DOI 10.31489/2022Ped3/84-95

УДК 37.014

С.А. Абдыманапов, А.Б. Барлыбаев, Б.А. Алтынбек*

*Esil University, Нур-Султан, Казахстан*
*(Корреспондирующий автор. E-mail: berik_aa@mail.ru)*

# Методика оценки рисков информационной безопасности на примере анализа *Learning Management Systems*

Активное развитие и применение новых цифровых технологий в образовании, с одной стороны, открыло новые возможности для повышения эффективности управления бизнес-процессами вуза. С другой — привело к значительному увеличению угроз безопасности, повышая уязвимость образовательных учреждений для киберпреступников. В последние годы стремительный рост различного рода инцидентов показывает, что традиционные подходы к информационной безопасности недостаточны. Следовательно, оценка рисков информационной безопасности стала важной задачей для большинства учебных заведений. Было предложено несколько моделей, чтобы помочь образовательным учреждениям решать проблемы с построением информационной безопасности. В данной статье предложена новая иерархическая структурированная модель оценки рисков информационной безопасности в учебных заведениях с использованием нечеткой логики. Новый метод оценки рисков информационной безопасности также описан на примере автоматизированных систем управления или ERP-систем (на примере систем управления обучением). Предложенная оценка рисков университета была смоделирована с использованием нечеткой логики в виде 15 fuzzy машин. В ходе ряда экспериментов мы тщательно изучили оценку рисков информационной безопасности различных программных продуктов, используемых в вузах. Предлагаемый метод должен решить проблему гибкой оценки рисков.

*Ключевые слова:* моделирование бизнес-процессов в вузах, риски информационной безопасности, оценка рисков, стандарты оценки информационной безопасности, политика в области образования, работа в области образования, общественность, безопасность в области образования.



## *Введение*

Известно, что ни один вуз не может быть застрахован от утечки данных, и что, когда происходят нарушения, они могут иметь серьезные последствия. На нарушение данных можно по-разному смотреть в разных областях. Любое действие по нарушению безопасности защищенных данных, которое приводит к передаче данных неавторизованным объектам, может рассматриваться как нарушение информационной безопасности (ИБ). Нарушение безопасности может быть результатом кибератаки, кражи или потери устройств, кражи или утечки данных сотрудников, таких как учетные данные безопасности, и человеческих ошибок. Основные кибератаки на LMS включают внедрение SQL injection, crosssite scripting (XSS) и повышение привилегий. SQL-инъекция — одна из наиболее распространенных атак, которые могут разрушить базу данных путем размещения созданного вредоносного кода в операторах SQL через ввод веб-страницы. Однако никаких значительных исследований, посвященных изучению, сравнению и оценке подходов, используемых калькуляторами риска для расследования утечек данных, не проводилось. Разработка эффективного решения для кибербезопасности позволяет нам уменьшить утечки данных, которым угрожают риски кибербезопасности, такие как кибератаки на хранилище, обработку и управление базами данных. Организация кибербезопасности в жизнедеятельности остается одной из главных нерешенных задач в ИКТ сфере.

Гипотеза — проблема в том, что в образовательных учреждениях сложно управлять информационной безопасностью в сложных системах, такими как система ERP. Почему разработчики программного обеспечения не могут полностью обезопасить сложную систему? Что могут предложить разработчики программного обеспечения для улучшения информационной безопасности сложных систем? Это обнаруживает проблему в достижении безопасности при программировании сложных систем. Небрежное пользование сотрудниками или просчеты при построении информационной безопасности отразятся на репутации и финансовых потерях учебных заведений. Разработчики программного обеспечения могут использовать модели построения информационной безопасности, которые не подходят для сложных систем. Учитывая должное внимание к предыдущим старым моделям, необходима более гибкая модель оценки информационной безопасности.

Для сложных систем не существует конкретных моделей и стандартов оценки информационной безопасности. В любом случае это указывает на важность изучения всех известных моделей оценки информационной безопасности. Есть ряд хороших работ на тему «Как оценить информационную безопасность программного продукта»?

