УДК: 65.012.8 DOI 10.33111/mise.101.3

Бєгун А.В., к.е.н., професор,
професор кафедри комп'ютерної математики та інформаційної безпеки,
ДВНЗ «КНЕУ імені Вадима Гетьмана»
Плахтій М.О., к.е.н.,
член української асоціації «UVCA» та громадської Ради
Державної служби інтелектуальної власності України,
директор ТОВ Front Manager
Осипова О.І., к.е.н., доцент,
доцент кафедри математичного моделювання та статистики,
ДВНЗ «КНЕУ імені Вадима Гетьмана»
Урденко О.Г., аспірант
кафедри комп'ютерної математики та інформаційної безпеки,
ДВНЗ «КНЕУ імені Вадима Гетьмана»

Biehun A.V., PhD in Economics,
Professor of the Department of Computer Mathematics
and Information Security,
SHEI KNEU named after V. Hetman
Plakhtiy M.O., PhD in Economics,
member of the Ukrainian Association "UVCA" and the Public Council
of the State Intellectual Property Service of Ukraine,
director of Front Manager LLC
Osypova O. I., PhD in Economics,
Associate Professor of the Department of Mathematical Modeling
and Statistics,
SHEI KNEU named after V. Hetman
Urdenko O. G.,
Postgraduate Student of the Department of Computer Mathematics
and Information Security, SHEI KNEU named after V. Hetman

АНАЛІЗ ЗОВНІШНІХ ТА ВНУТРІШНІХ ЗАГРОЗ ФУНКЦІОНУВАННЯ ЕЛЕКТРОННОГО КВИТКА НА ВИДОВИЩНІ ЗАХОДИ

THE ANALYSIS OF EXTERNAL AND INTERNAL THREATS OF ELECTRONIC TICKET FUNCTIONING AT ENTERTAINMENT EVENTS

Анотація. *Діяльність з продажу електронних квитків повною мірою піддається, як традиційним бізнес-загрозам, так і загрозам електронної комерції, створеним технологіями електронного бізнесу та широким використанням комп'ютерних і телекомунікаційних технологій. Загрози при операціях з продажу електронних квитків виникають практично на всіх етапах діяльності та зачіпають інтереси як продавців, так і покупців. Тому для компаній, що займаються продажем електронних квитків, очевидна необхідність комплексних заходів щодо виявлення та моніторингу таких загроз. Вирішення проблеми протидії загрозам безпеки підприємств, що здійснюють продаж електронних квитків на розважальні заходи, пов'язане насамперед із вирішенням питань захисту використовуваних у ньому інформаційних технологій, тобто забезпечення інформаційної безпеки. Класифікація загроз інформаційній безпеці є важливим*

етапом оцінки безпеки інформаційних систем та розробки заходів щодо забезпечення інформаційної безпеки підприємства. У даному дослідженні, яке має науково-методичний характер, класифіковано та систематизовано загрози, які супроводжують діяльність у сфері електронних квитків на розважальні заходи. Класифікація загроз інформаційній безпеці підприємств, що займаються продажем електронних квитків на розважальні заходи, здійснюється на основі поєднання таких критеріїв:
1) походження загрози: зовнішні та внутрішні загрози;
2) джерела загроз: загрози, викликані діяльністю людини; загрози, джерелом яких є програмне та апаратне забезпечення; загрози, які створює природне середовище;
3) намір реалізувати загрозу безпеці: навмисні та ненавмисні дії порушника.
Результати класифікації загроз інформаційної безпеки можуть бути в подальшому використані в процесі проведення аудиту інформаційної безпеки підприємства. Також у роботі розглянуто конкретні програмні рішення для проведення аудиту інформаційної безпеки підприємства.
Ключові слова: *електронні квитки, розважальні заходи, загрози інформаційної безпеки, аудит інформаційної безпеки*

