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

evolution in how organizations approach cybersecurity. However, no technology alone can guarantee safety. The effectiveness of ISMS depends on strategic planning, cross-functional cooperation, and a commitment to ongoing improvement.As digital infrastructure becomes increasingly complex and interdependent, ISMS will remain central to organizational success—protecting data, preserving trust, and enabling innovation in a secure environment.

Literature

1. Information security and value creation: The performance implications of ISO/IEC 27001 / M. Podrecca, G. Culot, G. Nassimbeni, M. Sartor // Computers in Industry. — 2022. — Vol. 142. — P. 103744.
2. The effect of organizational information security climate on information security policy compliance: The mediating effect of social bonding towards healthcare nurses / K. Dong, R. F. Ali, P. D. D. Dominic, S. E. A. Ali // Sustainability. — 2021. — Vol. 13, no. 5. — P. 2800.OWASP Foundation. "Secure coding practices: A guide for developers." Cybersecurity Standards Report, 2022.
3. Cyber security and ethical hacking: The importance of protecting user data / A. M. A. Hawamleh, A. S. M. Alorfi, J. A. Al-Gasawneh, G. AlRawashdeh // Solid State Technology. — 2020. — Vol. 63, no. 5. — Pp. 7894–7899.
4. A deeper look into cybersecurity issues in the wake of Covid-19: A survey / Moatsum Alawida, Abiodun Esther Omolara, Oludare Isaac Abiodun, Murad Al-Rajab // Journal of King Saud University - Computer and Information Sciences. — 2022. — Vol. 34, no. 10, Part A. — Pp. 8176–8206. https://www.sciencedirect.com/science/article/pii/S1319157822002762.
5. Phishing attacks: A recent comprehensive study and a new anatomy / Z. Alkhalil, C. Hewage, L. Nawaf, I. Khan // Frontiers in Computer Science. — 2021. — Vol. 3. — P. 563060.
6. Jenny, C. 10 Cybersecurity Trends for 2022/2023 / C. Jenny // FinancesOnline. — 2022. https://financesonline.com/cybersecurity-trends/.
7. Eliyan, L. F. DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges / L. F. Eliyan, R. Di Pietro // Future Generation Computer Systems. — 2021. — Vol. 122. — Pp. 149–171.
8. Cost of a Data Breach Report 2023. — 2023. https://www.ibm.com/reports/databreach.
9. Center, Identity Theft Resource. ITRC Annual Data Breach Report - ITRC / Identity Theft Resource Center. — 2023. https://www.idtheftcenter.org/publication/2023-data-breach-report/.

УДК 004.056.5

METHODS OF EMBEDDING MALICIOUS CODE INTO PDF FILES

Igumenshev Daniil Vladimirovich
daniiligumenshev@gmail.com
Student of faculty of Information Technologies Eurasian National University, Astana, Kazakhstan
Supervisor – Shakhmetova G.B.

Abstract

The Portable Document Format (PDF) has become a cornerstone of digital document exchange due to its platform-independent design and rich feature set. However, its complexity and support for embedded scripting languages such as JavaScript have made it a prime vector for cyberattacks. This research presents a comprehensive study of PDF-based malware with a focus on JavaScript injection. The paper demonstrated the feasibility of distributing a PDF file with embedded JS code inside. The

research concludes with practical recommendations for improving enterprise PDF security protocols, highlighting the need for layered defense strategies in the era of increasingly sophisticated document-based attacks.

Introduction

PDF malware has evolved significantly since its emergence in the early 2000s, paralleling advancements in document format capabilities. The integration of JavaScript in PDF specifications [1] introduced dynamic functionality but also created vulnerabilities exploitable through event handlers like `OpenAction` and `PageOpen`. Modern attacks leverage these features to execute payloads ranging from ransomware to credential harvesters.