В этой статье Bo Feng, Qiang Li, Yuede Ji and others предлагают новую модель анализа пользователей для поиска потенциальных жертв путем анализа большого количества личной информации и поведения пользователей в социальных сетях. Модель оценивает риск безопасности [1]. Pil Sung Woo, Sang Sun Hwang, Soon Hyun Hwang, Balho H. Kim провели исследование о теоретическом стандарте для создания безопасных систем путем анализа структуры системы управления информацией о мощности в дополнение к количественной оценке риска кибератак, которые остаются мало изученными [2]. В этой статье T. Kieras, M. Junaid Farooq, Q. Zhu описали Risk Analysis of IoT Supply Chain Threats (RIoTS), структуру оценки рисков безопасности, заимствованную из теории надежности систем, чтобы включить цепочку поставок [3]. Smart Grid Security Classification (SGSC) связан с методами анализа рисков (ANSSI standard methodology) с той разницей, что SGSC метод классификации имеет цель присвоить системе класс безопасности на основе (комбинаций) оценок, присвоенных различным аспектам уязвимости системы и соответствующим реализованным механизмам защиты [4]. В этой статье J.D. Marcovic-Petrovic, M.D. Stojanovic, S.V. Bostjancic Rakas предложили новый метод оценки рисков безопасности в сетях диспетчерского управления и сбора данных (SCADA) с использованием нечеткой логики [5]. W. Wang, F. Shi, M. Zhang, C. Xu, J. Zheng предложили метод ранжирования на основе разнородной информационной сети для оценки риска уязвимости в конкретной сети [6]. J. Wang, M. Neil, N. Fenton получили комбинированный подход «Extended Factor Analysis of Information Risk-Bayesian Networks» (EFBN), используя симуляцию Монте-Карло, и показали, что он может предоставить интегрированное решение для оценки рисков кибербезопасности и принятия соответствующих решений [7]. Это исследование направлено на представление наиболее популярных и интересных алгоритмов, используемых в настоящее время [8]. Исследуемый подход состоит из кластеризации уязвимостей путем использования текстовой информации в записях уязвимостей, а затем моделирования функции среднего значения уязвимостей путем ослабления предположения о монотонной функции интенсивности, которое преобладает в исследованиях, в которых используются модели надежности программного обеспечения (SRM) и неоднородный пуассоновский процесс в моделировании [9]. В этой статье Pan K., Teixeira A., Lopez C.D., Palensky P. проанализировали кибербезопасность системы управления энергопотреблением (EMS) от атак на данные. Результаты показывают, насколько уязвима EMS для атак на данные и как совместное моделирование может помочь в оценке уязвимости [10]. В этом исследовании представлены и сравниваются существующие методы Cyber Third-Party Risk Management (C-TPRM), созданные разными компаниями, для выявления наиболее часто используемых индикаторов и критериев оценок [11].

Стандарты кибербезопасности — это опубликованные материалы, в которых изложены методы, которые ориентированы на защиту киберсреды пользователя. Основная цель — снизить риски, в том числе предотвратить или смягчить кибератаки. Эти опубликованные материалы состоят из сборников инструментов, политик, концепций безопасности, мер безопасности, руководств, подходов к управлению рисками, действий, обучения, передовых методов, гарантий и технологий.

Основные стандарты по информационной безопасности:

1. ISO/IEC 27000 — Системы управления информационной безопасностью.

2. ISO/IEC 27001 — Информационные технологии — Методы обеспечения безопасности — Системы управления информационной безопасностью — Требования. Выпуск стандарта 2013 г. определяет систему управления информационной безопасностью таким же формализованным, структурированным и кратким образом, как другие стандарты ИСО определяют другие виды систем управления.

3. ISO/IEC 27002 — Кодекс практики для средств контроля информационной безопасности — по сути, подробный каталог средств контроля информационной безопасности, которыми можно управлять с помощью СУИБ.

4. ISO/IEC 27003 — Руководство по внедрению системы управления информационной безопасностью.

5. ISO 15408 — Этот стандарт разрабатывает так называемые «Общие критерии». Это позволяет безопасно интегрировать и протестировать множество различных программных и аппаратных продуктов.

6. IEC 62443 — Стандарт кибербезопасности определяет процессы, методы и требования к системам промышленной автоматизации и управления (СПАУ).

7. ETSI EN 303 645 — Стандарт содержит набор базовых требований к безопасности потребительских устройств Интернета вещей (IoT).

*Критерии оценки риска*

Нам необходимо определить критерии и метрики для оценки информационной безопасности программного обеспечения путем анализа вышеупомянутых стандартов. На основе междисциплинарного анализа (упомянутые выше исследования и стандарты) составлен перечень, состоящий из 50 рисков ИБ, который можно использовать в практической деятельности предприятия, поскольку нейтрализация (ликвидация, минимизация) рисков ИБ составляет сущность и содержание процесса обеспечения ИБ университета. На базе предложенного перечня могут быть также построены модели угроз, на основании которых осуществляется постановка задач на создание СИБ. Кроме того, перечень конкретных рисков может использоваться в ходе оценки влияния принимаемых мер ИБ на эффективность деятельности предприятия. Риски ИБ представлены в таблице 1.

Таблица 1

**Структура рисков**

| № | Risks |
|---|---|
| 1 | 2 |
| | 1. Organizational risks |
| | 1.1. Documentation risks |
| 1 | 1.1.1. Lack of signaling means in case of emergency situations. |
| 2 | 1.1.2. Lack of regulations for actions of information security employees in the event of an emergency situation. |
| 3 | 1.1.3. Uncontrolled use and write-off of information carriers. |
| 4 | 1.1.4. Lack of video surveillance systems for key nodes of information systems, access control to work premises. |
| 5 | 1.1.5. Uncontrolled use of the Internet. |
| | 1.2. Human risks |
| 6 | 1.2.1. Personnel errors, low qualifications. |
| 7 | 1.2.2. Intentional harm by disloyal employees. |
| 8 | 1.2.3. Malicious actions of the network administrator. |
| 9 | 1.2.4. Combining the duties of an Information System administrator and an Information Security administrator. |
| 10 | 1.2.5. Malicious acts when servicing. |
| | 2. Reputation (branding) risks |
| 11 | 2.1. Dissemination in the external environment of information of an economic nature that threatens the company's reputation. |
| 12 | 2.2. Mentioning a company in the context of extremism, money laundering, cyber threats and cyber terrorism. |
| 13 | 2.3. Use of uncertified and unlicensed products. |
| 14 | 2.4. Possibility of external penetration into the company’s Intranet system. |
| | 3. Privacy risks |
| | 3.1. Privacy regulations |
| 15 | 3.1.1. Lack of clear regulations for working with personal data. |
| 16 | 3.1.2. Acceptance of untested cryptographic information protection devices into operation. |
| 17 | 3.1.3. Lack of monitoring and analysis procedures for all performed operations. |
| 18 | 3.1.4. Lack of organizational procedures that allow for internal investigations of violations of confidentiality risks. |
| | 3.2. Authorization |
| 19 | 3.2.1. Long-term preservation of the authorization window in case of inactivity or in the event of an employee leaving the premises. |