Abstract. *E-ticketing activities are fully inherent in both traditional business threats and e-commerce threats posed by e-business technologies and the widespread use of computer and telecommunications technology. Threats in the sale of electronic tickets arise at almost all stages of activity and affect the interests of both sellers and buyers. Therefore, the need for comprehensive measures to identify and monitor threats is obvious to companies engaged in the sale of electronic tickets. The solution to the problem of counteracting the security threats of enterprises engaged in the sale of electronic tickets to entertainment events, primarily related to addressing the protection of information technology used in it, ie to ensure information security. The classification of threats to information security is an important step in assessing the security of information systems and the development of measures to ensure information security of the enterprise. In this study, which has a scientific and methodological nature, classified and systematized the threats that accompany the activities in the field of electronic tickets for entertainment events. The classification of threats to information security of enterprises engaged in the sale of electronic tickets to entertainment events is carried out on the basis of a combination of the following criteria:*
1. The origin of the threat: external and internal threats.
2. Sources of threats: threats caused by human activities; threats, the source of which are software and hardware; threats posed by the natural environment.
3. Intention to realize a security threat: intentional and unintentional actions of the violator.
The results of the classification of information security threats can be further used in the process of conducting an information security audit of the enterprise.
Specific software solutions for conducting an information security audit of the enterprise are also considered.
Keywords: *E-ticketing, entertainment events, threats of information security, information security audit*

Вступ. Протягом останніх десятиліть розвиток комп'ютерних технологій і розповсюдження використання Інтернету призвели до істотних змін у способах ведення бізнесу. Електронна комерція розвинулася як новий ринок, що створює можливості для зростання у багатьох галузях економіки. Індустрія дозвілля та розваг є однією з

таких галузей, оскільки з розповсюдженням Інтернету досить швидко почала впроваджувати продаж електронних квитків на видовищні заходи. Заміна традиційних паперових квитків електронними квитками виявилася ефективною комерційною практикою для підприємств, що працюють в індустрії дозвілля та розваг. Дійсно, електронний квиток — це чудовий інструмент економії коштів, оскільки він може знизити та навіть усунути витрати, пов'язані з друком, доставкою, зберіганням та продажем квитків. Також електронний квиток має ряд переваг порівняно з паперовим квитком для покупців — простота та швидкість купівлі, електронний квиток неможливо пошкодити, загубити тощо. Крім того інтеграція в квитковий бізнес електронних платежів і системи електронних замовлень дозволяє отримувати важливі маркетингові дані про смаки, споживчі переваги, цінності, доходи покупців. За допомогою IT-технологій і Big data аналітиці підприємства, що займаються продажем електронних квитків, можуть формувати докладні бази даних про своїх покупців, здійснювати електронну розсилку новин, надавати статистичні, візуальні і рекламні матеріали [1].

Однак, діяльності в сфері продажу електронних квитків в повній мірі притаманні як традиційні підприємницькі ризики, так і специфічні для електронної комерції ризики, породжені технологіями електронного бізнесу та широким застосуванням засобів комп'ютерної та телекомунікаційної техніки. Зокрема, такі ризики, як: ризик порушення конфіденційності інформації; ризик спотворення інформації; ризик втрати інформації; ризик збою інформації. Причини виникнення цих ризиків криються у специфічних загрозах електронної діяльності і включають у себе зовнішні (віруси і шкідливі програми; хакерські атаки; шахрайства; спам; загроза заволодіння інтелектуальною власністю правовласника) і внутрішні загрози (крадіжка інформації; саботаж; недостатній професіоналізм або недбалість співробітників). Таким чином, ризики в торгівлі електронними квитками виникають практично на всіх етапах діяльності і зачіпають інтереси як продавців, так і покупців. Тому необхідність проведення комплексних заходів щодо виявлення, управління та моніторингу загроз є очевидною для підприємств, що займаються продажем електронних квитків. І особливої актуальності дана проблема набуває зараз, коли індустрія видовищних заходів переживає глибоку кризу і тільки починає відновлюватись після півторарічного простою, спричиненого пандемією Covid-19 [2].

Тому метою даної роботи є ідентифікація та систематизація загроз, що супроводжують діяльність у сфері реалізації електронних квитків на видовищні заходи.

Для досягнення поставленої мети ми ставимо перед собою такі завдання:

1) ідентифікувати та класифікувати загрози, що супроводжують діяльність у сфері продажу електронних квитків на видовищні заходи;

2) дати коротку характеристику програмним інструментам IT-аудиту, що можуть бути використані підприємствами, які займаються реалізацією електронних квитків на видовищні заходи, з метою виявлення та протидії основних загроз.