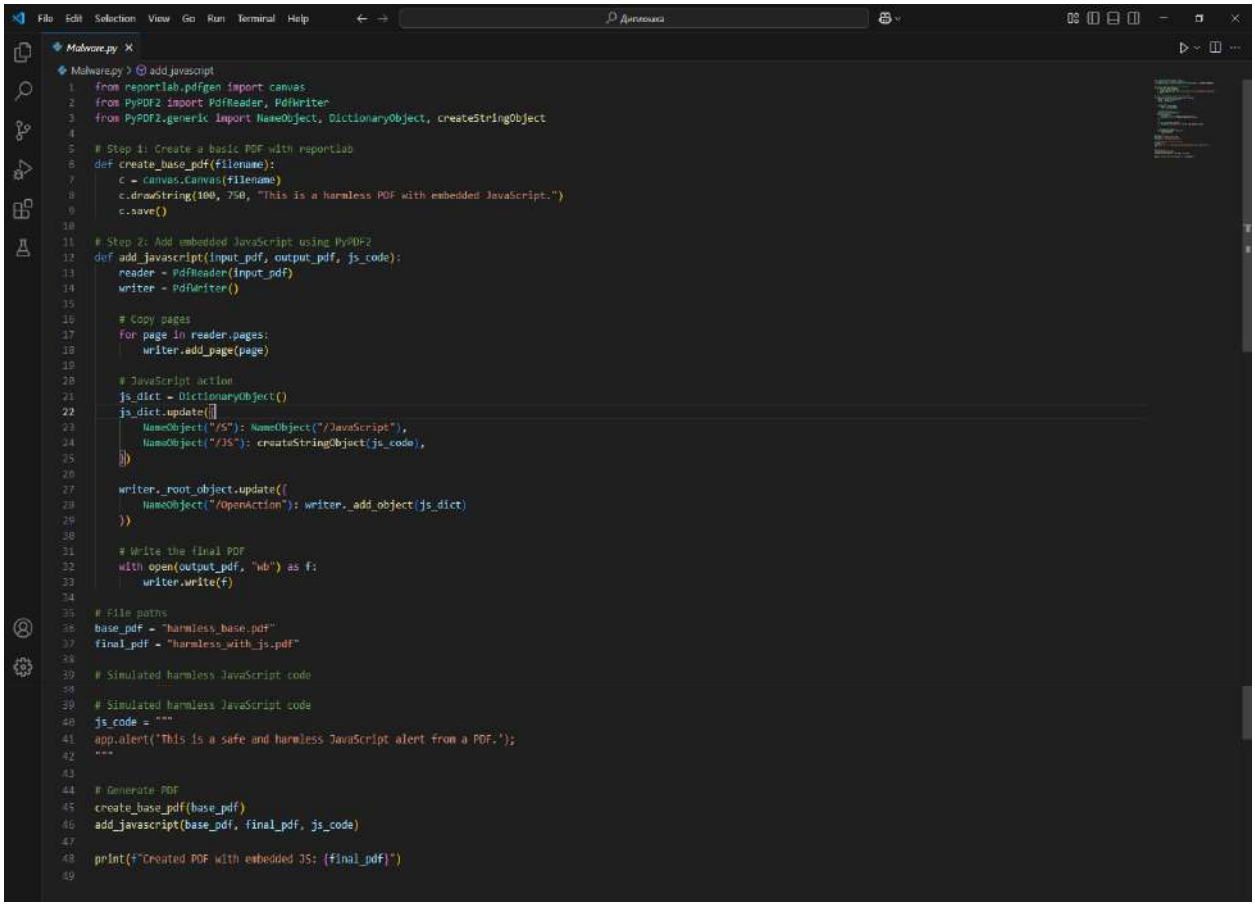
Main types of PDF exploit:

1. **JavaScript Execution**:
   PDFs support JavaScript through the `/JS` and `/JavaScript` objects, enabling interaction with document elements. Attackers exploit this via social engineering (e.g., fake invoice attachments) to trigger malicious scripts. The theoretical basis lies in the Turing-complete nature of JavaScript [2], allowing arbitrary code execution within the PDF reader's context.
2. **Polyglot Files**:
   Polyglot files exploit format ambiguities to masquerade as both PDFs and executables. This technique relies on the MZ-PDF header collision [3], where parsers interpret the same byte sequence differently. Theoretically, such files bypass signature detection by satisfying superficial format checks while hiding payloads in unvalidated regions.
3. **XFA Forms**:
   XML Forms Architecture (XFA) enables dynamic form rendering but can be abused to fetch external resources. From a theoretical standpoint, XFA's XML-based structure allows injection of malicious URLs, leading to drive-by downloads or cross-site scripting (XSS) attacks.

Implementation Methodology

1. JavaScript Embedding

A PDF is more than just a document for displaying text and images; it can also contain embedded JavaScript that executes when the document is opened. Attackers exploit this feature by embedding scripts that prompt users to perform actions that lead to malware installation or data theft.



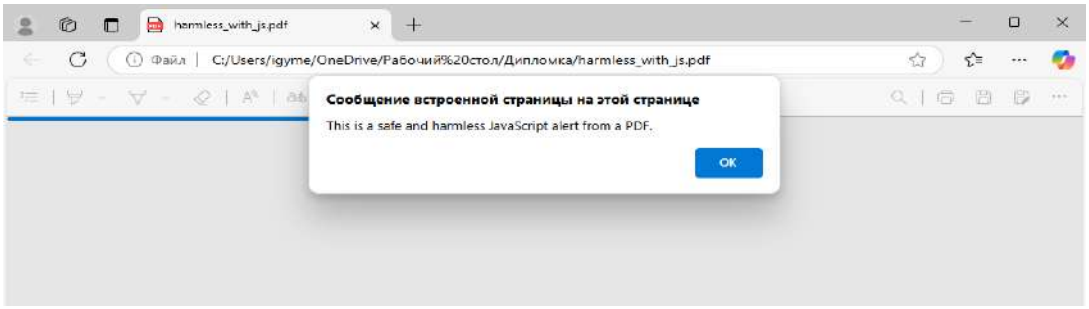
Picture 1. Advanced python code for creation of .PDF file with Embedded JS code

