

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

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

**Студенттер мен жас ғалымдардың
«GYLYM JÁNE BILIM - 2023»
XVIII Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ**

**СБОРНИК МАТЕРИАЛОВ
XVIII Международной научной конференции
студентов и молодых ученых
«GYLYM JÁNE BILIM - 2023»**

**PROCEEDINGS
of the XVIII International Scientific Conference
for students and young scholars
«GYLYM JÁNE BILIM - 2023»**

**2023
Астана**

УДК 001+37
ББК 72+74
G99

**«GYLYM JÁNE BILIM – 2023» студенттер мен жас ғалымдардың
XVIII Халықаралық ғылыми конференциясы = XVIII
Международная научная конференция студентов и молодых
ученых «GYLYM JÁNE BILIM – 2023» = The XVIII International
Scientific Conference for students and young scholars «GYLYM JÁNE
BILIM – 2023». – Астана: – 6865 б. - қазақша, орысша, ағылшынша.**

ISBN 978-601-337-871-8

Жинаққа студенттердің, магистранттардың, докторанттардың 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 и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001+37
ББК 72+74

ISBN 978-601-337-871-8

**©Л.Н. Гумилев атындағы Еуразия
ұлттық университеті, 2023**

Бұлттарды ұйымдардың қызметіне енгізу кезінде жалпы ақпараттық қауіпсіздікті қамтамасыз етуді реттейтін жалпыланған стандарттар, нормативтік актілер мен заңдар қолданылады. Алайда, технологияның ерекшелігі мен оны іске асырудың күрделілігін ескере отырып, бұлтты өнімдермен жұмыс істеу кезінде ақпараттық қауіпсіздікті қамтамасыз етудің әдістерін егжей-тегжейлі қарастыруға бағытталған стандарттар қажет.

Қазіргі таңда осындай құжаттар бар және жаңартылып отырады. Олардың көмегімен, тұтынушылар технологияны және онымен қалай жұмыс істеу керектігін көбірек түсінетін болады. Сервисті ұсыну сапасын жақсартуға бағытталған бағдарламалық қамтама провайдерлері мен әзірлеушілеріне қойылатын белгілі бір талаптар мен шектеулер бар. Бұл қызметтің қауіпсіздік деңгейін де, тұтынушылардың сенім деңгейін де едәуір арттырады деп болжауға болады.

Пайдаланылған әдебиеттер тізімі:

1. “Безопасность и защита данных в облачных технологиях”. <https://boodet.online/blog/bezopasnost-i-zashhita-dannyh-v-oblachnyh-tehnologiyah-boodet-online?ysclid=lerz51fj27108923164>
2. У.Шнайдер, “Безопасность при использовании облачных сервисов. Журнал сетевых решений LAN”.
3. Защита информации в облачных сервисах. URL: <https://smoff.ru/howitworks/zashchita-informacii-v-oblachnyh-servisah>
4. Что такое безопасность облака? URL: <https://www.kaspersky.ru/resource-center/definitions/what-is-cloud-security>

ӘОЖ 004.056.57

ПРОГРАММАЛЫҚ ҚАМТАМАНЫҢ ҚҰЖАТТАЛМАҒАН МҮМКІНДІКТЕРІН АНЫҚТАУ ӘДІСТЕРІ МЕН ҚҰРАЛДАРЫН ЗЕРТТЕУ

Альсеитов Олжас Айдосович
olzhas010111@gmail.com

Л.Н.Гумилев атындағы Еуразия ұлттық университеті
ақпараттық-технологиялар факультетінің ақпарат қорғау жүйесі мамандығының 1 курс
магистранты
Ғылыми жетекшісі - Туребаева Р.Д. , Сауханова Ж.С.

Кіріспе:

Заманауи ақпараттық технологияларды, есептеу техникасын және телекоммуникациялық жүйелердің негізі болып программалық қамтама болып табылады. Ақпараттық технологиялар қарқынды өсуі адам қызметінің әртүрлі салаларында қолдануы және ақпараттық технологияның адам өмірінің сапалық көрсеткіштеріне ықпалының артуы программалық қамтаманың жұмысының көлемін ұлғайту, үлкен ресурстарды тарту қажеттілігі бойынша сапа және біліктілік талаптарын әзірлеу, арттыру салдарына әкеліп соқтырды. Заман талабына сай ақпараттық технологиялар қарқынды өсуден негізгі ақпарат қорғау ережелеріне және оның жолдарын қолдануға әкелді. Егер бірнеше жыл бұрын программалық қамтама тек функционалды түрде дұрыс және қажетті тапсырмаларды істейтін талаптар қойылса, қазіргі уақытта программалық қамтама құнды ақпарат ағып кетуінен, жүйенің шабуылдарға осал болуынан қорғайды. Программалық қамтаманың маңызды осалдығы құжатталмаған мүмкіндіктері болып табылады. Негізгі бөлімде құжатталмаған мүмкіндіктерді анықтауға арналған негізгі талдау әдістері мен құралдарына шолу жасаймын және статистикалық талдау негізінде өзімнің жасаған жүйедегі осалдықты анықтау процессін жүргіздім.

Негізгі бөлім:

Бағалау объектісінің осалдықтары мен құжатталмаған мүмкіндіктерін анықтау бойынша жүргізілетін талдауларды:

1. Программалық қамтаманы expertтік талдау әдістері мен құралдарын зерттеу

2. Программалық қамтаманы статикалық талдау әдістері мен құралдарын зерттеу
3. Программалық қамтаманы динамикалық талдау әдістері мен құралдарын зерттеу
4. Программалық қамтаманы талдау reverse engineering әдістері мен құралдарын зерттеу

Эксперттік талдау объектінің осалдығы мен құжатталмаған мүмкіндіктерін анықтауды көздейтін зерттеу нәтижелері бойынша бағалау объектісіне құжаттама және басқалар қол жетімді ақпараттық көздер, басқа зерттеушілерден алынған зерттеу нәтижелері, бағалау объектісінің архитектурасын талдау, сондай-ақ жүйеге енуге тестілеуді өткізу. Негізгі эксперттік талдау әдістермен жүргізу кезінде пайдаланылатын талдау болып табылады: құжаттама, осалдықтарды сканерлеу, шабуылдарды модельдеу, тестілеу ену, деректерді визуализациялау.

Статикалық талдау осалдықтар мен құжатталмаған мүмкіндіктерін анықтауды қарастырады программалық қамтаманың (кодты талдау) зерттеу нәтижелері бойынша бағалау объектісінің бағдарламалық кодын нақты орындалу кезінде зерттеледі. Программалық қамтаманы статикалық талдау барысында оған статикалық модель құрастырып, сол модель негізінде статикалық әдістерді қолданады. Статикалық талдаудың негізгі әдістері: талдау, процедурааралық контекстке сезімтал талдау, ресми тексеру. Статикалық талдау жүргізу үшін арнайы статикалық анализаторлар қолданылады.

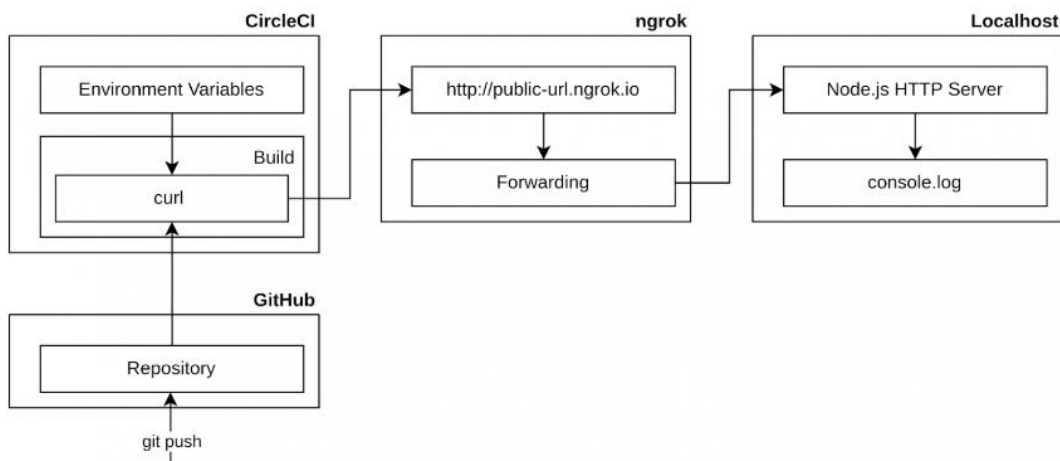
Динамикалық талдау осалдықтар мен құжатталмаған мүмкіндіктерін анықтауды қарастырады программалық қамтаманың (кодты талдау) тікелей режимде зерттеу нәтижелері кодтың орындалуы кезінде орындалады. Динамикалық талдау жүргізу кезінде бағдарламаның кірісі арнайы құрылған ақпарат арқылы беріледі. Программалық қамтаманың орындау барысында оның орындалу нәтижелерін тіркеуді жүзеге асырады, оның ішінде бағдарламаның орындалу жолдары жазылады, жадының өзгеру процессін анықтайтын сызбаларды және процессор регистрлері, шығыс деректері жазылады. Динамикалық талдау үшін әдістерін ендірілгенге қатысты қолдану программалық қамтаманың оның жұмыс істеу ортасын қалпына келтіруді қажет етеді, оның аппараттық және программалық қамтаманың эмуляциялау жүзеге асырылады қамтамасыз ету. Бұл жағдайда динамикалық талдау әдетте қолданылатын ендірілген программалық қамтаманың үзінділері бар кодты талдайды. Негізгі әдістермен динамикалық талдау: бұл фазинг, жеңіл салмақтағы белсенділікті талдау бағдарламалардың өзара әрекеттесу процестері, белгіленген деректерді бақылау, сондай-ақ басқа әдістер. Динамикалық талдау мыналармен жүзеге асырылады: фаззерді, қолданба белсенділігі мониторын, қайта қолдану қамтамасын пайдалану, декомпрессор, профиль жасаушы.

