладач»

Для опису взаємодій об'єктів застосуємо модель СЕН, використовуючи стандарт IEEE LTSA (Learning Technology System Architecture), який визначає принципи побудови графічних моделей взаємодії об'єктів [8]. Об'єкти, що беруть участь у взаємодії, позначають за цим стандартом овалами, взаємозв'язки, потоки інформації та даних між ними – стрілками, а інформаційні сховища (файли, бази даних та знань, цифрові бібліотеки) – прямокутниками. Можна розглядати як парні взаємодії, в яких беруть участь лише два об'єкти, так і більш складні, в яких задіяні три і більше об'єктів. Множина таких взаємодій I визначається множиною усіх підмножин множини об'єктів O, тобто її булеаном 2^O. Проте, не всі такі комбінації утворюють допустимі взаємодії об'єктів, а більшість специфічних загроз, які виявляються у простих взаємодіях, повторюються і в складніших. Тому розглянемо лише частину складних взаємодій, які дозволяють виявити найпоширеніші специфічні загрози.

Розглянемо для прикладу взаємодію «студент-викладач» (рис. 1), яка найчастіше зустрічається у системах електронного навчання.

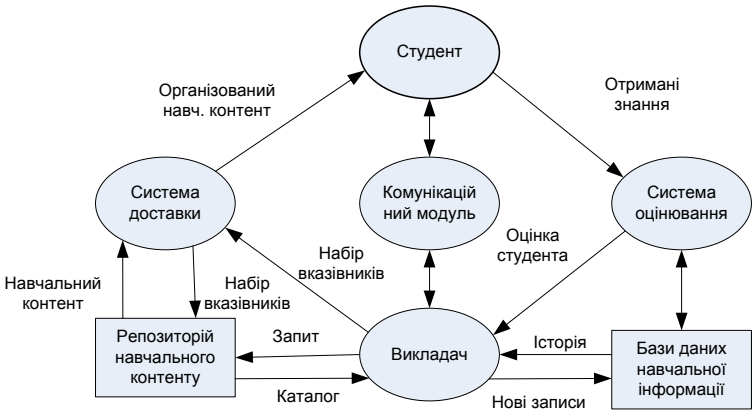

Рис. 1. Модель взаємодії «студент-викладач»

Тут можна виділити, зокрема, такі **типи** взаємодій: проведення різних видів занять зі студентами (лекцій, практичних занять, лабораторних робіт, консультацій тощо), проведення контрольних заходів (модульного контролю, заліків, екзаменів тощо), індивідуальна робота викладача зі студентом тощо.

Суб'єктами взаємодії у всіх випадках є студент та викладач ($S = \{s_1, s_2\}$), **об'єктами** – система доставки, комунікаційний модуль, система оцінювання, репозиторій навчального контенту, бази даних навчальної інформації ($O = \{o_1, o_2, o_6, o_7, o_8\}$). **Мета** взаємодії залежить від її типу. Під час взаємодії виникають такі **інформаційні потоки**: навчальний контент, обмін знаннями між студентом і викладачем через комунікаційний модуль; каталог контенту, доступний викладачеві; набір вказівників, що формує викладач; організований навчальний контент, що відправляється студентові; отримані знання, які студент демонструє системі оцінювання; оцінка студента, яку формує система оцінювання; історія про попередні навчальні досягнення студента; нові записи про актуальні навчальні досягнення студента, які зберігаються у базах даних навчальної інформації.

Визначаємо множину R_s кожного суб'єкта. Студент отримує, зокрема, наступні права та обов'язки:

$r_{s_s}^{(1)}$ – особистої участі у всіх взаємодіях в рамках СЕН, передбачених навчальною програмою;

$r_{s_s}^{(2)}$ – особистого доступу до інформаційних ресурсів СЕН;

$r_{s_s}^{(3)}$ – отримання якісних знань, навиків та умінь згідно навчальної програми;

$r_{s_s}^{(4)}$ – об'єктивності вимірювання рівнів його навченості;

$r_{s_s}^{(5)}$ – володіння особистими навчальними досягненнями, які зафіксовані в базах даних навчальної інформації;

$r_{s_s}^{(6)}$ – конфіденційності інформації, яка циркулює у всіх його взаємодіях із СЕН;

$r_{s_s}^{(7)}$ – конфіденційності персональних даних.