Практична цінність роботи полягає у можливості використання результатів проведеного дослідження в процесі аудиту інформаційної безпеки на підприємствах, що займаються продажем електронних квитків на видовищні заходи.

Загрози, що супроводжують діяльність у сфері продажу електронних квитків на видовищні заходи. Компанії у ході здійснення своєї професійної діяльності стикаються з різноманітними загрозами, які, так чи інакше, впливають, на ведення бізнесу, і негативно позначаються на фінансовому становищі організації. Сучасний стан справ бізнесу диктує необхідність використання в роботі компаній, обґрунтованих технічних і економічних методів і засобів, що дозволяють кількісно і якісно вимірювати загрози діяльності компанії, а також адекватно оцінювати фінансування витрат на заходи щодо протидії цим загрозам. Побудова практично будь-якої системи моніторингу загроз має починатися з ідентифікації можливих загроз: необхідно точно визначити, які умови і чинники можуть негативно вплинути на діяльність компанії і оцінити наскільки вони потенційно небезпечні. Класифікація загроз дає можливість структурувати всі потенційні загрози, обрати оптимальний варіант рішення на основі класифікаційних ознак, допомагає орієнтуватися в різноманітті існуючих загроз і є джерелом інформації про них [3].

Система продажу електронних квитків — це велика і складна система з величезною структурою і широким спектром загроз з усіх боків. Як уже було зазначено, діяльності в сфері продажу електронних квитків у повній мірі притаманні як традиційні підприємницькі ризики та загрози, так і специфічні для електронної комерції загрози, породжені технологіями електронного бізнесу та широким застосуванням засобів комп'ютерної та телекомунікаційної техніки.

Основними джерелами виникнення загроз, що супроводжують діяльність у сфері продажу електронних квитків на видовищні заходи, є [4]:

1) **зовнішнє бізнес середовище.** Цілком законні дії інших учасників бізнесу та зміни в зовнішньому бізнес-середовищі можуть загрожувати компанії. Прикладом загроз можуть бути зміни в поведінці клієнтів, ефективність роботи постачальників та обмінний курс;

2) **злочинна діяльність людей або організацій.** Сюди відносяться загрози, що пов'язані з тими особами чи організаціями, які з будь-якої причини мають намір займатися діяльністю, яка є незаконною (або, принаймні, неетичною) та потенційно руйнівною для бізнесу. Приклади таких дій включають: шахрайство, псування матеріальних цінностей компанії, відмову в обслуговуванні, вірусні атаки і т.д.;

3) **правова система.** Окрім нового законодавства, що запроваджується у відповідь на стрімкий розвиток електронного бізнесу, важливо пам'ятати, що всі звичні правила, що регулюють звичайну підприємницьку діяльність, також діють і для підприємств, що займаються електронною комерцією! Необхідно також враховувати законодавство інших країн, в яких компанія може здійснювати свою діяльність через канали електронного бізнесу;

4) **бізнес-стратегія підприємства.** Помилковий вибір основних напрямів діяльності, неможливість побудови ефективної комунікації з клієнтами та постачальниками, неефективна організація основних бізнес-процесів на підприємстві здатні породжувати ризики в підприємницькій діяльності;

5) **Менеджмент та персонал компанії.** Ще одним істотним джерелом ризиків є працівники компанії. Неефективний менеджмент, незрозумілі права та обов'язки, недосконала система управління персоналом, недостатня кваліфікація працівників є потенційними факторами ризику в компанії;

6) **технології.** Інформаційні та комунікаційні технології лежать в основі діяльності в сфері продажу електронних квитків. Клієнти, постачальники, співробітники і багато інших людей щодня використовують інформаційно-комунікаційні технології для купівлі або продажу електронних квитків. При цьому дані учасники відносин чекають дотримання конфіденційності та цілісності інформації, що надається ними.

Рішення проблеми протидії загрозам безпеки підприємств, що займаються діяльністю у сфері реалізації електронних квитків на видовищні заходи, в першу чергу пов'язано з вирішенням питань захисту інформаційних технологій, застосовуваних у ній, тобто із забезпеченням інформаційної безпеки.

У широкому сенсі під загрозою (взагалі) зазвичай розуміють потенційно можливу подію, процес або явище, які можуть (впливаючи на що-небудь) привести до нанесення збитку чиїмось інтересам.

