ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2025»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2025»

PROCEEDINGS
of the XX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2025»

2025
Астана

УДК 001(06)
ББК 72я631
F96

«ǴYLYM JÁNE BILIM – 2025» студенттер мен жас ғалымдардың XX Халықаралық ғылыми конференциясы = XX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2025» = The XX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2025». – Астана: – 3813 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-08-5373-7

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.В сборник вошли доклады студентов, магистрантов, докторантов имолодыхученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001(06)
ББК 72я431
F96

ISBN 978-601-08-5373-7

Л.Н. Гумилев атындағы Еуразия ұлттық университеті, 2025

		сауаттылығын арттыру	
203.	Эрболат А.	Орта мектепте нанотехнология ұғымын оқытудың тиімді әдістері	808

СЕКЦИЯ 2

СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ И КОММ УНИКАЦИОННЫЕ ТЕХНОЛОГИИ

	Подсекция 2.1 Цифровая трансформация образования	
204.	Адалбек Н. «Традиционные и интеллектуальные подходы в обучении»	812
205.	Бакенова А.А. «Цифровизация тестирования: разработка нейросетевого приложения для формирования заданий по английской грамматике»	816
206.	Бекмурат А.Е. «Инновационные методы обучения информатике в школе на основе искусственного интеллекта»	821
207.	Назарова А.Т. «Развитие цифровых компетенций учителей в условиях персонализированного обучения»	826
208.	Нуриева Д.Р. «Цифровая трансформация педагогики: роль информационных технологий в повышении квалификации преподавателей»	830
209.	Абдуашимова П.М. «Білім беру процесінде жасанды интеллект технологияларын қолданудың тиімділігі»	833
210.	Ажибаева А.Д. «Мектеп информатикасын оқытудағы кемшіліктерді жою жолдары»	837
211.	Асылбек М.А. «Орта мектепте білім беру үдерісінде үлкен деректерді қолдану әдістемесі»	842
212.	Аталова А.Е. «Әлеуметтік желілерді информатика пәні бойынша оқыту құралы ретінде пайдалану»	845
213.	Балтабаев Н.П. «Мектептерде сабақ кестесін автоматтандыруға арналған интеллектуалды жүйе құру»	851
214.	Балтабаев Н.П., Дәрменов Ә.М., Мұратова М.М. «Жасанды интеллект негізінде жаратылыстану пәндерін оқытуды жетілдіру: BilimALL AI платформасының мүмкіндіктері»	854
215.	Баумуратова Х.Б. «АКТ оқыту барысында бастауыш сынып оқушыларының цифрлық сауаттылықтарын қалыптастырудың әдістемесі»	856
216.	Баумуратова Ш.Б. «Жасанды интеллект негізінде инклюзивті білім беруді жетілдіру»	859
217.	Ғазиз Ж.Е. «Бастауыш мектепте ақпараттық-коммуникациялық технологияларды оқыту әдістемесі»	863
218.	Дәрменов Ә.М. «Информатиканы қолжетімді ететін мобильді "BilimAll" қосымшасы»	866
219.	Дүйсегалиева Н.А. «HIGH-TOUCH HIGH-TECH моделі арқылы болашақ информатика мұғалімдерін машиналық оқыту негізінде даярлаудың	870