| 1 | 2 |
|---|---|
| 20 | 3.2.2. Unauthorized access to passwords and keys. |
| 21 | 3.2.3. Failure to respect the confidentiality of passwords. |
| 22 | 3.2.4. Violations of the order of storage and transmission of passwords. |
| 23 | 3.2.5. Inaccurate identification of Information System users. |
| 24 | 3.2.6. The absence of protective measures in the systems, ensuring the impossibility of denying the authorship of the operations and transactions carried out. |
| 25 | 3.2.7. Lack of mechanisms for registering unauthorized access to information for identification, authorization of customers and employees. |
| | 3.3. Unauthorized access |
| 26 | 3.3.1. Unauthorized access to data in Information System and PC. |
| 27 | 3.3.2. Leakage of service information through various channels. |
| 28 | 3.3.3. The ability to remotely retrieve information from external positions. |
| 29 | 3.3.4. Possibility of uncontrolled information retrieval from internal positions. |
| 30 | 3.3.5. Unauthorized use of the electronic payment system, remote service. |
| 31 | 3.3.6. Virtual theft and forgery using personal data. |
| | 3.4. Theft |
| 32 | 3.4.1. Interception of data in various ways. |
| 33 | 3.4.2. Actual theft and theft of technical equipment (phones, laptops, flash drives, communicators, etc.). |
| | 4. Integrity risks |
| | 4.1. Hardware integrity |
| 34 | 4.1.1. The usual failure of technical equipment (average). |
| 35 | 4.1.2. Failure of technical means due to force majeure circumstances. |
| 36 | 4.1.3. Changing the configuration of information processing facilities and systems. |
| | 4.2. Software integrity |
| 37 | 4.2.1. Software control failures. |
| 38 | 4.2.2. Penetration of malicious codes into information systems. |
| 39 | 4.2.3. The emergence of windows of vulnerability in the protection of information systems associated with the use of “patches” in protected software. |
| 40 | 4.2.4. Software attacks on the capabilities of processors and RAM. |
| 41 | 4.2.5. Combining the responsibilities of a software developer and user. |
| | 4.3. Integrity of information |
| 42 | 4.3.1. Loss or unavailability of important data. |
| 43 | 4.3.2. Use of incomplete or distorted information. |
| 44 | 4.3.3. Violations of the order of copying (backing up) information. |
| | 5. Availability risks |
| 45 | 5.1. Unauthorized latent long-term exploitation of information and computing resources. |
| 46 | 5.2. DDoS attacks on the ABS and employees' computers. |
| 47 | 5.3. Unauthorized remote access to Information System and PC. |
| 48 | 5.4. Unprotected remote access (authorized) to Information System and PC. |
| 49 | 5.5. Insecurity of email. |
| 50 | 5.6. SPAM threats. |

Таблица 1 представлена в виде онтологии рисков на рисунке 1. Эти характеристики полностью соответствуют определению оценки рисков информационной безопасности программного продукта. Проблема апеллирует к решению трех вопросов: шкалы безопасности программного обеспечения, регламентации поведения пользователей, списка требований к разработчикам программного обеспечения. Поэтому мы предлагаем следующую методику оценки информационной безопасности с использованием нечеткой логики.