Қолмен талдау осалдықтар мен программалық қамтаманы анықтауды қарастыруды бағалау объектісінің бастапқы немесе қалпына келтірілген кодын сараптау нәтижелерін зерттейді. Қолмен талдау кезінде қолданылатын негізгі әдістер белгіленген деректерді қадағалау, код бөлімдерін қолмен талдау, деректерді визуализациялау әдістері қолданылады.

Бағалау объектісінің ықтимал қауіпті функционалдық мүмкіндіктерін анықтау үшін құжаттамаға (спецификация, формуляр, пайдаланушы (бағдарламашы) нұсқаулығы, Нұсқаулық) талдау жүргізілуі тиіс әкімші (жүйелік бағдарламашы), сондай-ақ басқа да бағдарламалық, конструкторлық және пайдалану құжаттамасы) және өзге де қолжетімді бағалау объектісі туралы мәліметтерді қамтитын дереккөздерді пайдаланады.

Бағалау объектісі туралы алынған мәліметтерді талдау нәтижесінде бағалау объектісінің ықтимал қауіпті функционалдық мүмкіндіктері анықталуға немесе олардың жоқтығы расталуға тиіс.

Құжатталмаған мүмкіндіктерді анықтау үшін өзім жасаған программалық қамтама ішінде қолданатын log4j Java тілінің кітапханасын талдадым. Осы технология программалық қамтамада болатын барлық әрекеттерді сақтайды. 2022 жылы маусым айында Java өзінің жазбаларында осы жүйеде құжатталмаған мүмкіндік осалдығы табылғаны жайлы жазған. Негізгі талдау әдісі ретінде статикалық талдауды алдым.



1-сызба. Осалдықты табу үшін жүргізілетін шабуыл қадамы

Сызбада көрсетілген жүйе бойынша мен GitHub – CircleCL – ngrok – localhost технологиялар қолданып, статикалық талдау жүргіздім. Программалық қамтамада негізгі табылған осал жері tomcat программалық әдісімен байланысты болды:

```

Java
<property name="LOGS" value="./logs" />
  <appender name="Console"
    class="ch.qos.logback.core.ConsoleAppender">
    <layout class="ch.qos.logback.classic.PatternLayout">
      <Pattern>
        %white(%d{ISO8601}) ${HOSTNAME} tomcat %highlight(%-5level)
[%blue(%t)] %yellow(%C{1.}): %msg%n%throwable
      </Pattern>
    </layout>
  </appender>
  
```

1-кесте. Tomcat әдісі log4j программалық қамтамсында ақпарат ағып кетуіне соқтыруы

Pattern әдісі ішінде қолданытан tomcat жүйеде барлық болатын әрекеттерді қарапайым IP адресі білу және curl әдісі арқылы толығымен ақпараттарды алып кетуге болады. Осалдықты анықтап және шешімі ретінде жүйені жаңартып, осалдықты алып тастадым.

