ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

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

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

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

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

2023
Астана

УДК 001+37
ББК 72+74
G99

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

ISBN 978-601-337-871-8

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 и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001+37
ББК 72+74

ISBN 978-601-337-871-8

– енгізу деректері ретінде сапалық бағалауларды өткізу мүмкіндігі, сондай-ақ шығу нәтижелері ретінде, яғни деректер мәндерімен ғана емес, олардың сенімділік және тарату дәрежелерімен жұмыс жасау мүмкіндігі;

– күрделі динамикалық жүйелерді жылдам модельдеу мүмкіндігі және оларды берілген дәлдік деңгейімен салыстырмалы талдау.

Нақты деректер болмаған жағдайда да қандайда бір критерийлердің мәндері туралы шешім қабылдаушы тұлға немесе сарапшы оларды сөзбен сипаттай алады, мысалы «соңғы бірнеше жыл біздің бәсекелестік артықшылықтарымыз айтарлықтай жоғары», «осы жыл бойы сұраныстың жоғары деңгейі сақталуда» және т.б. Осындай бағалаулар тиістілік функцияларының лингвистикалық айнымалыларын анықтауға және оларды басқа неғұрлым детерминделген көрсеткіштермен қатар компьютерлік өңдеу толығымен жеткілікті [3].

Бірқатар авторлардың зерттеулері анықталған бұлдыр жиындар динамикасы барлық дамушы жүйелерде байқалатынын көрсетті. Сонымен қатар, авторлар динамикалық ортада бұлдыр жиындар және олардың сәйкес тиістілік функцияларынды төмендегілер байқалатынын анықтады:

– аралық емес уақыт аралықтарында бұлдыр жиындардың тиістілік дәрежесі әртүрлі;

– бұлдыр жиындар элементтерінің жинағы өзгеріске ұшырайды;

– қандай-да бір бұлдыр жиын түрлі тиістілік функциясымен ұсынылуы мүмкін, уақыт аралығында өзгеретін.

Модель құрудің толық кезеңін қамтитын динамикалық бұлдыр жиынның тиістілік функциясын динамикалық деп атаймыз.

Қолданылған әдебиеттер тізімі

1. Солодуша С.В. Методы построения интегральных моделей динамческих систем: алгоритмы и приложения в энергетике: дис. ... док. техн. наук: 05.13.18. – Иркутск: Ин-т сис. Энер. им. Л.А. Мелентьева, 2018. – 353 с.

2. Терелянский П.В., Костикова А.В. Принятие решений на основе динамических нечетких множеств // Аудит и финансовый анализ. – 2013. – №1. – С. 449-457.

3. Махажанова У.Т. Динамикалық жүйелерде шешімдерді қабылдауды қолдау (шағын және орта бизнесті несиелендіру мысалында): дис. ... PhD док: 6D070300. – Астана: Л.Н. Гумилев ат. ЕҰУ, 2021. – 99с.

УДК 004.056.53

БЕЗОПАСНОСТЬ И УСТРАНЕНИЕ УЯЗВИМОСТИ ОПЕРАЦИОННОЙ СИСТЕМЫ

Жұмашев Санжар Маратқалиұлы
zhumashevsanzhar@gmail.com
магистрант 1-ого курса ЕНУ им. Л.Н.Гумилева, Нур-Султан, Казахстан
Научный руководитель – к.ф.-м.н., доцент Сауханова Ж.С.

Аннотация: *Данная обзорная статья посвящена проблеме безопасности операционных систем. В ней поясняется актуальность и важность рассматриваемой темы, приведение примеров уязвимости из практики, статистических данных. Кроме того, предложены рекомендации для устранения уязвимостей.*

Ключевые слова: *пользователь, операционная система, вредоносная программа, информационные технологии, система безопасности, уязвимость.*

В наше время компьютеры и операционные системы стали неотъемлемой частью нашей жизни и повседневной работы. Но с появлением новых технологий и возможностей также появляются и новые угрозы для безопасности данных и информации, хранимых на компьютерах и в сетях. Поэтому обеспечение безопасности операционных систем становится все более важным аспектом при использовании компьютеров.

Уязвимости операционных систем могут привести к серьезным последствиям, таким как потеря данных, нарушение конфиденциальности, повреждение программного обеспечения и даже

к угрозе безопасности жизни и здоровья людей. Поэтому важно иметь понимание о том, как уязвимости возникают и как их можно устранить.

" Безопасная операционная система сводит к минимуму риск атак и максимально защищает системные ресурсы" [1, 685]. Роль устранения уязвимостей в обеспечении безопасности операционных систем не может быть переоценена. Разработчики операционных систем регулярно выпускают обновления и исправления, которые устраняют уязвимости и улучшают безопасность системы. Тем не менее, безопасность операционной системы также зависит от действий пользователя, таких как использование сильных паролей, установка антивирусного программного обеспечения и обновление операционной системы.