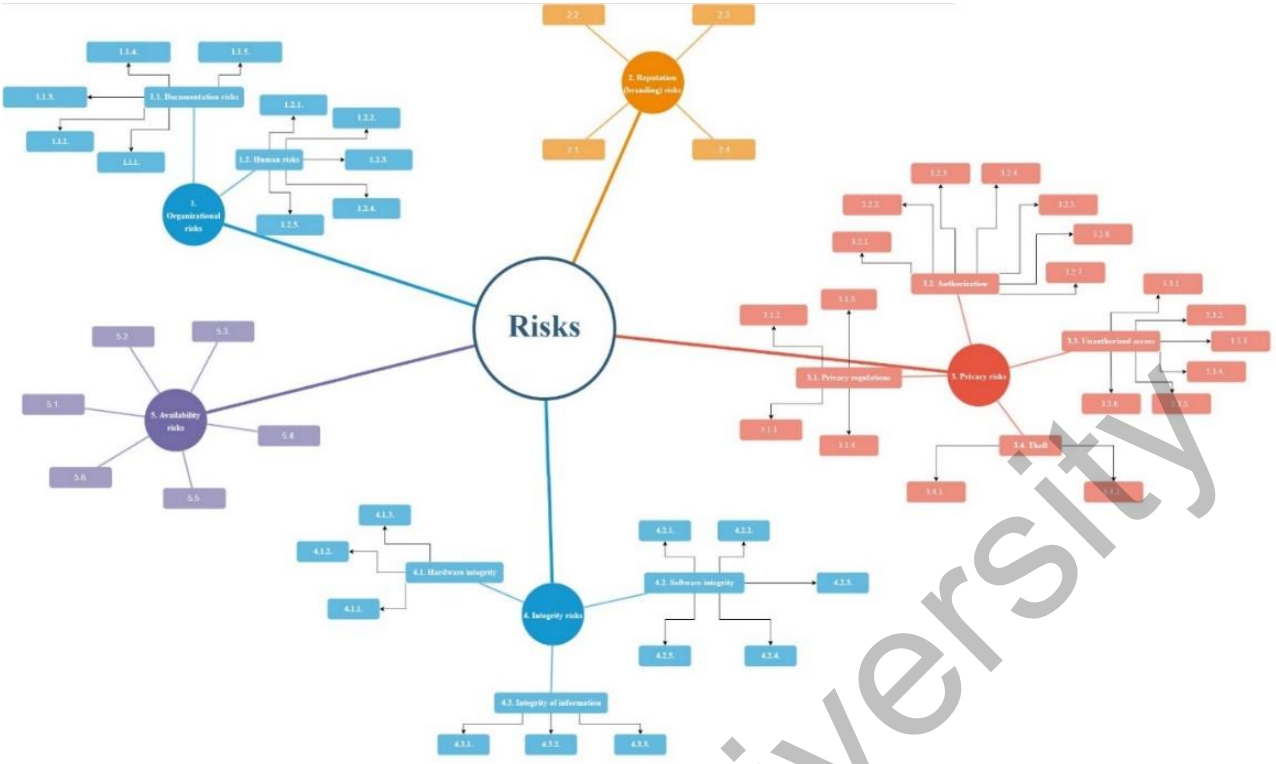


Рисунок 1. Онтология рисков

Гибкая модель оценки информационной безопасности требует выполнения нечеткой логики из-за ее гибкости и изменчивости при оценке любого изначально жестко заданного параметра. Нечеткий подход помогает принимать решения с различными вариантами, нечеткостью и уязвимостью. Это практично для работы с неопределенностью, сложностью и принятия решений по сложным вопросам противоречивого характера. В статье M.I., Tariq, S. Ahmed, , N.A. Memon и другие утверждают, что приоритезация средств управления информационной безопасностью с использованием нечеткого AHP приводит к эффективной и рентабельной оценке средств управления информационной безопасностью для организации с целью выбора наиболее подходящих из них. Предлагаемый формализованный подход и процессы определения приоритетов основаны на стандартах Международной организации по стандартизации и Международной электротехнической комиссии (ISO/IEC) 27001: 2013. Результаты оценки ясно показали преимущества предлагаемого метода с использованием нечеткой логики по сравнению с чисто объективным подходом с точки зрения более точной оценки рисков и более высокой отдачи от инвестиций в безопасность [5]. M.I. Tariq предложил структуру оценки информационной безопасности в облачных системах, которая была реализована с использованием системы нечеткого вывода, основанной на теории нечетких множеств, и правила нечеткой логики. MATLAB® использовались для тестирования структуры. Нечеткие результаты подтверждают, что предложенная структура может быть использована для защиты информации в среде облачных вычислений.

Мы предлагаем 4 уровня осязаемости в оценке информационной безопасности программного приложения. На первом уровне как внешние, так и внутренние компоненты информационной безопасности используются как индикатор цели оценки риска. На первом уровне мы устанавливаем цель Risk. Для удобства в группировании на втором уровне мы вводим первый уровень классификации рисков. На третьем уровне описываются риски, либо задается подгруппа классификации рисков. На четвертом уровне описываются риски, при условии, что на третьем уровне не были описаны риски. Данную структуру можно использовать как отдельно (поэлементно) для оценки рисков определенных групп и подгрупп, так и как средство для комплексной (целостной) оценки информационной безопасности программного продукта, использующегося в учебных заведениях.

Далее, используя классификацию критериев оценки рисков информационной безопасности, мы строим 15 машинных фаз с использованием алгоритма Mamdani. Для этого моделирования очень подходит программный продукт Matlab.

*Нечеткая модель оценки риска информационной безопасности*

В первой нечеткой машине 1.1. Documentation risks мы будем использовать входные переменные: 1.1.1. Lack of signaling means in case of emergency situations; 1.1.2. Lack of regulations for actions of information security employees in the event of an emergency situation; 1.1.3. Uncontrolled use and write-off of information carriers; 1.1.4. Lack of video surveillance systems for key nodes of information systems, access control to work premises; 1.1.5. Uncontrolled use of the Internet. Выходной переменной будет 1.1. Documentation risks.

Во второй нечеткой машине 1.2. Human risks мы будем использовать входные переменные: 1.2.1. Personnel errors, low qualifications; 1.2.2. Intentional harm by disloyal employees; 1.2.3. Malicious actions of the network administrator; 1.2.4. Combining the duties of an Information System administrator and an Information Security administrator; 1.2.5. Malicious acts when servicing. Выходной переменной будет 1.2. Human risks.

В третьей нечеткой машине 1. Organizational risks обслуживания мы будем использовать входные переменные: 1.1. Documentation risks; 1.2. Human risks. Выходной переменной будет 1. Organizational risks.

В четвертой нечеткой машине 2. Reputation (branding) risks мы будем использовать входные переменные: 2.1. Dissemination in the external environment of information of an economic nature that threatens the company's reputation; 2.2. Mentioning a company in the context of extremism, money laundering, cyber threats and cyber terrorism; 2.3. Use of uncertified and unlicensed products; 2.4. Possibility of external penetration into the company's Intranet system. Выходной переменной будет 2. Reputation (branding) risks.