	инновациялық тәсілдері туралы»	
220.	Еликбай А.Ж. «Ақпараттық дәуірде білім берудің жаңа кезеңі – Инфографика»	874
221.	Жаңабекқызы А. «EDCAFE AI көмегімен сабақты жоспарлау»	879
222.	Жумабекова У.Б., Сабырова М.Е., Сабыров Т.С. «Информатика пәнін жобалап оқыту технологиясы»	883
223.	Кендебай Н.А. «EDUVISION білім беру процесін қадағалайтын қосымша»	888
224.	Көшенова А. «Цифрлық сауаттылықтың мектеп курсы бойынша интеллектуалдық оқу басылымдарына арналған дидактикалық материалдар»	891
225.	Куанышева Д.Ж. «Инклюзивті білім беруде педагогтың ақпараттық-коммуникациялық технологияларды (АКТ) қолдану даярлығын жетілдіру»	893
226.	Мауленова М.А. «Үлкен деректерді өңдеуде машиналық оқытудың әдістері мен құралдары»	897
227.	Мылтыкбаева Ж.Т. «Жаратылыстану пәндерін STEM білім беру мен ROS операциялық жүйесі негізінде кешенді оқыту»	901
228.	Надирхан Г.Е. «Ауыл мектептерінде цифрлық оқытуды дамыту мүмкіндіктері»	903
229.	Орынбаев М.Ж. «Компьютерлік көру алгоритмдерін машиналық оқыту негіздері бойынша қолданудың оқу-әдістемелік негіздері»	907
230.	Сабитова А.Б., Ражапова А.Н. «Жасанды интеллект және білім: болашақ мұғалімдерге арналған жаңа мүмкіндіктер»	910
231.	Сагындыкова А.С. «Болашақ информатика мұғалімдерін магистратураға даярлаудағы онлайн-курстардың рөлі»	915
232.	Сайлау Ж.Б. «Халықаралық зерттеуге оқушыларды АКТ арқылы дайындаудағы педагогтердің құзыреттілігін арттыру жолдары»	918
233.	Төрәлі Қ.Н. «Бастауыш сынып оқушыларының цифрлық сауаттылығын дамытудың ерекшеліктері»	923
234.	Турмаганбетова З.П., Алтыбаева А.Н. «Ерекше білімді қажет ететін оқушыларға мектеп информатика курсын оқытуды ұйымдастыру»	927
235.	Халхабай А. ««Алгоритмдеу және бағдарламалау» курсы бойынша мобильді қосымшаны оқу үдерісінде қолдану»	931
236.	Ысмайыл Н. «Мектеп информатика курсында жобалық оқыту әдісін енгізу»	936
237.	Ізбасарова М.Р. «Білім берудегі тестілеу жүйелері»	938

Подсекция 2.2

Интеллектуальные информационные системы

238.	Amantayeva Gulden Turarkyzy «Comparative analysis of models and methods in heart disease prediction problems»	944

239.	Tanirbergenov Meirbek Sagyndykovich «Facial Recognition-Based Attendance Management»	947
240.	Toleubay Daniyar Manatuly «Cardiac disease prediction using machine learning algoritms»	952
241.	Yerezhepov Rakhat Aibulatovich «Detecting logical fallacies in web content with nlp-powered crawling»	957
242.	Ажикенов Арман Русланович, Абашев Арслан Азатабекович «Оптимизация дорожного трафика в Астане через симуляцию транспортных потоков»	962
243.	Аманжол Альфараби Маликович, Сабит Мадияр, Кушербаев Бекзат Алибекулы «Система визуализации и анализа данных о передвижении нефти на основе интерактивной карты»	968
244.	Аскапова Мадина Куанышбековна «Параллельді қазақ-түрік сөйлеу корпусы қалыптастырудың әдісі мен моделін құру»	972
245.	Бекқожин Дастан Ақанұлы «Терең оқыту негізінде қолжазба таңбаларын тану программалық құралын әзірлеу»	975
246.	Дакенов Алишер Мырзахметұлы «Анализ сигналов ЭЭГ нейросетевыми методами для ранней диагностики нейродегенеративных заболеваний»	978
247.	Доспол Нәзгүл Нурланқызы, Жеткенбай Лена «Балабақшадағы балалардың эмоциялық жағдайын бақылауға арналған эмоцияларды тану жүйесін әзірлеу»	987
248.	Ермекбай Айболат, Молдабек Елжан «Жасанды интеллект негізінде веб-қосымша әзірлеу»	992
249.	Жұмал Жания Ержанқызы, Абдурахман Жансая Берікжанқызы «Применение голосового ИИ-помощника в геймифицированной образовательной среде»	1001
250.	Каримов Руслан Жасиинович «Эффективность существующих ИИ-решений в основных направлениях транспортной логистики»	1007
251.	Кубиева Сабина Талгатовна, Утепбергенова Зарина Арманкызы «Разработка iot системы по уходу за растениями на базе искусственного интеллекта»	1012
252.	Кудобаев Даниал Дулатович «Разработка информационной системы для автоматизации стоматологических услуг»	1017
253.	Мусина Данель Тлеухановна «Интеллектуальные инструменты автоматизированной диагностики надежности информационных систем»	1024
254.	Рогова Ксения Александровна, Қабдыбек Ризат Досмжанұлы, Джумадиева Тогжан Бекежановна «Мониторинг инженерных конструкций на основе искусственного интеллекта»	1030