Загрозою інтересам суб'єктів інформаційних відносин будемо називати потенційно можливу подію, процес або явище, які за допомогою впливу на інформацію, її носії та процеси обробки можуть прямо або побічно призвести до нанесення шкоди інтересам даних суб'єктів.

Джерело загрози — це потенційні антропогенні, техногенні або стихійні носії загрози безпеки.

Основними джерелами загроз інформаційній безпеці є:

• стихійні лиха і аварії (повінь, ураган, землетрус, пожежа тощо);

• збої і відмови в роботі устаткування (технічних засобів);

• помилки проектування і розробки компонентів програмних та апаратних засобів (апаратних засобів, технології обробки інформації, програм, структур даних і т.п.);

• помилки експлуатації (користувачів, операторів та іншого персоналу);

• навмисні дії порушників і зловмисників (скривджених осіб з числа персоналу, злочинців, шпигунів, диверсантів і т.п.).

Класифікація загроз інформаційної безпеки на підприємствах, що займаються реалізацією електронних квитків на видовищні заходи. Класифікація загроз інформаційній безпеці особливо важлива при оцінці захищеності інформаційних систем в реальних умовах експлуатації [5]. Усі загрози безпеки спрямовані проти програмних і технічних засобів інформаційної системи. В кінцевому підсумку, ці загрози впливають на безпеку інформаційних ресурсів і призводять до порушення основних властивостей зберігання та обробки інформації.

В роботах [5, 6] для класифікації загроз інформаційній безпеці запропоновано поєднувати такі критерії:

1) походження загрози: зовнішні та внутрішні загрози;

2) джерела загроз:

✓ загрози, що обумовлені людською діяльністю;

✓ загрози, джерелом яких є програмно-апаратні засоби;

✓ загрози, джерелом яких є природне середовище.

Джерелами 1-ї групи загроз безпеці інформації виступають суб'єкти, дії яких можуть бути кваліфіковані як умисні або випадкові злочини. Ця група найобширніша і представляє найбільший інтерес з точки зору організації захисту, так як дії суб'єкта завжди можна оцінити, спрогнозувати і прийняти адекватні заходи. Ме-

тоди протидії у цьому випадку керовані і безпосередньо залежать від волі організаторів захисту інформації.

Джерела загроз 2-ї групи менш прогнозовані, безпосередньо залежать від властивостей техніки і тому вимагають особливої уваги. Даний клас джерел загроз безпеці інформації є особливо актуальним у сучасних умовах, так як функціонування бізнесу, а особливо електронний бізнес, засновано на широкому використанні інформаційно-комунікаційних технологій.