Операционные системы могут содержать различные типы уязвимостей, которые могут стать объектом атак со стороны злоумышленников. Некоторые из них включают:

- уязвимости, связанные с доступом: нарушение прав доступа к файлам и папкам в операционной системе, возникающие из-за ошибок в правах доступа или из-за слабых паролей;
- сетевые уязвимости: использование сетевых протоколов и служб операционной системы, которые могут привести к уязвимостям, например, уязвимость в протоколе TCP/IP, которая позволяет злоумышленнику получить доступ к сети или выполнить атаку на сетевые ресурсы;
- уязвимости, связанные с программным обеспечением: ошибки в коде операционной системы или ее компонентов, например, уязвимость, которая позволяет злоумышленнику выполнить произвольный код на компьютере пользователя;
- физические уязвимости: связанные с физической доступностью к компьютеру, например, уязвимость, которая позволяет злоумышленнику получить доступ к компьютеру через не закрытую дверь;
- уязвимости, связанные с конфигурацией системы: неправильная конфигурация системы или ее компонентов, например, уязвимость, которая возникает из-за отключения безопасных настроек по умолчанию.

Чтобы обеспечить безопасность операционной системы, необходимо регулярно проверять наличие обновлений и исправлений, а также применять рекомендации по безопасности [2].

Статистические данные являются важным элементом при анализе уязвимостей операционных систем. Некоторые из наиболее интересных статистических данных включают три позиции. Рассмотрим их.

1. Наиболее уязвимые операционные системы: в 2021 году, по данным National Vulnerability Database (NVD), наибольшее количество уязвимостей было обнаружено в операционных системах Windows, Linux и macOS. Windows остается лидером в этом списке, с долей более 50% от общего числа уязвимостей, а у macOS и Linux доля составляет примерно по 20%.

2. Распространенные типы уязвимостей: среди наиболее распространенных типов уязвимостей, обнаруженных в 2021 году, были уязвимости веб-приложений, уязвимости сетевой безопасности, уязвимости, связанные с использованием привилегий, и уязвимости в базах данных. Согласно отчету Verizon Data Breach Investigations Report 2021, уязвимости веб-приложений остаются самым распространенным типом уязвимостей в течение последних нескольких лет.

3. Статистика эксплойтов: согласно отчету "The State of Endpoint Security Today" за 2021 год, 70% компьютерных атак основываются на известных уязвимостях, для которых уже существуют патчи. Это подчеркивает важность регулярного обновления операционных систем и программного обеспечения.

Исходя из этих статистических данных, можно заключить, что наиболее эффективным способом устранения уязвимостей является регулярное обновление операционных систем и ПО, а также внимательное отслеживание обновлений безопасности [3, 4].

Устранение уязвимостей в операционных системах является важной частью поддержания безопасности. Существуют различные методы для устранения уязвимостей, включая патчи, обновления безопасности, исправления ошибок и т.д. "Ключом к обеспечению безопасности является создание и настройка систем с хорошо спроектированной архитектурой безопасности,

правильно установленными патчами и пользователи, обученные передовым методам обеспечения безопасности." [5, 563].

Одним из наиболее распространенных методов устранения уязвимостей является выпуск патчей и обновлений безопасности операционных систем. Эти обновления содержат исправления уязвимостей и других ошибок, а также улучшения производительности и функциональности. Обновления могут быть выпущены как отдельные исправления для конкретных уязвимостей, так и регулярные обновления, содержащие исправления для нескольких уязвимостей.

Кроме того, существует широкий набор инструментов для сканирования уязвимостей и оценки безопасности операционных систем. Они могут использоваться для выявления уязвимостей и нахождения решений для их устранения. Некоторые из этих инструментов доступны как часть операционной системы, например, Security Center в операционных системах Windows.

Однако, не всегда обновление безопасности является достаточным для устранения всех уязвимостей. Некоторые уязвимости могут быть обнаружены и использованы до того, как операционная система обновится. В таких случаях может потребоваться более детальный анализ и исправление проблемы на уровне программного обеспечения [6].

Примеры из практики могут помочь более наглядно представить важность безопасности операционных систем и последствия уязвимостей, если их не устранить вовремя.

Один из известных примеров - атака WannaCry в 2017 году. Эта атака была связана с уязвимостью в Windows, которую Microsoft выпустила патч для восстановления безопасности в марте 2017 года. Однако, не все пользователи систем Windows установили этот патч, что привело к тому, что атака WannaCry распространилась по всему миру и затронула более 200 000 компьютеров в более чем 150 странах. Эта атака привела к серьезным последствиям, включая остановку работы компаний и организаций, а также потерю данных. После этой атаки Microsoft выпустила дополнительный патч для всех поддерживаемых версий Windows, чтобы исправить уязвимость.

Еще один пример - уязвимость в операционной системе MacOS High Sierra, обнаруженная в 2017 году. Эта уязвимость позволяла злоумышленникам получить неограниченный доступ к системе, не требуя пароля администратора. Apple выпустила обновление безопасности, которое исправило уязвимость, но на тот момент многие пользователи оставались уязвимыми.