255.	Сафонова Софья Александровна «Современные аспекты информационной безопасности в облачных вычислениях: модели, угрозы и методы защиты»	1034
256.	Смаилова Назгүл Батырбекқызы «Терең оқыту арқылы кітап ұсыныстарын әзірлеу: collaborative filtering, content-based және nlp әдістерінің комбинациясы»	1041
257.	Тажібай Аружан Айдосқызы, Кудубаева Сауле Альжановна «Көру қабілеті әлсіз адамдарға арналған аі дауыстық көмекші: нақты уақытта объектілерді анықтау және қашықтықты бағалау»	1046
258.	Тайжанов Азамат Жанкелдіұлы «Python тілінде фильмдердің интеллектуалды ұсыныс жүйесін әзірлеу»	1051
259.	Умирзахов Сундетали Кабылбекович «Сұраныстарды интеллектуалды талдау негізінде ұйымның сайты үшін чат-бот құру»	1055
260.	Шайхстан Марғұлан «IOT Сенсорлары негізінде ауа ластану деңгейін болжау»	1060

Подсекция 2.3

Современные тенденции в программной инженерии и управлении в условиях цифровой индустрии

261.	Bekenova A.B. «Development of a registration panel for users and doctors with integration into the database»	1077
262.	Bolat A.Zh. «Data analysis methods and decision making using big data and machine learning tools»	1081
263.	Алтайұлы А. «Visual studio интегралды ортасында «қойма қызметкерлеріне арналған» мәліметтер қорын жобалау»	1086
264.	Арап А.Қ. «Ақылды сурет салушы роботты әзірлеу»	1088
265.	Артыкбекқызы А. «Ақылды үйлердегі заттар интернеті(iot) мен робототехниканың өзара әрекеттесуі»	1091
266.	Ахметова А.Д. «Тоңазытқыштағы өнімдерді бақылауға және тағам әзірлеу ұсынысын беруге арналған программалық қосымша»	1096
267.	Дәрібай Д.Д. «Робототехниканы қолдану арқылы қойма логистикасындағы қолданыстағы басқару жүйелерін талдау»	1100
268.	Жамбулов С.Ж. «Білім алушыларды информатика және программалау олимпиадаларына дайындауда жасанды интеллекттің қолданысы»	1102
269.	Каиржан Р.С. «Development of system for recognition of emotional states of employees based on computer vision methods on Raspberry Pi»	1108
270.	Кайрекенова Н.Р. «Өнеркәсіптік роботты көру үшін машиналық оқытудың заманауи тәсілдері: әдістер, деректер жиынтығы және оптимизациялау»	1111

271.	Калижан А.К. «Разработка системы биометрической аутентификации с предотвращением deepfake атак»	1113
272.	Касылкасова К.Н. «Программное обеспечение smartmed для обработки медицинских данных и диагностики»	1118
273.	Қабдешев Ә.Е. «Жөтелді талдау негізінде денсаулықты диагностикалаудың интеллектуалды программасын әзірлеу»	1120
274.	Махаев Е.Е. «Разработка облачного приложения для автоматизации деятельности сети аптек»	1123
275.	Муратов М.М. «Эффективность единой информационной системы агропромышленного комплекса»	1126
276.	Нуржанова А.Б. «Современные методы классификации эмоций: анализ подходов и перспективы развития»	1130
277.	Нурпеисова З.Р. «Обзор и исследование методов искусственного интеллекта для анализа рынка недвижимости»	1134
278.	Рақымбек А.С. «Кітапқұмарларға арналған платформа: кітаптарды оқу және бөлісу үшін әлеуметтік желіні жобалау және іске асыру»	1138
279.	Сагидуллина Д.С. «Visual studio интегралды ортасында «қаржылық транзакцияларды қадағалау және талдауға арналған»мәліметтер қорын жобалау»	1144
280.	Төлеубай Д.М. «Yolov10 қолдану арқылы рентген суреттерінде сүйек сынуын анықтауды кешенді зерттеу»	1147
281.	Утегенова Д.Б. «Visual studio интегралды ортасында «фитнес орталық қызметкері үшін» мәліметтер қорын жобалау»	1152
282.	Шаймуратов А.Ж. «Проектирование аппаратно-программного комплекса для автоматизированного учета железнодорожного подвижного состава»	1154
	Подсекция 2.4 **Информационная безопасность**	
283.	Akniyet N. «Smart home automation and security system using arduino uno r4 and esp32 microcontrollers with telegram integration»	1158
284.	Askhatov A. «Analysis of social engineering methods and development of a defense strategy for corporate structures»	1165
285.	Bekturganov A.B. «Development of an early detection model for ddos attacks based on network traffic analysis»	1170
286.	Gabdullin A. «Analysis of modern wireless network security protocols and prospects for their development»	1174