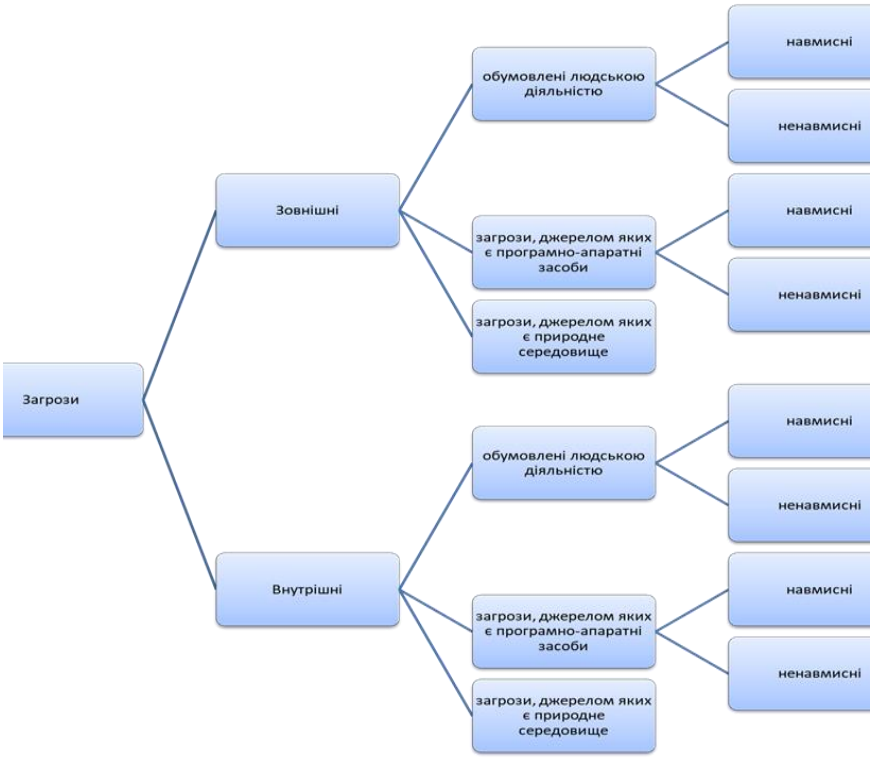

Рис. 1. Класифікація загроз інформаційної безпеки

Третя група джерел загроз об’єднує, обставини, що становлять непереборну силу, тобто такі обставини, які носять об’єктивний і абсолютний характер, поширюється на всіх. Такі джерела загроз майже не піддаються прогнозуванню і тому заходи захисту від них повинні застосовуватися завжди. Стихійні джерела потенційних загроз інформаційній безпеці, як правило, є зовнішніми по

відношенню до захищається і під ними розуміються, перш за все, природні катаклізми;

3) намір реалізувати загрозу безпеці:

✓ навмисні дії порушника;

✓ ненавмисні дії порушника.

Схематично такий процес класифікації загроз інформаційної безпеки подано на рис. 1

У табл. 1 наведено основні зовнішні загрози інформаційній безпеці підприємства, що займається реалізацією електронних квитків на видовищні заходи, залежно від джерела походження загрози.

Таблиця 1

ЗОВНІШНІ ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ПІДПРИЄМСТВА, ЩО ЗАЙМАЄТЬСЯ РЕАЛІЗАЦІЄЮ ЕЛЕКТРОННИХ КВИТКІВ НА ВИДОВИЩНІ ЗАХОДИ[1]

Загрози, що обумовлені людською діяльністю	**Загрози, джерелом яких є програмно-апаратні засоби**	**Загрози, джерелом яких є природне середовище**
✓ Несанкціонований продаж е-квитків третіми особами[1] ✓ Несанкціонована процедура верифікації е-квитків[1] ✓ Несанкціонований друк е-квитків[1] ✓ Хакерські атаки[1] ✓ Фішингові атаки[1] ✓ Вірусні атаки[1] ✓ Атака «жорсткою силою» [1] ✓ Впровадження SQL-коду[1] ✓ Міжсайтовий скріптінг[1] ✓ Блокування кошика на сайті продавця[1] ✓ Шахрайство з кредитними картками[1] ✓ DoS-атаки[1] ✓ Кіберсквотинг[1] ✓ Перехват веб-сторінки[1] ✓ Несанкціонований доступ до бази даних клієнтів заходу, модифікування даних у БД	✓ Перевантаження та зриви сайту чи мережі в пікові періоди[2] ✓ Збій в роботі інтернет-провайдеру[2] Ризик конфліктів із платіжною системою[2]	✓ Ушкодження/ поломка обладнання внаслідок настання форс-мажорних обставин природного характеру[2] ✓ Ушкодження/ знищення інформації внаслідок настання форс-мажорних обставин природного характеру[2] ✓ Пошкодження життєзабезпечуючих комунікацій (електропостачання, кондиціонування та вентиляція) внаслідок настання форс-мажорних обставин природного характеру[2]

[1] символом «[1]» позначено навмисні загрози, «[2]» — ненавмисні загрози, «[12]» — загрози, які можуть бути як навмисними, так і ненавмисними

У табл. 2 наведено основні внутрішні загрози інформаційній безпеці підприємства, що займається реалізацією електронних квитків на видовищні заходи, залежно від джерела походження загрози. Так як загрози, джерелом яких є навколишнє середовище, в основному є загрозами зовнішнього походження, в табл. 2 ця група загроз не представлена.