The script on Picture 1 is designed to create a PDF that tricks users into enabling JavaScript, a tactic often used in phishing attacks or malware distribution. However, in this case, the embedded JavaScript is harmless and only displays a pop-up message rather than executing malicious actions. Understanding how this works requires an exploration of PDF structure, JavaScript execution within PDFs, and how attackers leverage these techniques for social engineering.

This script follows a common pattern. First, it contains decoy content, meaning that the PDF includes a fake security alert, making users believe they need to enable JavaScript. Second, it injects JavaScript into the PDF, which mimics Adobe Reader alerts. Finally, it does not contain any harmful payloads, meaning that the script does not download or execute external code.

2. Executing of JavaScript after opening PDF file

The PDF document is structured with an embedded JavaScript alert (Picture 2). The purpose is to deceive users into thinking they need to enable JavaScript. The script uses a method that places text inside the document at a specific location. This simulates a warning message that makes users believe they need to take an action.



Picture 2 Example of opening PDF file by Acrobat with JS function powered on

The script then embeds JavaScript into the PDF. When the PDF is opened in a JavaScript-enabled viewer such as Adobe Reader, it will trigger the script. The script, in this case, is a simple pop-up alert that states that a security update is required and that the user should enable JavaScript to proceed. This mimics a legitimate Adobe warning but does not perform any harmful actions.

Finally, the script generates and downloads the PDF file, which contains the decoy message and the embedded JavaScript.

While this script is harmless, attackers often modify it to perform malicious activities. Instead of displaying an alert, real-world attacks embed JavaScript that downloads and executes external code. Attackers may use this method to redirect users to malicious sites that automatically download malware. Another common method is credential theft. Attackers can use JavaScript inside PDFs to steal credentials by embedding fake login forms that appear when the document is opened. In such cases, the stolen credentials are transmitted to an attacker-controlled server. A more advanced technique involves logging keystrokes within a PDF to steal sensitive information entered by the user.

To prevent such attacks, several best practices should be followed. First, users should disable JavaScript in their PDF readers, as many PDF viewers allow them to do so. Second, security filters should scan PDFs attached to emails for embedded JavaScript. If detected, the PDF should be blocked or flagged for review. Third, user awareness is critical. Educating users about fake security alerts and encouraging them not to enable JavaScript unnecessarily can reduce the effectiveness of such attacks. Fourth, security software should be configured to scan and analyze PDFs for malicious scripts before allowing them to open.

While this example only demonstrates a harmless pop-up, it highlights an important ethical dilemma. Embedding scripts inside PDFs can be misused. Security professionals must adhere to ethical guidelines when testing or demonstrating such capabilities. Any testing should be conducted in controlled environments, and real-world implementation should follow legal and ethical standards.

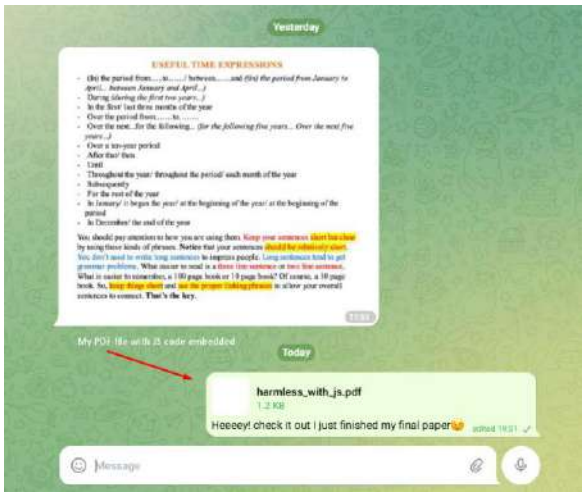
This script illustrates how JavaScript can be embedded in a PDF to trick users into taking an action. While the example is benign, similar techniques are widely used in cyberattacks. Understanding these methods allows security researchers and IT professionals to implement better defenses against such threats.

3. Direct distribution of the PDF file through open sources

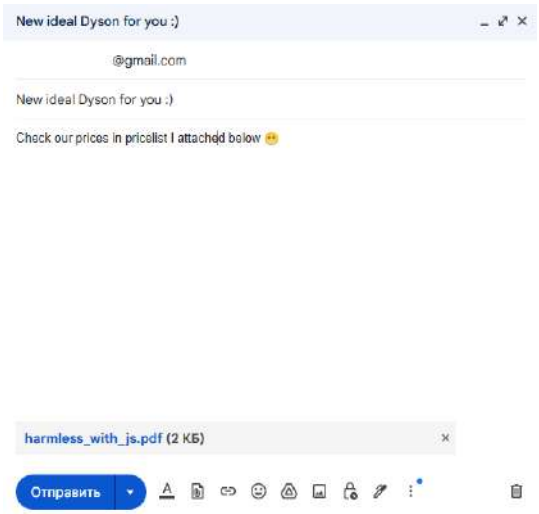
For example, several social networks, messengers, and the most common method — email distribution — were used (Picture 3-4).