В пятой нечеткой машине 3.1. Privacy regulations мы будем использовать входные переменные: 3.1.1. Lack of clear regulations for working with personal data; 3.1.2. Acceptance of untested cryptographic information protection devices into operation; 3.1.3. Lack of monitoring and analysis procedures for all performed operations; 3.1.4. Lack of organizational procedures that allow for internal investigations of violations of confidentiality risks. Выходная переменная — 3.1. Privacy regulations.

В шестой нечеткой машине 3.2. Authorization мы будем использовать входные переменные: 3.2.1. Long-term preservation of the authorization window in case of inactivity or in the event of an employee leaving the premises; 3.2.2. Unauthorized access to passwords and keys; 3.2.3. Failure to respect the confidentiality of passwords; 3.2.4. Violations of the order of storage and transmission of passwords; 3.2.5. Inaccurate identification of Information System users; 3.2.6. The absence of protective measures in the systems, ensuring the impossibility of denying the authorship of the operations and transactions carried out; 3.2.7. Lack of mechanisms for registering unauthorized access to information for identification, authorization of customers and employees. Выходная переменная — 3.2. Authorization.

В седьмой нечеткой машине 3.3. Unauthorized access мы будем использовать входные переменные: 3.3.1. Unauthorized access to data in Information System and PC; 3.3.2. Leakage of service information through various channels; 3.3.3. The ability to remotely retrieve information from external positions; 3.3.4. Possibility of uncontrolled information retrieval from internal positions; 3.3.5. Unauthorized use of the electronic payment system, remote service; 3.3.6. Virtual theft and forgery using personal data. Выходная переменная — 3.3. Unauthorized access.

В восьмой нечеткой машине 3.4. Theft, machine мы будем использовать входные переменные: 3.4.1. Interception of data in various ways; 3.4.2. Actual theft and theft of technical equipment (phones, laptops, flash drives, communicators, etc.). Выходная переменная — 3.4. Theft.

В девятой нечеткой машине 3. Privacy risks мы будем использовать входные переменные: 3.1. Privacy regulations; 3.2. Authorization; 3.3. Unauthorized access; 3.4. Theft. Выходная переменная — 3. Privacy risks.

В десятой нечеткой машине 4.1. Hardware integrity мы будем использовать входные переменные: 4.1.1. The usual failure of technical equipment (average); 4.1.2. Failure of technical means due to force majeure circumstances; 4.1.3. Changing the configuration of information processing facilities and systems. Выходная переменная — 4.1. Hardware integrity.

В одиннадцатой нечеткой машине 4.2. Software integrity мы будем использовать входные переменные: 4.2.1. Software control failures; 4.2.2. Penetration of malicious codes into information systems; 4.2.3. The emergence of windows of vulnerability in the protection of information systems associated with the use of «patches» in protected software; 4.2.4. Software attacks on the capabilities of processors and

RAM; 4.2.5. Combining the responsibilities of a software developer and user. Выходная переменная — 4.2. Software integrity.

В двенадцатой нечеткой машине 4.3. Integrity of information мы будем использовать входные переменные: 4.3.1. Loss or unavailability of important data; 4.3.2. Use of incomplete or distorted information; 4.3.3. Violations of the order of copying (backing up) information. Выходная переменная — 4.3. Integrity of information.

В тринадцатой нечеткой машине 4. Integrity risks мы будем использовать входные переменные: 4.1. Hardware integrity; 4.2. Software integrity; 4.3. Integrity of information. Выходная переменная — 4. Integrity risks.

В четырнадцатой нечеткой машине 5. Availability risks мы будем использовать входные переменные: 5.1. Unauthorized latent long-term exploitation of information and computing resources; 5.2. DDoS attacks on the ABS and employees' computers; 5.3. Unauthorized remote access to Information System and PC; 5.4. Unprotected remote access (authorized) to Information System and PC; 5.5. Insecurity of email. 5.6. SPAM threats. Выходная переменная — 5. Availability risks.

В четырнадцатой нечеткой машине 5. Availability risks мы будем использовать входные переменные: 5.1. Unauthorized latent long-term exploitation of information and computing resources; 5.2. DDoS attacks on the ABS and employees' computers; 5.3. Unauthorized remote access to Information System and PC; 5.4. Unprotected remote access (authorized) to Information System and PC; 5.5. Insecurity of email. 5.6. SPAM threats. Выходная переменная — 5. Availability risks.

В пятнадцатой нечеткой машине Risks мы будем использовать входные переменные: 1. Organizational risks; 2. Reputation (branding) risks; 3. Privacy risks; 4. Integrity risks; 5. Availability risks. Выходная переменная — 5 Risks.

Все 15 нечетких машин тесно связаны, которые показаны на рисунке 2. Характеристики представляют собой значения подклассов. Подклассификации обеспечивают ценность классификаций, которые позволяют оценить информационную безопасность.

Нижнее и верхнее значения определяют трапециевидную функцию принадлежности для каждой входной и выходной переменной. Для каждой нечеткой машины использовался центроидный метод дефаззификации. На рисунке 2 приведены результаты испытаний для каждой из пятнадцати нечетких машин. Результат дефаззификации показан синим в правом углу. Для примера использовалась Система управления обучением Platonus v5.2 (build#788) в Esil University http://pl.kuef.kz/.