Викладач отримує, зокрема, наступні права та обов'язки:

$r_{s_2}^{(1)}$ – особистої участі у всіх взаємодіях в рамках СЕН, передбачених навчальною програмою;

$r_{s_2}^{(2)}$ – конфіденційності інформації, яка циркулює у всіх його взаємодіях із СЕН;

$r_{s_2}^{(3)}$ – індивідуальної організації навчального контенту;

$r_{s_2}^{(4)}$ – конфіденційності персональних даних;

$r_{s_2}^{(5)}$ – особистого доступу до інформаційних ресурсів СЕН;

$r_{s_2}^{(6)}$ – об'єктивності вимірювання рівнів навченості студентів.

4. Формування множини специфічних загроз

Можна виділити такі типи загроз:

- Порушення будь-якого із прав та обов'язків множини R_S;
- Порушення будь-якого із правил безпечного доступу до об'єктів множини P_O.

Ці порушення, хоч поодинокі чи систематичні, призводять до зниження якості освіти та порушення прав інших учасників навчального процесу. Кожне з таких потенційних порушень являє собою загрозу t з множини специфічних загроз T ($t \in T$).

Надалі розглянемо, для прикладу, специфічні загрози першого типу в рамках взаємодії «студент-викладач», які зумовлені порушенням прав і обов'язків множини R_S.

Загрози в рамках взаємодії «студент-викладач», суб'єктом яких виступає студент:

$t_{s_1}^{(1)}$ – відмовляється від особистої участі у взаємодії в рамках СЕН, своє суверенне право добровільно передає іншій особі;

$t_{s_1}^{(2)}$ – передає право доступу до інформаційних ресурсів СЕН іншій особі, що дає можливість вчитися неавторизованим користувачам;

$t_{s_1}^{(3)}$ – відмовляється від отримання якісних знань, навиків та умінь, наприклад, не виконує систематично завдання, списує, чи отримує сторонню допомогу (підказування), не відмовляючись при цьому від права на володіння особистими навчальними досягненнями;

$t_{s_1}^{(4)}$ – відмовляється від об'єктивності оцінювання, наприклад, підкуповує викладача;

$t_{s_1}^{(5)}$ – відмовляючись від особистої участі у взаємодії в рамках СЕН, студент автоматично розкриває іншій особі конфіденційну інформацію, яка циркулює у всіх його взаємодіях, що може призводити до порушення права на конфіденційність інших учасників СЕН.

Далі наведемо опис виявлених специфічних загроз за такою схемою: суб'єкт виникнення загрози, об'єкт загрози, вразливість СЕН, яка спричинює появу загрози, та потенційні наслідки від реалізації загрози.

$t_{s_1}^{(1)}$ – *«Добровільна підміна особи»*. **Суб'єктом** виникнення загрози є студент, який добровільно відмовляється від свого суверенного права. **Об'єктом** загрози є бази даних навчальної інформації та комунікаційний модуль, цілісність яких порушується за реалізації загрози. **Вразливістю** СЕН є недосконаліть системи автентифікації. **Потенційні наслідки** від реалізації загрози: компрометація документа про освіту, порушення цілісності баз даних навчальної інформації, розкриття іншій особі конфіденційної інформації, яка циркулює у всіх його взаємодіях, що може призводити до порушення права на конфіденційність інших учасників СЕН.

$t_{s_1}^{(2)}$ – *«Несанкціонована передача прав доступу до ресурсів СЕН»*. **Суб'єктом** виникнення загрози є студент, який надає свої автентифікаційні дані сторонній особі за певну грошову винагороду чи за дружніми взаємовідносинами. **Об'єктом** загрози є репозиторій навчального контенту, до якого здійснюється несанкціонований доступ. **Вразливістю** є недосконаліть системи автентифікації СЕН. **Потенційні наслідки** від реалізації загрози: призводить до порушення авторських прав, недоотримання прибутків власниками СЕН, розкриття іншій особі конфіденційної інформації, що може призводити до порушення права на конфіденційність інших учасників СЕН.