Таблиця 2

ВНУТРІШНІ ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ПІДПРИЄМСТВА, ЩО ЗАЙМАЄТЬСЯ РЕАЛІЗАЦІЄЮ ЕЛЕКТРОННИХ КВИТКІВ НА ВИДОВИЩНІ ЗАХОДИ[2]

Загрози, що обумовлені людською діяльністю	**Загрози, джерелом яких є програмно-апаратні засоби**
• Неправомірне відключення обладнання або зміна режимів роботи пристроїв і програм[12] • Псування носіїв інформації персоналом[12] • Нелегальне впровадження та використання програм[12] • Ігнорування організаційних обмежень (установлених правил) при роботі в системі[12] • Некомпетентне використання, настроювання або неправомірне відключення засобів захисту персоналом служби безпеки[12] • Пересилання даних за помилковою адресою абонента (пристрої) [12] • Введення помилкових даних[12]	• Відсутність брандмауера[12] • Втрата аудиторського сліду[12] • Використання неліцензійного програмного забезпечення[12] • Помилка чи упущення в розробці програмного забезпечення[12] • Порушення ідентифікації та авторизації[12] • Порушення захисту від зловмисного ПЗ[12] • Порушення в роботі допоміжних технічних засобів (охорони, сигналізації, телефонії) [12]

Результати класифікації загроз інформаційній безпеці в подальшому можуть використовуватись у процесі проведення аудиту інформаційної безпеки підприємства.

Далі розглянемо конкретні програмні рішення для проведення аудиту інформаційної безпеки підприємства.

Програмні інструменти IT-аудиту на підприємствах, що займаються реалізацією електронних квитків на видовищні заходи. Сьогодні інструменти аудиту стають усе важливішими для IT-аудитора. Наразі інструменти аудиту відіграють ключову роль у розумінні того, як функціонують інформаційні системи, адже IT-середовища, додатки, онлайн транзакції, тощо, стають дедалі складнішими та інтегрованими у всі сфери

[2] символом «[1]» позначено навмисні загрози, «[2]» — ненавмисні загрози, «[12]» — загрози, які можуть бути як навмисними, так і ненавмисними

діяльності підприємства. Відповідно для кожного IT-аудиту аудитор має чітко визначити, чи має він потребу у використанні спеціальних інструментів аудиту і головне — які саме інструменти аудиту варто використати для досягнення найкращих результатів. Офіційно спеціальні інструменти аудиту мають назву Інструменти і прийоми комп'ютеризованої підтримки аудиту (CAATTs) [7, 8].

Зважаючи на те, що CAATTs дозволяють аудитору аналізувати великі об'єми даних, IT-аудит на підприємствах, що займаються реалізацією електронних квитків із використанням CAATT дозволяє виконати комплексний аналіз, охопивши всі операції та зафіксувати відхилення, як-то дублювання покупців, продавців або транзакцій.

Також беззаперечною перевагою використання CAATTs на підприємствах, що займаються реалізацією електронних квитків, є широкі можливості CAATTs у сфері тестування надійності вебсайтів і глибшого розуміння IT-інфраструктури компанії (апаратне забезпечення і мережеві зв'язки). У табл. 3 наведено перелік найбільш адаптованих для потреб електронного бізнесу CAATTs та їх коротку характеристику [7].

Висновки. Діяльності в сфері продажу електронних квитків у повній мірі притаманні як традиційні для підприємницької діяльності загрози, так і специфічні для електронної комерції загрози, породжені технологіями електронного бізнесу та широким застосуванням засобів комп'ютерної та телекомунікаційної техніки. Загрози при торгівлі електронними квитками виникають практично на всіх етапах діяльності і зачіпають інтереси як продавців, так і покупців.

Таблиця 3

ІНСТРУМЕНТИ І ПРИЙОМИ КОМП'ЮТЕРИЗОВАНОЇ ПІДТРИМКИ АУДИТУ

Назва CAATTs	Коротка характеристика
Аналіз безпеки Microsoft	Може ефективно використовуватися з метою оцінювання рівня прогалин в операційних системах Microsoft та важливих налаштувань, що пов'язані із безпекою. Вартість: безкоштовно
Тестер SSL Labs	Дозволяє оцінити якість зашифрованого зв'язку і отримати детальний звіт. Вартість: безкоштовно
NMAP	Дний продукт являє собою сканер безпеки, який допомагає виявити хости і сервіси в комп'ютерній мережі та створити таким чином «карту» мережі. Вартість: безкоштовно