Рисунок 2. Тестовые расчеты fuzzy машин рисков

Мы смоделировали на Matlab нечеткую экспертную систему с использованием алгоритма Мамдани для оценки рисков информационной безопасности программного обеспечения. Что касается лингвистических переменных, мы использовали критерии рисков из таблицы 1. Теперь перед нами стояла задача — запрограммировать эту модель в единую нечеткую экспертную систему. Нечеткая экспертная система разработана на языке программирования C #. Нечеткая экспертная система приведена на рисунке 3.


Рисунок 3. Нечеткая экспертная система оценки рисков информационной безопасности.

*Оценочный эксперимент*

Классическая формула Риска по стандарту NIST 800-30:

$$R = P(t) * S$$

*R – Risk.*
*P(t) – вероятность угрозы информационной безопасности.*
*S – стоимость актива.*

Так как мы хотим провести корреляцию среди различных методов, то нам необходимо провести нормализацию расчетых формул:

$$\mathrm{R_{norm}} = \frac{\mathrm{P(t) - P(t)_{min}}}{\mathrm{P(t)_{max} - P(t)_{min}}} * \frac{\mathrm{S - S_{min}}}{\mathrm{S_{max} - S_{min}}}$$

Формула Риска по стандарту ISO/IEC TR 13335-3:1998:

$$R = P(t) * P(v) * S$$

*P(t) – вероятность угрозы информационной безопасности.*
*P(v) – вероятность наличиця уязвимости.*
*S – стоимость актива.*

$$R_{norm} = \frac{P(t) - P(t)_{min}}{P(t)_{max} - P(t)_{min}} * \frac{P(v) - P(v)_{min}}{P(v)_{max} - P(v)_{min}} * \frac{S - S_{min}}{S_{max} - S_{min}}$$

Формула Риска по стандарту BS 7799:

$$R = S * L(t) * L(v)$$

$S$ – *стоимость актива.*
$L(t)$ – уровень угрозы.
$L(v)$ – уровень/степень уязвимости.

$$R_{norm} = \frac{S - S_{min}}{S_{max} - S_{min}} * \frac{L(t) - L(t)_{min}}{L(t)_{max} - L(t)_{min}} * \frac{L(v) - L(v)_{min}}{L(v)_{max} - L(v)_{min}}$$

Затем мы проводим эксперимент, чтобы оценить риск информационной безопасности программного обеспечения, используемого некоторыми университетами. A. Omarbekova и соавт. [12, 13] описали использование автоматизированных систем управления в некоторых университетах. Кроме того, эти 6 LMS оцениваются экспертом, по оценке качества программного обеспечения. Результаты оценки описаны в таблице 2. Список программного обеспечения, используемого в качестве роли LMS:

1. Platonus v5.2 (build# 1003) в Евразийском национальном университете им. Л.Н. Гумилева, https://edu.enu.kz/.
2. Canvas в Казахском государственном юридическом университете им. М.С. Нарикбаева, https://kazguu.instructure.com/login/canvas.
3. Академический портал ВКГТУ в Восточно-Казахстанском государственном техническом университете им. Д. Серикбаева, http://www.do.ektu.kz/doektu/Default.aspx? lang=en.
4. Система UNIVER в Казахском национальном университете имени аль-Фараби, https://univer.kaznu.kz/user/login.
5. Портал КГУ в Костанайском государственном университете им. А. Байтурсынова, http://ksu.edu.kz/ru/portal/.
6. Портал в Astana IT University, https://moodle.astanait.edu.kz/.

Таблица 2

**Результаты оценки Learning Management Systems**

| LMS | NIST 800–30 | ISO/IEC TR 13335–3:1998 | BS 7799 | ISREFES | Expert |
|---|---|---|---|---|---|
| edu.enu.kz | 0,193 | 0,396 | 0,385 | 0,293 | 0,189 |
| kazguu.instructure.com | 0,701 | 0,798 | 0,764 | 0,741 | 0,698 |
| do.ektu.kz | 0,602 | 0,693 | 0,68 | 0,642 | 0,598 |
| univer.kaznu.kz | 0,823 | 0,9 | 0,898 | 0,857 | 0,81 |
| ksu.edu.kz | 0,411 | 0,501 | 0,481 | 0,45 | 0,401 |
| moodle.astanait.edu.kz | 0,517 | 0,599 | 0,577 | 0,547 | 0,499 |

Согласно NIST 800–30, ISO/IEC TR 13335–3:1998, BS 7799 и ISREFES, оценка проводилась неспециалистами в области информационной безопасности программного обеспечения. Эти аудиторы изучили характеристики и подхарактеристики этих методологий оценки рисков информационной безопасности. Аудиторы давали оценки строго по правилам описанной методики. После просмотра всей процедуры они поместили оценочные оценки для 6 образцов программного обеспечения в 2-, 3-, 4-, 5-ый столбцы 2-ой таблицы.

Последний столбец результатов в таблице 2 поставил специалист в области криптографии, архитектуры программного обеспечения, он также имеет соответствующие сертификаты. Когда эксперт оценивал качество 6 программ, он опирался на свой опыт, а не на определенный метод. То есть эксперт не использовал описанные приемы. Кроме того, этот эксперт много времени работал с этими программными обеспечениями, поэтому он знает, как выбрать лучшее. Следовательно, оценка эксперта более объективна, так как эксперт ставит оценку на основе личного опыта работы с 6 программами и опыта разработки безопасного программного обеспечения. Далее мы проводим корреляционное исследование. Это исследование даст нам понимание эффективности нашей методологии. Результаты анализа представлены в таблице 3.