287.	Garifullin A. «Modern information security management systems: construction and implementation in the digital era»	1179
288.	Igumenshev D.V. «Methods of embedding malicious code into pdf files»	1182
289.	Issabay T.B. «Utilizing sandboxes for cybersecurity training: a hands-on approach»	1187
290.	Kalybayev S. «Overview of modern authentication methods in telecommunication systems: from passwords to biometrics»	1191
291.	Kerim A. «Owasp top 10 and alternative methods of its compilation»	1194
292.	Yergazin A. «Analysis of a protection of hybrid intrusion detection and prevention system (idps) for low-latency 5g networks with adaptive learning using edge computing»	1199
293.	Yerzhanova Y.Y. «Key attacks in web forensics: xss, sql injection and rce»	1204
294.	Zhakay A. «Fundamentals of modern cryptography: from encryption to digital signatures»	1209
295.	Айдарова А.А. «Visualvm көмегімен cast-128 және kuznyechik блоктық шифрларының кілт генерациясын салыстыру және стандарттарға шолу»	1214
296.	Акимбекова Д.М., Каиржанова Д.Ж. «Жергілікті желінің қауіпсіздігін қамтамасыз ететін негізгі параметрлер»	1220
297.	Аскаров А.Д. «Разработка и исследование эффективности метода и инструмента для выявления фейковых новостей в социальных сетях»	1224
298.	Ауесхан Н. «Аномалияларды анықтау әдістерін талдау»	1229
299.	Ерболатов А. «Анализ вредоносных программ с помощью ии и криптографическая защита»	1332
300.	Ерболатова А.Ж. «Neuvector және kubernetes: контейнерлік ортадағы қауіпсіздікті қамтамасыз ету тәсілдері»	1336
301.	Жанатаев М.К. «Стеганография на основе lsb: реализация сокрытия данных в медиафайлах»	1338
302.	Жарасхан Н.Ж., Қайупов Е.К. «Crystals-kyber алгоритмін ресурсы шектеулі құрылғыларға оңтайландыру»	1343
303.	Жолдасбаев М.Ә. «Заманауи операциялық жүйелердегі жады дампы кескінін алу құралдарын талдау және салыстыру»	1348
304.	Жолмұратұлы Б., Маратов Ә.Б., Ховдабай Н.А. «Екі факторлы	1353

	аутентификацияның қауіпсіздігі және оның қолданылуы»	
305.	Кадринов Д.М. «Автоматизация внедрения альтернативной soar платформы на основе средств со свободной лицензией»	1357
306.	Казбаганбетова М.А. «Wireshark бағдарламасын пайдаланып желілік трафикті талдау және ақпараттық қауіпсіздікті қамтамасыз ету»	1361
307.	Кәкімбек Ә.Қ., Серікбай А.Е., Наурызбаев Д.Е. «MITM шабуылы туралы»	1366
308.	Кеттеш Б.Н. «ELF талдауындағы capstone: сызықтық және рекурсивті дизассемблерлеу»	1370
309.	Көшкінбаева Ф.Қ. «Linux қорғаудың заманауи әдістеріне талдау.openvas және nmap көмегімен осалдықтарды анықтау»	1374
310.	Қадыр Н.Е. «Заманауи фишинг түрлері мен олардың ұйымдық ақпараттық жүйелерге ықпалы»	1379
311.	Қажкен Е.Е., Темиржан С.А. «Қауіпсіздік инцитенттеріне қалай жауап беруге болады?»	1384
312.	Қартбай Е.Ғ., Тынарбай Н.И. «MITM шабуылы (адамның ортадағы шабуылы)»	1388
313.	Маратов Б.Ж. «Әлеуметтік инженерия қауіпсіздікке қатер ретінде: қызметкерлерді қорғау және оқыту әдістері»	1393
314.	Магзумов А.М. «Websocket протоколындағы осалдықтарды талдау»	1397
315.	Майданов А.С. «Автоматизация процесса анализа оперативной памяти с использованием python»	1401
316.	Мақсат Ә., Нурсеитов С. «Блокчейн қажеттілік пе, әлде сән бе?»	1406
317.	Қ. Мырзағалиұлы. «Инциденттерді анықтауда желілік логтарды талдаудың маңызды рөлдері»	1409
318.	Нурбатуров С.К. «Интеграция honeypot в ит-инфраструктуру компании»	1412
319.	Нуриева Д.Р., Исайнова А.Н. «Анализ рисками безопасности данных в медицинских учреждениях»	1415
320.	Нұрлан А.Т. «Кескіндердегі статистикалық стегоанализ әдістері»	1420
321.	Оралбеков Е.А. «Ddos-шабуылдардың жаңа буыны»	1424