$t_{s_1}^{(3)}$ – *«Порушення правил навчального процесу»*. **Суб'єктом** загрози є несумлінний студент, який списує, використовує підказки. **Об'єктом** загрози є бази даних навчальної інформації, цілісність якої порушується. **Вразливістю** є організаційні недоліки СЕН. **Потенційні наслідки** від реалізації загрози: невідповідність знань студента навчальній програмі.

$t_{s_1}^{(4)}$ – *«Загроза об'єктивності оцінювання»*. **Суб'єктами** загрози виступають як студент, так і викладач, оскільки, незважаючи на те, що ініціатором реалізації загрози є студент, без згоди викладача ця загроза не реалізується. **Об'єктами** загрози є база даних навчальної інформації та система оцінювання, цілісність яких порушується. **Вразливістю** є організаційні недоліки СЕН. **Потенційні наслідки** від реалізації загрози: компрометація документа про освіту, порушення цілісності баз даних навчальної інформації.

$t_{s_1}^{(5)}$ – *«Непряме порушення права на конфіденційність інших осіб»*. **Суб'єктом** загрози виступає студент, який відмовляється від особистої участі у взаємодіях в СЕН. **Об'єктом** загрози база даних навчальної інформації, конфіденційність якої порушується. **Вразливістю** є недосконаліть системи автентифікації СЕН. **Потенційні наслідки** від реалізації загрози: порушення права на конфіденційність інших учасників СЕН.

, Висновки

1. Запропоновано підхід до виявлення та аналізу специфічних загроз інформаційній безпеці систем електронного навчання.
2. На основі розробленого підходу проаналізовано взаємодію «студент-викладач» та виявлено специфічні загрози, суб'єктом яких виступає студент.
3. В подальших дослідженнях необхідно сформувати якомога повнішу множину специфічних загроз безпеці СЕН та розробити методи і засоби, які дозволять убезпечитися від них.

Список використаних джерел

1. Закон України Про захист персональних даних. / Верховна Рада України // Відомості Верховної Ради України. – Київ, 2012. - №34. – ст. 481. 2. Christian Josef Eibl. Discussion of Informtion Security in E-Learning. / Christian Josef Eibl // SIegen University, Department of Electrotechnics and Informatics, 2010. 3. Спирягин М.И., Спирягин В.И., Клюев С.А., Валуйский Е.А., Усенко Ф.П. Использование смарт-карт для защиты информации в процессе дистанционного обучения. / Спирягин М.И. // Проблеми програмування. – Київ, Національна академія наук України, Інститут програмних систем, 2006. - №2-3. Спеціальний випус. – С.226-230. 4. Defta Costinela-Luminita. Security issues in e-learning platforms. / Defta Costinela-Luminita // World Journal on Educational Technology. – Cyprus, Academic World Education and Research Center, 2011. – Vol.3, issue 3. – pp. 153-167. 5. Hajwa Hayaati Mohd Alwi, Ip-Shing Fan. E-Learning and Information Security Management. / Hajwa Hayaati Mohd Alwi, Ip-Shing Fan // International Journal of Digital Society. – United Kingdom, Cranfield University, 2010. – Vol. 1, issue 2. – pp. 148-156. 6. Чекурін В.Ф., Будік О.О. Взаємодія об'єктів і аналіз загроз інформаційній безпеці систем електронного навчання. / Чекурін В.Ф., Будік О.О. // Вісник Східноукраїнського національного університету ім. В.Даля. – Луганськ, Видавництво СНУ ім. В.Даля, 2011. - №7 (161), Ч1. – С.112-119. 7. Чекурін В.Ф., Будік О.О. Підхід до формування вимог інформаційної безпеки систем електронного навчання. / Чекурін В.Ф., Будік О.О. // Вісник Національного університету «Львівська політехніка». – Львів, Видавництво НУ ЛП, 2011. - Автоматика, вимірювання та керування, №695. – С.133-140. 8. Офіційний сайт IEEE - http://www.ieee.org.