Таблица 3

**Матрица парных коэффициентов корреляции**

| Стандарты | NIST 800–30 | ISO/IEC TR 13335–3:1998 | BS 7799 | ISREFES | Expert |
|---|---|---|---|---|---|
| NIST 800–30 | 1 | 0,987446 | 0,983351 | 0,996518 | 0,999639 |
| ISO/IEC TR 13335–3:1998 | 0,987446 | 1 | 0,998312 | 0,997058 | 0,989458 |
| BS 7799 | 0,983351 | 0,998312 | 1 | 0,994682 | 0,985049 |
| ISREFES | 0,996518 | 0,997058 | 0,994682 | 1 | 0,997437 |
| Expert | 0,999639 | 0,989458 | 0,985049 | 0,997437 | 1 |

ISREFES показал самую сильную положительную корреляцию с NIST 800–30, ISO/IEC TR 13335–3:1998, BS, Expert. Остальные же методики оценки имеют лишь одну высокую корреляцию больше 0,99, если исключить ISREFES из выборки.

Новизна состоит в использовании в качестве основного показателя понятия «риск». Также по смыслу Риск делится на Organizational risks, Reputation (branding) risks, Privacy risks, Integrity risks, Availability risks. Нечеткость дает ту самую гибкость в характеристиках воздействия, снимается влияние коэффициентов робастности на итоговую оценку.

*Вывод*

В настоящей статье предложен новый метод оценки риска информационной безопасности программных продуктов LMS университетов. Методика основана на нечеткой логике с использованием алгоритма Мамдани. Построенная нечеткая экспертная система располагает расширенной классификацией критериев оценки риска, которая основана на анализе упомянутых выше стандартов. На основе междисциплинарного анализа (упомянутые выше исследования и стандарты) составлен перечень, состоящий из 50 рисков ИБ, который можно использовать в практической деятельности учебных заведений, поскольку нейтрализация (ликвидация, минимизация) рисков ИБ составляет сущность и содержание процесса обеспечения ИБ вуза. На базе предложенного перечня могут быть также построены модели угроз, на основании которых осуществляется постановка задач на создание СИБ. Кроме того, перечень конкретных рисков может использоваться в ходе оценки влияния принимаемых мер ИБ на эффективность деятельности вуза. Этот нечеткий метод делает вычисления гибкими, поскольку количество параметров, жестко заданных на начальном этапе, постоянно увеличивается. Результаты и заключение экспериментов подтверждают правильность разработанной методики. ISREFES показал результат > 0.99, самую сильную положительную корреляцию с NIST 800–30, ISO/IEC TR 13335–3:1998, BS, Expert. Остальные же методики оценки имеют лишь одну высокую корреляцию больше 0,99, если исключить ISREFES из выборки. Нечеткость придает гибкость оценке. Эта методика может быть использована для оценки рисков информационной безопасности любой сложной (социально значимой ERP-системы) автоматизированной системы управления, используемой в других сферах, например, в банковском секторе, медицинских информационных системах и т.д. Единственным недостатком этих методов является высокая трудоемкость экспертов при оценивании.

*Исследование финансируется Комитетом науки Министерства образования и науки Республики Казахстан (Грант № AP08856687).*



Список литературы

1 Feng, B., Li, Q., Ji, Y., Guo, D., & Meng, X. (2019). Stopping the Cyberattack in the Early Stage: Assessing the Security Risks of Social Network Users. *Security and Communication Networks*, Article ID 3053418. https://doi.org/10.1155/2019/3053418

2 Woo, P.S., Hwang, S.S., Hwang, S.H. & Kim, B.H. (2019). Risk assessment for the security of power information control systems. *International Journal of Smart Grid and Clean Energy*, 8(4), 488–494.

3 Kieras, T., Farooq, M.J., & Zhu, Q. (2020). RIoTS: Risk Analysis of IoT Supply Chain Threats *Symposium: IEEE 6th World Forum on Internet of Things (WF-IoT 2020)*. https://doi.org/10.1109/WF-IoT48130.2020.9221323

4 Shrestha, M., Johansen, Ch., Noll, J., & Roverso, D. (2020). A Methodology for Security Classification applied to Smart Grid Infrastructures. *International Journal of Critical Infrastructure Protection*, 28. https://doi.org/10.1016/j.ijcip.2020.100342

5 Marcovic-Petrovic, J.D., Stojanovic, M.D., & Bostjancic Racas, S.V. (2019). A Fuzzy AHP Approach for Security Risk Assessment in SCADA Networks. *Advances in Electrical and Computer Engineering*, 19, 69–74.

6 Wang, W., Shi, F., Zhang, M., Xu, C., & Zheng, J. (2020). A vulnerability risk assessment method based on heterogeneous information network. *IEEE Access*, 9163374, 148315–148330.