322.	Рамазанова Ж, Нұрлан А, Жайсанбаева А. «Бұлтты технологияларды пайдалану кезіндегі тәуекелдер мен қауіпсіздік шараларын зерттеу»	1430
323.	Сахатбекқызы Т., Бахтиярқызы Т.А. «IoT құрылғыларының желідегі қауіпсіздігін қалай қамтамасыз етуге болады: стратегиялар және packet tracer көмегімен модельдеу»	1434
324.	Серғазы М. «Повышение производительности разработчиков с помощью интегрированных искусственных интеллектов и соображения кибербезопасности»	1440
325.	Султанов А.М. «Стеганография в кибербезопасности казахстана»	1443
326.	Танатаров Е., Іргебай С., Султанов А. «WI-FI желісінде шақырылмаған қонақтарды автоматты түрде анықтау жүйесі»	1447
327.	Таубай М.Е. Раматуллаев Ә.А. «Фишинг: желідегі beef әдісі арқылы алдау және одан сақтану»	1452

СЕКЦИЯ 3
ЕСТЕСТВЕННЫЕ НАУКИ

		ПОДСЕКЦИЯ 3.1 АКТУАЛЬНЫЕ ПРОБЛЕМЫ СОВРЕМЕННОЙ БИОЛОГИИ	
328.	Акимкара А.Б.	Гербарийдің ботаникалық зерттеулерде қолданылуы және гербарий қорындағы кеппе шөптің қалыптасу ерекшеліктері	1457
329.	Ақылбек А.	Астана қаласындағы ботаникалық бағының ландшафттағы *geranium sanguineum* биологиялық ерекшеліктеріне сипаттама беру	1459
330.	Әділхан Ж.	Мобильді байланыс пен қолданбалардың адамның мінез-құлқына әсерін анықтау	1463
331.	Базарбаева Қ.	Жасөспірімдерде девиантты мінез-құлықтың даму қаупі	1467
332.	Байдосова А.Б.	Методика использования игровых технологий на уроках биологии	1471
333.	Байдосова А.Б.	Актуальные проблемы современной биологии с использованием игровых технологий в образовании	1474
334.	Ғазизова Ә.	Сәулеленген егеуқұйрықтардың бүйректеріндегі морфофунционалдық өзгерістерді салыстырмалы бағалау	1477
335.	Еркін З.Б.	Биология сабақтарында оқушылардың сыни ойлау қабілетін жетілдіруде блум таксономиясын пайдалану	1482
336.	Жанабергенова	Кенеттен жүрек өлімі: генетикалық аспектілері	1486

The analysis shows that biometric methods are becoming increasingly popular, especially in the financial sector where accuracy and security are critical. However, biometrics still needs improvement, especially when it comes to protecting users' personal data.

3. Prospects for the development of authentication methods

1) Adaptive authentication – using context data (location, device, behavioral factors) to dynamically select the security level. This approach is already being actively used in banks and cloud services.

2) Blockchain technology – decentralized identification, which allows to exclude intermediaries and reduce the risks of hacking centralized databases. There are already projects that use blockchain to authenticate users without the need to store passwords.

3) AI and machine learning – automatic analysis of behavioral data to detect anomalies and improve authentication accuracy. According to recent studies, behavioral authentication based on machine learning can reduce the number of false biometrics by 30-40%.

4) Quantum cryptography is the protection of communication channels with the help of quantum keys, resistant to hacking even using quantum computers. This technology is still under development, but may become a security standard in the future.

4. Conclusion

The integration of biometric technology into authentication processes is rapidly gaining traction, driven by the increasing prevalence of biometric scanners in smartphones and other devices, coupled with the demand for enhanced security and seamless customer experiences. Biometric authentication methods offer a compelling alternative to traditional password-based systems, providing a more secure and convenient way to verify user identities. Biometric identification is recognized as the most reliable form of authentication, experiencing rapid growth and offering enhanced security compared to conventional methods like tokens and credentials.

Literature

1. **Brookson C.** *Security in current systems.* IEE Colloquium on Security in Current Systems, 1995, pp. 1–4. DOI: 10.1049/ic:19950131

2. **Mohammed A.H.Y., Dziyauddin R.A., Latiff L.A.** *Current Multi-factor of Authentication: Approaches, Requirements, Attacks and Challenges.* International Journal of Advanced Computer Science and Applications (IJACSA). 2023. 14(1). DOI: 10.14569/IJACSA.2023.0140119.

3. Stallings W. Cryptography and Network Security: Principles and Practice. – Pearson, 2021.

4. Modi K., Devaraj L. Advancements in Biometric Technology with Artificial Intelligence. 2022 https://arxiv.org/abs/2212.13187

OWASP TOP 10 AND ALTERNATIVE METHODS OF ITS COMPILATION

Kerim Aruzhan

kerim.aruzhan03@gmail.com

Master's student at the Faculty of Information Technology, The L.N. Gumilyov Eurasian National University, Astana, Kazakhstan

Supervisor – Ospanova A. B.