Закінчення табл. 3

Назва CAATTs	Коротка характеристика
OWASPZAP	Являє собою легкий та зручний у використанні програмний продукт для виявлення вразливих місць у веб-додатках. Вартість: безкоштовно
Sptunk	Цей інтегрований інструмент дозволяє збирати, індексувати та заносити в режимі реального часу дані реєстру в сховище пошуку та потім генерувати графіки, звіти, тощо. Вартість: є безкоштовним для особистого використання (до 500 МБ на день)
Hexicon Disco	Дозволяє здійснювати аналіз бізнес-процесів на основі реєстру подій. Основною метою використання даного програмного рішення є отримання нових знань з реєстру подій, що записується інформаційною системою. Вартість: залежно від комплектації, з обмеженим функціоналом можна завантажити безкоштовно
IDEA	Представляє собою інструмент аналізу даних, що призначений суттєво прискорити та підвищити ефективність проведення IT-аудиту і виявити недоліки системи контролю. Вартість: залежно від комплектації
Olikview	Являє собою потужну платформу бізнес-інтелекту, яку також можуть використовувати аудитори в процесі IT-аудиту. Вартість: залежно від комплектації, з обмеженим функціоналом можна завантажити безкоштовно
BWISE	Представляє собою програмне забезпечення для корпоративного управління, яке аудитори можуть використовувати для проведення IT-аудиту. Вартість: залежно від комплектації

Тому необхідність проведення комплексних заходів щодо виявлення та моніторингу загроз є очевидною для підприємств, що займаються продажем електронних квитків.

Рішення проблеми протидії загрозам безпеки підприємств, що займаються діяльністю у сфері реалізації електронних квитків на видовищні заходи, в першу чергу пов’язано з вирішенням питань захисту інформаційних технологій, застосовуваних у ній, тобто із забезпеченням інформаційної безпеки. При цьому класифікація загроз інформаційній безпеці є важливим етапом при оцінці захищеності інформаційних систем та розробці заходів щодо забезпечення інформаційної безпеки підприємства.

У роботі класифікація загроз інформаційній безпеці підприємств, що займаються діяльністю у сфері реалізації електронних квитків на видовищні заходи, проведена на основі поєднання таких критеріїв:

1. походження загрози: зовнішні та внутрішні загрози;
2. джерела загроз: загрози, що обумовлені людською діяльністю; загрози, джерелом яких є програмно-апаратні засоби; загрози, джерелом яких є природне середовище;
3. намір реалізувати загрозу безпеці: навмисні та ненавмисні дії порушника.

Результати класифікації загроз інформаційній безпеці в подальшому можуть використовуватись у процесі проведення аудиту інформаційної безпеки підприємства.

Також розглянуто конкретні програмні рішення для проведення аудиту інформаційної безпеки підприємства, що займається продажем квитків на видовищні заходи.

Бібліографічні посилання

1. Сравнительный анализ билетных систем: [електронний ресурс]. — Режим доступу: http://www.sporteventcenter.ru/images/НИР_1_Тоцкая_сравнение_билетных_систем_в_спорте.pdf
2. Global Online Event Ticketing Industry: market impact survey — covid-19 & looming recession: [електронний ресурс]. — Режим доступу: https://www.reportlinker.com/p05819087/Global-Online-Event-Ticketing-Industry.html?utm_source=GNW
3. Класификация угроз информационной безопасности: [електронний ресурс]. — Режим доступу: https://www.cnews.ru/reviews/free/oldcom/security/elvis_class.shtml
4. Managing the Risks of e-Business: [електронний ресурс]. — Режим доступу: http://facultyresearch.london.edu/docs/03managingtherisksupton.doc
5. Zingming Zhao et al 2019 J. Phys.: Research on risk assessment technology of China's railway ticket selling and reservation systemConf. Ser. 1325 01200
6. Jouini, M., Rabai, L. B. A. and Aissa, A. B. (2014), "Classification of security threats in information systems", *Procedia Computer Science*, Jan1, Vol. 32, P. 489–496.
7. Практична методологія IT-аудиту: [електронний ресурс]. — Режим доступу: http://dkrs.kmu.gov.ua/kru/doccatalog/document?id=134082
8. Zhao, N., Yen, D.C. and Chang, I. (2004), "Auditing in the e-commerce era", Information Management & Computer Security, Vol. 12 No. 5, P. 389-400. https://doi.org/10.1108/09685220410563360

Статтю подано до редакції 27.10.2021