7 Wang, J., Neil, M., & Fenton, N. (2019). A Bayesian Network Approach for Cybersecurity Risk Assessment Implementing and Extending the FAIR Model. *Computers & Security*, 89, 101659. https://doi.org/10.1016/j.cose.2019.101659

8 Alemami, Y., Afendee Mohamed, M., & Atiewi, S. (2019). Research on Various Cryptography Techniques. *International Journal of Recent Technology and Engineering*, 8(2S3), 395–405.

9 Movahedi, Y., Cukier, M., Andongabo, A., & Gashi, I. (2019). Cluster-based vulnerability assessment of operating systems and web browsers. *Computing*, 101(2), 139–160.

10 Pan, K., Teixeira, A., Lopez, C.D., & Palensky, P. (2017). Co-simulation for cyber security analysis: Data attacks against energy management system. *IEEE International Conference on Smart Grid Communications*, 253–258. https://doi.org/10.1109/SmartGridComm.2017.8340668

11 Lv, L.Li, H., Wang, L., Xia, Q., & Ji, L. (2019). Failure mode and Effect Analysis (FMEA) with extended MULTIMOORA method based on interval-valued intuitionistic fuzzy set: Application in operational risk evaluation for infrastructure. *Information (Switzerland)*, 10(10):313, 1–22. https://doi.org/10.3390/info10100313

12 Omarbekova, A.S., Nurgazinova, G.S., Sharipbay, A.A., Barlybayev, A., & Bekmanova, G.T. (2017). Automatic formation of questions and answers on the basis of the knowledge base. *Proceedings of 2017 International Conference on Engineering and Technology, ICET 2017*, 1–3. https://doi.org/10.1109/ICEngTechnol.2017.8308192

13 Omarbekova, A., Sharipbay, A., & Barlybaev, A. (2017). Generation of Test Questions from RDF Files Using PYTHON and SPARQL. *Journal of Physics: Conference Series*, 806(1), 012009. https://doi.org/10.1088/1742–6596/806/1/012009

С.А.Абдыманапов, А.Б. Барлыбаев, Б.А. Алтынбек

## Learning Management Systems талдау мысалында ақпараттық қауіпсіздік тәуекелдерін бағалау әдістемесі

Білім беруде жаңа цифрлық технологиялардың белсенді дамуы мен қолданылуы, бір жағынан, жоғары оқу орнының бизнес-процестерін басқарудың тиімділігін арттыру үшін жаңа мүмкіндіктер ашты. Екінші жағынан, бұл киберқылмыскерлер үшін оқу орындарының осалдығын арттыра отырып, қауіпсіздік қатерлерінің едәуір жоғарылауына әкеледі. Соңғы жылдары әр түрлі оқиғалардың қарқынды өсуі ақпараттық қауіпсіздікке дәстүрлі тәсілдердің жеткіліксіз екенін көрсетті. Демек, ақпараттық қауіпсіздік тәуекелдерін бағалау көптеген оқу орындары үшін маңызды міндетке айналды. Білім беру мекемелеріне ақпараттық қауіпсіздікті құру мәселелерін шешуге көмектесетін бірнеше модельдер ұсынылды. Мақалада бұлдыр логиканы қолдана отырып, оқу орындарындағы ақпараттық қауіпсіздік тәуекелдерін бағалаудың жаңа иерархиялық моделі ұсынылған. Ақпараттық қауіпсіздік тәуекелдерін бағалаудың жаңа әдісі автоматтандырылған басқару жүйелері немесе ERP жүйелері мысалында сипатталған (оқытуды басқару жүйелері мысалында). Университет ұсынған тәуекелдерді бағалау 15 fuzzy машиналар түрінде бұлдыр логиканы пайдалана отырып модельденді. Бірқатар тәжірибелер барысында университеттерде қолданылатын әртүрлі бағдарламалық өнімдердің ақпараттық қауіпсіздік тәуекелдерін бағалау мұқият зерттелген. Ұсынылған әдіс тәуекелдерді икемді бағалау мәселесін шешуі керек.

*Кілт сөздер:* жоғары оқу орындарында бизнес-үрдістерді модельдеу, ақпараттық қауіпсіздік тәуекелдері, тәуекелдерді бағалау, ақпараттық қауіпсіздікті бағалау стандарттары, білім беру саласындағы саясат, білім беру саласындағы жұмыс, қоғам, білім беру саласындағы қауіпсіздік.

S.A. Abdymanapov, A.B. Barlybayev, B.A. Altynbek

## InfoSec Risk Assessment Methodology based on the example of Learning Management Systems Analysis

The active development and application of new digital technologies in education, on the one hand, has opened up new opportunities for improving the efficiency of the university's business process management. On the other hand, this has led to a significant increase in security threats and the vulnerability of educational institutions to cyber criminals. The recent rapid growth of various incidents regarding cybercrimes shows the insufficiency of traditional approaches to information security. Consequently, information security risk assessment has become an important task for most educational institutions. Several models have been proposed to help educational institutions solve problems with building information security. This article proposes a new

hierarchical structured model for assessing information security risks in educational institutions using fuzzy logic. A new method for assessing information security risks is also described using the example of automated control systems or ERP systems (for example, training management systems). The proposed risk assessment of the university was modeled using fuzzy logic in the form of 15 fuzzy machines. In the course of a number of experiments, we carefully studied the assessment of information security risks of various software products used in universities. The proposed method should solve the problem of flexible risk assessment.

*Keywords:* modeling of business processes in universities, information security risks, risk assessment, information security assessment standards, education policy, work in the field of education, public, security in the field of education.