Қорытынды:

Қазіргі уақытта бағдарламалық жасақтамадағы негізгі қауіп - құжатталмаған мүмкіндіктердің болуы. Құжатталмаған мүмкіндіктерді іздеудің қолданыстағы құралдарының ешқайсысы оларды анықтауға кепілдік бермейді. Кешенді тестілеу қолдану бұл мәселені шешуге кепілдік беріп қана қоймай, сонымен қатар бұл процесті автоматтандыруға мүмкіндік береді. Сонымен қатар бар ақпарат қауіпсіздігінің басқа салаларында пайдалануға болатын жылдам әрекет ету бөлігінде бағдарламалық кодты оңтайландыру. Жалпығы ортақ программалық қамтаманың құжаттамалмаған мүмкіндіктерін осалдығын барлық мүмкін және жиі кездесетін жүйелерден қорғау қажет. Болашақтағы жұмыстарды осы әдістерді тікелей басқа жүйелерді практикалық іс жүзінде қолдануын қарастырамын.

Қолданылған әдебиеттер тізімі:

1. Evans, Richard. E-commerce, Competitiveness and Local and Regional Governance in Greater Manchester and Mersey side: A Preliminary Assessment // Urban Studies. — С. 947–975.
2. Online Retail Industry Profile: United States // Datamonitor Plc. – 2012. – С. 1–36 З. Лось А.Б., Нестеренко А.Ю., Рожков М.И. Криптографические методы защиты информации. –М.: Юрайт, 2016.
3. Сергеева Ю. С. Защита информации. Конспект лекций / Ю. С. Сергеева. – М.: А – Приор, 2015. – 128 с.
4. Альферов А. А. и др. Основы криптографии: Учебное пособие. – М.: Гелиос АРВ, 2001. – 34 с.
5. Конеев И. Р., Беляев А. В. Информационная безопасность предприятия. – СПб.: Питер, 2001. – 87 с

УДК 004.896

ИССЛЕДОВАНИЕ ПРОИЗВОДИТЕЛЬНОСТИ ГАЗОАНАЛИТИЧЕСКОЙ МУЛЬТИСЕНСОРНОЙ СИСТЕМЫ ПРИ ВАРИАЦИИ КОНЦЕНТРАЦИЙ МОДЕЛЬНЫХ АНАЛИТОВ

Альсеитов Олжас Айдосович
olzhas010111@gmail.com

Магистрант 1-кого курса ОП 7М06306 «Системы информационной безопасности» факультета информационных технологий, ЕНУ им. Л.Н.Гумилева, Астана, Казахстан

Сыдыков Данияр Маратович
ds.mag84@gmail.com

Магистрант 2-кого курса ОП 7М06306 «Системы информационной безопасности» факультета информационных технологий, ЕНУ им. Л.Н.Гумилева, Астана, Казахстан

Научный руководитель – Сатыбалдина Д.Ж.

Одной из задач Экологического кодекса Республики Казахстан является работы по обеспечению постоянного и систематического сбора, накопления, хранения и анализа экологической информации, в том числе с использованием современных цифровых технологий [1]. В этой связи являются актуальными исследования связанные с разработкой недорогих, портативных и быстрых цифровых систем экспресс оценки качества воздуха во внелабораторных условиях.

В качестве потенциальных кандидатов для включения в цифровые системы экологического мониторинга для детектирования вредных примесей в воздухе предлагаются газоаналитические системы типа «электронный нос», которые основаны на сенсорной технология искусственного обоняния [2]. Достижения в развитии технологии газовых сенсоров, электроники, биохимии и искусственного интеллекта позволили разработать устройства, способные измерять и характеризовать летучие ароматы, выделяемые из множества источников, для многочисленных применений [3].

Газоаналитическая система типа «электронный нос» обычно состоит из мультисенсорной матрицы, блока предобработки информации, блока обработки сенсорных данных и библиотеки сенсорных откликов на известные газообразные вещества [4]. Матрица перекрёстно-реагирующих сенсоров представлена линейкой постепенно различающихся сенсоров, выбранных для реагирования на широкий спектр химических классов и распознавания аналитов и их смесей. Выходные данные от отдельных сенсоров собираются вместе и интегрируются для создания уникального цифрового отклика, наподобие отпечатка пальца, что позволяет осуществить идентификацию и классификацию аналитов. Одной из важных проблем сенсорной технологии искусственного обоняния является необходимость применения алгоритмов машинного обучения для предварительного длительного «обучения» сенсорной системы. После серии экспериментов с