Introduction. The OWASP Top 10 is a widely recognized and influential list of the most critical security risks for web applications, compiled by the Open Web Application Security Project (OWASP). This list serves as a guideline for developers, security professionals, and organizations to prioritize security improvements and mitigate the most prevalent vulnerabilities (OWASP

Foundation, 2021). The purpose of this article is to explore the methodology behind OWASP Top 10, compare it with alternative vulnerability classification method CWE Top 25, and analyze the differences. The goal is to provide a comprehensive understanding of these methodologies and how they impact the cybersecurity landscape.

The OWASP Top 10 is updated periodically in every 3–4 years. Its last update was in 2021 and in 2025 it should be updated again. The 2021 edition introduced several changes, including three new categories, renaming and re–scoping of four categories, and consolidation of others.

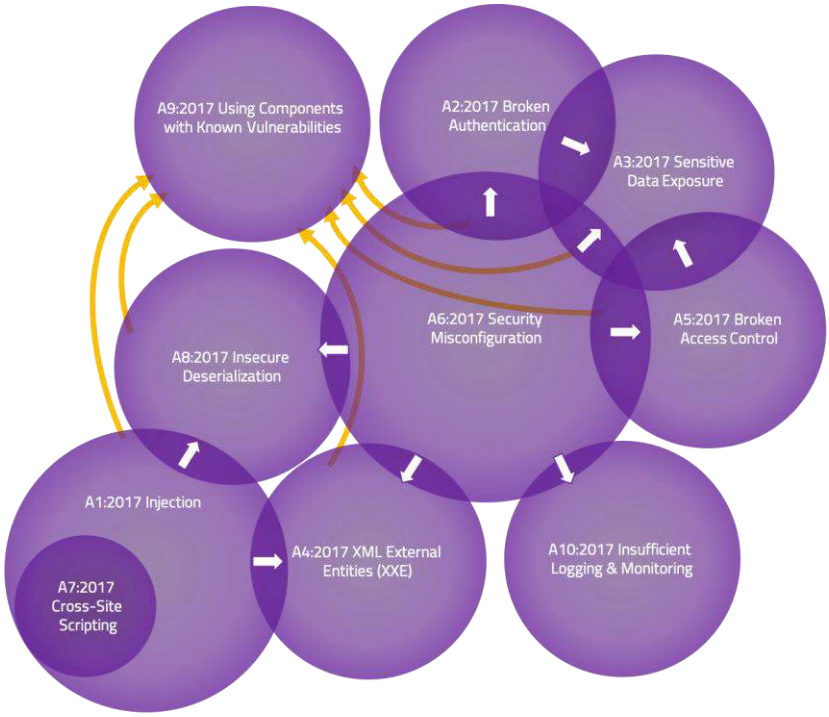
Methodology of OWASP Top 10. This section explores the methodology used to create the OWASP Top 10, focusing on data collection, analysis, categorization, and ranking.

Data Collection. The OWASP Top 10 is compiled from a diverse range of data sources, ensuring a broad and accurate representation of real–world security vulnerabilities. The key contributors to this dataset include:

- Security testing companies – Vulnerability assessment and penetration testing data.
- Bug bounty platforms – Reports from ethical hackers identifying security flaws.
- Industry reports – Published research on emerging threats and security trends.
- Security vendors – Findings from automated and manual security assessments.
- Open–source contributions – Community submissions from cybersecurity professionals.

For the 2021 OWASP Top 10, data was collected from 500,000+ web applications and several million vulnerability records worldwide. This represents a significant increase from the 114,000 applications analyzed in the 2017 edition, providing a broader and more accurate dataset. Also previously data collection was focused on a defined subset of nearly 30 CWEs (Common Weakness Enamuration) with an additional findings similar to that. Which makes experts primarly focus on such CWEs and rarely on other CWEs. After consideration OWASP Foundation decided to not give a list of CWEs but ask for all data without any restriction. That was huge change that maked dataset skyrocket from nearly 30 CWEs to almost 400 CWEs to analyze.

Data Analysis and Categorization. The significant increase of CWEs changed how to categorize them. OWASP decided to focus on root cause of vulnerabilities not symptom type. For example, instead of listing "Sensitive Data Exposure" as a vulnerability, they now look at the underlying issues, like cryptographic failures or misconfigurations. This shift helps security teams address the core problem rather than just mitigating the symptoms. Even with that all vunerabilities can be similar at some point and overlap with each other as it can be seen in picture 1.