The very first way was popular messenger which didn’t even warn user about possible consequences of sending/receiving the file. Some people across the internet are not aware about the risk of downloading PDF file, basically in most cases the file will be useless, but in some cases as people is using Adobe Acrobat Reader which is a possible way of executing harmful JavaScript code on PC or even mobile phone.

In the context of email distribution, a widely used email service—Gmail—was utilized. The distribution of the file did not encounter any obstacles; neither the sender nor the recipient were notified of the presence of embedded JavaScript code or the potential consequences and harm it could subsequently cause.



Picture 3 Direct spreading of the PDF file across messengers



Picture 4 Sending Phishing E-mail with PDF file

In the context of email distribution, a widely used email service—Gmail—was utilized. The distribution of the file did not encounter any obstacles; neither the sender nor the recipient were notified of the presence of embedded JavaScript code or the potential consequences and harm it could subsequently cause.

Conclusion

The widespread adoption of PDFs in digital communication, coupled with their intricate structure and embedded scripting capabilities, has rendered them a prime target for cyber attacks. In this study, was demonstrated how techniques such as JavaScript embedding, polyglot file construction and XFA exploitation are leveraged to bypass conventional security mechanisms and deliver malicious payloads. Through practical implementations and real-world distribution scenarios—including messaging platforms and email— was illustrated how easily these threats can spread without raising suspicion.

Disabling JavaScript in PDF viewers, implementing intelligent scanning systems, and promoting user awareness are critical steps toward reducing the risk of infection. As document-based threats grow more sophisticated, continued research into proactive and intelligent detection methods remains essential [4]. Through a deeper understanding of both the theoretical and practical aspects of PDF malware, more resilient defenses can be developed against this evolving threat landscape.

Literature

1. Adobe Systems, *PDF Reference, Sixth Edition*, Adobe Portable Document Format Version 1.7, November 2006.
2. D. Maiorca, G. Giacinto, and I. Corona, "A structural and content-based approach for the detection of malicious PDF files," in *Proceedings of the IEEE Symposium on Security and Privacy Workshops*, 2012, pp. 95–102.
3. N. Sethi and A. Singh, "Detection of Malicious PDF Files Using Machine Learning," *International Journal of Computer Applications*, vol. 182, no. 47, pp. 1–6, 2019.
4. ClamAV, "Clam AntiVirus," [Online]. Available: https://www.clamav.net/. [Accessed: April 4, 2025].

UDC 004

UTILIZING SANDBOXES FOR CYBERSECURITY TRAINING: A HANDS-ON APPROACH

Issabay Temirlan Bakytbekuly
isabayev14@mail.ru
Master's student of L.N. Gumilyov ENU, Faculty of Information Technology, Department of Information Security, specialty "Information Security Systems", Astana, Kazakhstan.
The scientific supervisor is PhD doctor, Associate Professor of the Department of Information Security, Akhmetova Zh. Zh.

Abstract. As cyber attacks turn out to be more advanced and widespread, the demand for cybersecurity professionals who can handle reality-based issues grows more rapidly day after day. Traditional education systems that are usually based on theory cannot provide the field practice necessary to combat the reality-based issues of modern-day cyberattacks. Sandboxes - isolated platforms in which malware and cyberattacks are safely tested and analyzed - have become a central element in the training of cybersecurity professionals. This article examines the use of sandboxes for training in cybersecurity, ranging from various sandbox types to the benefits of experiential learning and sandbox limitations. Based on successful use cases and studies, in this article, one gets a critical understanding of the way sandboxes are shaping the future of cybersecurity training.

Keywords: Cybersecurity training, Sandboxes, Malware analysis, Hands-on learning, Static sandboxes, Dynamic sandboxes, Hybrid sandboxes, Penetration testing, Incident response

1. Introduction to Cybersecurity Training. The digital revolution has changed almost every aspect of life, especially bringing with it huge benefits, but also growing threats to cybersecurity. As increasingly sophisticated cyber attacks are carried out against organizations, governments, and individuals, there is an urgent need for cybersecurity experts with both theoretical knowledge and practical experience. Traditional education methods - based mostly on lectures and theoretical understanding - are no longer sufficient to equip cybersecurity practitioners for the dynamic and sophisticated nature of today's threats. Consequently, institutions and organizations are adopting more