Эти примеры показывают важность устранения уязвимостей в операционных системах и необходимость регулярных обновлений безопасности [7, 8].

Важно понимать, что уязвимости в операционных системах являются неизбежными, поэтому необходимо принимать меры для их устранения и обеспечения безопасности системы в целом. Как мы видели, существует множество способов устранения уязвимостей, таких как обновления безопасности, патчи и утилиты управления уязвимостями.

Однако, не стоит забывать, что безопасность операционной системы зависит не только от технических мер безопасности, но и от правильной настройки системы, адекватной политики безопасности и осведомленности пользователей. Поэтому для будущего улучшения безопасности важно обучать пользователей базовым мерам безопасности и продолжать развивать, а также улучшать технологии безопасности.

Итак, обеспечение безопасности операционных систем и устранение уязвимостей являются непременными условиями для защиты нашей конфиденциальной информации, обеспечения надежной работы систем и защиты жизни и здоровья людей.

Список использованных источников

1. A. Silberschatz, P. B. Galvin (Author), G. Gagne. Operating System Concepts. ISBN 978-1118063330. -Wiley. – 2012. - 976 с.

2. Operating System Security. OWASP, 2021. - URL: https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A6-Security_Misconfiguration

3. Information Technology Laboratory. National Vulnerability Database. URL: https://nvd.nist.gov/

4. Verizon Data Breach Investigations Report, 2021. URL: https://enterprise.verizon.com/resources/reports/dbir/
5. S. L. Pfleeger. Security in Computing. - Prentice Hall, 2006. - 845 с. - ISBN 978-0132390774.
6. What is Vulnerability Management? // Tenable, URL: https://www.tenable.com/solutions/vulnerability-management
7. R. Cellan-Jones. Massive ransomware infection hits computer in 99 countries // BBC News. 2017. URL: https://www.bbc.com/news/technology-39901382
8. D. Lee. Apple rushes to fix major password bug // BBC News, 2017. URL: https://www.bbc.com/news/technology-42161823

ӘОЖ 004

БҰЛТТЫ ҚОЙМАДАҒЫ ҚАУІПСІЗДІК: БҰЛТТАҒЫ ДЕРЕКТЕР МЕН ҚОЛДАНБАЛАРДЫ ҚАУІПСІЗ САҚТАУ

Исабай Темірлан Бақытбекұлы
isabayev14@mail.ru
Ақпараттық қауіпсіздік жүйелері мамандығының Л.Н.Гумилев атындағы ЕҰУ студенті, Астана, Қазақстан
Ғылыми жетекші – Е.Қайупов

Бұлтты қойма - бұл деректерді жергілікті құрылғыда сақтаудың орнына провайдердің серверлерінде қашықтағы жерде сақтауға мүмкіндік беретін қызмет болып табылады. Бұлтты қойма пайдаланушыға желіге қосылған кез келген құрылғы арқылы деректерді интернет арқылы сақтауға, синхрондауға және бөлісуге мүмкіндік береді. Бұлтты қойманың әртүрлі түрлері Google Drive, Dropbox, OneDrive, iCloud және тағы басқалары болады. Бұлтты қойманың басты артықшылықтары:

- кез-келген құрылғыдан және интернетке қол жетімді әлемнің кез-келген нүктесінен деректерге қол жеткізу мүмкіндігі;
- деректерді бірнеше құрылғылар арасында синхрондау мүмкіндігі;
- құжаттар мен жобаларды басқа пайдаланушылармен бірлесіп жұмыс істеудің ыңғайлы тәсілі;
- жергілікті құрылғы істен шыққан жағдайда деректерді жоғалтудан қорғау;
- деректердің автоматты сақтық көшірмесі;

Сондай-ақ, бұлтты қоймада деректер қашықтан сақталады. Бұлтты қойманы пайдаланудың кемшіліктері:

- деректерге қол жеткізу үшін интернетке кіру қажеттілігі;
- бұлтты қоймаға рұқсатсыз кіру жағдайында деректердің бұзылуы және құпиялылықтың бұзылу қаупі;
- бұлтты қойма провайдерінің серверіне кіру проблемалары туындаған жағдайда деректерге қол жеткізуді шектеуж
- деректерді қорғауды шектеулі бақылау, өйткені бұлтты қойма провайдерінің міндеті;
- деректерді сақтаудың үлкен көлемі қажет болған жағдайда бұлтты қойма пайдаланудың жоғары құны.

Бұлтты қойма қауіпсіздігі - бұлтты есептеу жүйелерін қорғауға арналған киберқауіпсіздік бөлімі. Бұған барлық желілік инфрақұрылым нысандарында, онлайн қолданбалар мен платформаларда құпиялылық пен деректерді қорғау кіреді. Бұлтқа негізделген провайдерлер де, жеке тұлғалар, шағын және орта бизнес немесе корпорациялар болсын, пайдаланушылар да атсалысуы керек болып табылады. Бұлтты қойма қызметтері тұрақты Интернет байланысы бар серверлерде орналастырылады. Сондықтан бұлтта сақталған жеке деректердің қол