Picture 1. Category Relationships ([6])

Also another major improvement in OWASP's methodology was the shift from frequency–based ranking to incidence rate–based ranking.

- Frequency–based ranking: Prioritizes vulnerabilities based on how often they appear, which can overrepresent some issues (e.g., Cross–Site Scripting).
- Incidence rate–based ranking: Focuses on how many applications were affected by at least one instance of a vulnerability, preventing high–frequency, low–impact vulnerabilities from dominating the list.

This shift allowed OWASP to better balance widespread security risks and critical but underreported threats.

Selecting categories. Unlike traditional security reports that rely solely on statistical data, the OWASP Top 10 takes a hybrid approach to selecting categories. They have two primary components to define the list. Its not fully data–driven but also contains industry survey. What it means? It means that OWASP Top 10 not only consider pure statistical data. They make an industry survey where they ask opinions of experts, which makes it special. How they define which one is more important? In 2017, they decided to go with 8:2 where 8 vulnerabilities will be from statical data and other 2 vulnerabilities from survey. For example, thanks to that approach, in 2021, “Insecure Design” was included in list.

Risk Ranking System. Once all 10 categories for OWASP Top 10 was decided, OWASP Foundation should decide how to place them. The main Methodology that they use to do that is OWASP Risk Ranking Methodology. This considers likelihood and impact to determine overall risk. In 2017, OWASP ranked categories by Exploitability, Detectability, and Impact. However, in 2021 they decided to change it and use data for Exploitability and Impact. In the end, their ranking were based on three key risk factors:

- Exploitability – How easy is it for attackers to exploit this vulnerability?
- Prevalence – How common is this vulnerability across applications?
- Impact – What is the potential damage if the vulnerability is exploited?

As we can see in picture 2, each risk factors have its own scores, and each score is typically assigned a value from 1 to 3.

Threat Agents	Exploitability	Prevalence	Technical Impact	Business Impacts
App Specific	Easy (3)	Widespread (3)	Severe (3)	App / Business Specific
	Average (2)	Common (2)	Moderate (2)	
	Difficult (1)	Uncommon (1)	Minor (1)	

Picture 2. Risk Rating System

Also OWASP includes CVSS (Common Vulnerability Scoring System) data from the National Vulnerability Database (NVD) to measure Exploitability and Impact score more precisely.

Risk Calculation Formula.

$$\text{Risk} = (\text{Exploitability} + \text{Prevalence}) \times (\text{Technical Impact})$$

Where,

- Exploitability Score: Derived from CVSS metrics, considering factors such as attack complexity, required privileges, and user interaction.
- Prevalence Score: Based on how often the vulnerability appears in real–world applications.
- Technical Impact Score: Evaluates the potential consequences (e.g., data theft, system compromise).

For example, in 2017, injection was in first place. It's exploitability was easy (3), prevalance – common (2), detectability (was not considered in 2021 list) – easy (3), technical impact – severe (3).

$$Likelihood = \frac{(3+2)}{2} \times (3) \; = \; 7{,}5$$

In the severity score that can be seen in picture 3, we can see that 7,5 = High.

Likelihood and Impact Levels	
0 to <3	LOW
3 to <6	MEDIUM
6 to 9	HIGH

Picture 3. Severity Score ([2])

Alternative Compilation Method. Several methodologies exist for ranking security vulnerabilities beyond OWASP Top 10, including the CWE Top 25, OWASP Mobile Security Top 10, OWASP API Security Top 10, NIST Cybersecurity Framework (CSF) and etc. In this section we

will consider 2024 CWE Top 25 as an alternative method, and will discuss the differencess between OWASP Top 10 and CWE Top 25.

2024 CWE Top 25. The 2024 CWE Top 25 was calculated by analyzing public vulnerability information from CVE records, focusing on root cause mappings to Common Weakness Enumeration (CWE) categories. Unlike OWASP Top 10, where they uses industry survey, CWE Top 10 is pure statistical data, which rely only on evidences. The methodology consists of several key steps:

- Dataset Collection. The dataset for 2024 included all CVE vulnerabilities that was published from June 1, 2023 to June 1, 2024. Also to improve accuracy, the CWE Team conducted automated analysis to identify CVE records that required remapping. After finding these records, CWE Team collaboratied with organizations responsible for assigning CVE IDs – to refine CWE mappings.
- CWE Mapping Normalization. CWE Team maps vulnerabilities using View–1003: Weaknesses for Simplified Mapping of Published Vulnerabilities, which includes 130 CWE categories, and if they will not find correct category, it will be adjusted to their closest ancestor category.
- Scoring and Risk Ranking System. The final CWE Top 25 ranking was determined using the Danger Score, which is calculated based on frequency and severity.

Each CWE was ranked using the formula:

$$\text{Danger Score}(\text{CWEx}) = \text{Frequency}(\text{CWEx}) \times \text{Severity}(\text{CWEx})$$

Where,

- Frequency(CWE_x) – Normalized frequency of CWE occurrences in CVE dataset.
- Severity(CWE_x) – Normalized severity score (average CVSS v3.0 or v3.1 base score).

Differences between OWASP Top 10 and CWE Top 25. The OWASP Top 10 and the CWE Top 25 are both widely recognized security vulnerability classification frameworks, but they differ in methodology, scope, and ranking approach. In table 1. were provided a comparison between OWASP Top 10 and CWE Top 25. Here we can see some major differences such as, focus, target audience, scope, data sources, data collection approach, ranking factors, update frequency, and latest edition.

Table 1.

Comparison Between OWASP Top 10 and CWE Top 25.

Factor	OWASP Top 10	CWE Top 25
Focus	Web application security vulnerabilities	General software weaknesses
Target Audience	Web developers, security testers	Security researchers, software engineers
Scope	Covers issues like authentication failures, injection attacks, and access control flaws	Covers programming errors like buffer overflows, memory corruption, and input validation issues
Data Sources	Security testing companies, bug bounty platforms, vendor reports, open–source contributions	National Vulnerability Database (NVD), CVE data, CVSS scores
Data Collection Approach	Combination of statistical data (80%) and industry surveys (20%)	Purely statistical approach

Ranking Factors	Exploitability, Prevalence, Impact	Frequency of occurrence, CVSS severity score
Update Frequency	Every 3 - 4 years	Annually
Latest Edition	2021 (Next update in 2025)	2024

Conclusion. Our article analyzed the Methodology of OWASP Top 10 and compared it to CWE Top 25. Their key differences were in data collection, where if OWASP Top 10 approached hybrid manner of statistical data and industry survey, CWE Top 25 purely relied on statistical data that was prodived in NVD, CVE, and etc. Also another difference in methodology was in ranking factors, where OWASP Top 10 uses their own Risk Ranking Methodology that contains exploitability, prevalence, and impact, and CWE Top 25 uses frequency of occurrence, CVSS severity score.

Literature

1. Indusface. Understanding the OWASP Top 10 risk score [Electronic resource]. – Indusface, 2024. – URL: https://www.indusface.com/learning/owasp–top–10–risk–score/
2. OWASP Foundation. OWASP Risk Rating Methodology [Electronic resource]. – URL: https://owasp.org/www–community/OWASP_Risk_Rating_Methodology
3. OWASP Foundation. OWASP Top 10:2021[Electronic resource]. – URL: https://owasp.org/Top10/
4. CWE. 2024 CWE Top 25 most dangerous software weaknesses [Electronic resource]. – URL: https://cwe.mitre.org/top25/archive/2024/2024_methodology.html
5. CWE. CWE Top 25 most dangerous software weaknesses [Electronic resource]. – URL: https://cwe.mitre.org/top25/
6. OWASP Foundation. The data [Electronic resource]. – URL: https://www.owasptopten.org/thedata

ANALYSIS OF A PROTECTION OF HYBRID INTRUSION DETECTION AND PREVENTION SYSTEM (IDPS) FOR LOW-LATENCY 5G NETWORKS WITH ADAPTIVE LEARNING USING EDGE COMPUTING

Yergazin Adil
ergazin.200332@gmail.com
Department of Information Security System, Faculty of Information Technologies, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan
Supervisor – Z. Tashenova

1. Introduction

The next generation of mobile networks is developing and evolving in the current era of digitalization, including 5G technology that is utilized in many spheres to meet customer needs with the possession of design priorities on efficiency, versatility, and scalability to match with characteristics based on connectivity and performance of the systems. 5G cellular networks should be efficient, and they differ in terms of requirements and features. In accordance with the emergence of 5G technologies, more improvements were utilized to maintain 5G networking, to reach clients needs, and to be efficient where distinct services vary on the options of requirements and features [28].

The novelty of this research lies in the development and evaluation of a Hybrid IDPS that integrates adaptive learning and edge computing. Adaptive learning reduces false positives and identifies new threats, while edge computing ensures low-latency responses and scalability for a high-density device environment. This dual approach offers an innovative framework to enhance the