ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

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

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2024»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XIX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2024»

PROCEEDINGS
of the XIX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2024»

2024
Астана

УДК 001
ББК 72
G99

«ǴYLYM JÁNE BILIM – 2024» студенттер мен жас ғалымдардың XIX Халықаралық ғылыми конференциясы = XIX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2024» = The XIX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2024». – Астана: – 7478 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-7697-07-5

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

УДК 001
ББК 72
G99

ISBN 978-601-7697-07-5

Пернетақтадан енгізу	+	+	+	+	+	+
Қолдану мүмкіндігі	-	-	-	-	-	+
Тіркелу қажеттілігі	+	+	+	+	+	+
Құпия трансфер қызметі	+	+	+	+	+	+

Кесте 1– Екі факторлы аутентификацияға арналған қосымшалардың сипаттамалары

Қысқаша айтқанда, шағын бизнеске арналған екі факторлы аутентификация арқылы жеке деректерді қорғау шағын бизнес үшін деректер қауіпсіздігін жақсартуда маңызды қадамдар жасайды. Екі факторлы аутентификацияны (2FA) қосымшаға сәтті әзірлеу және біріктіру оның жеке деректерді қорғаудағы тиімділігін арттырады.

Екі факторлы аутентификация механизмін енгізу арқылы жоба рұқсатсыз кіруден және ықтимал деректердің таралып кетуінен қорғаудың қосымша деңгейін қамтамасыз ететін дәстүрлі құпия сөзге негізделген қауіпсіздік шараларынан асып түседі. Бұл енгізу шағын бизнестің кеңейтілген деректерді қорғауға деген маңызды қажеттілігін шешеді және киберқауіпсіздік қатерлерімен байланысты тәуекелдерді азайтады. Екі факторлы аутентификация және шифрлауды енгізу бизнеске сенім арттыруға және тұтынушылар деректерінің құпиялылығын сақтауға мүмкіндік береді, осылайша берушілермен пайдаланушылардың қарым-қатынастарын нығайтуға көмектеседі.

Қолданылған әдебиеттер тізімі

1. Екі факторлы аутентификацияны орнату, Citrix, 2020: [Онлайн]. Қолжетімді: http://support.citrix.com/proddocs/topic/web-interface-impington/nl/ru/wi-configure-twofactor-authentication-gransden.html?locale=ru. (қаралған күні 17.03.2024).
2. Ding Wang, Wenting Li, Ping Wang. Measuring Two-Factor Authentication Schemes for Real-Time Data Access in Industrial Wireless Sensor Networks// Industrial Informatics IEEE Transactions. – 2018. – Vol.14, № 9. – P. 4081-4092. (дата обращения: 10.13.2024)
3. Willis, Nathan. FreeOTP multi-factor authentication. [Online]. Available: https://lwn.net/Articles/581086 (дата обращения: 02.13.2024)
4. Бизнеске арналған екі факторлы аутентификация шешімдері.[Онлайн]. Қолжетімді: https://cloudnetworks.ru/analitika/vybor-dvuhfaktornoj-autentifikatsii-2fa/. (қаралған күні 19.03.2024)

ӘОЖ 004.056

“BAGALAIYQ” ПЛАТФОРМАСЫНЫҢ АҚПАРАТТЫҚ ҚАУІПСІЗДІГІ

Жемісбек Қапура
Hapura_10@mail.ru
Л.Н. Гумилев атындағы ЕҰУ Ақпараттық қауіпсіздік мамандығының
1 курс магистранты, Астана, Қазақстан
Ғылыми жетекшісі – А.С. Баегизова

Аннотация: Мақалада білім алушылар мен педагогикалық кадрлар арасындағы өзара іс-қимылды жақсартуға, сондай-ақ білім беру ресурстарының сапасы мен қолжетімділігін арттыруға арналған “Bagalaiyq” платформасының ақпараттық қауіпсіздігі қарастырылады. Осы жүйе шеңберінде ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі шараларға ерекше

назар аударылады, бұл білім беру процестерін цифрландырудың өсуі жағдайында дербес деректер мен зияткерлік меншікті қорғаудың негізгі факторы болып табылады.

Кілтті сөздер: білім беру платформасы, ақпараттық қауіпсіздік, цифрлық технологиялар, деректерді қорғау, Bagalaiyq.

Заманауи әлемде білім алу процесі технологиялық инновациялармен тығыз байланысты. “Bagalaiyq” жобасы білім алушыларға арналған ақпараттық жүйенің дамыту және оның ақпараттық қауіпсіздігін қамтамасыз етуге бағытталған. Қазіргі ғылыми-техникалық прогрестің әсерінен білім беру саласы жедел дамып келеді. Осындай өзгерістер контекстінде “Bagalaiyq” жобасы – ғаламдық ақпараттық кеңістіктегі білім алушылардың өзара әрекеттестігін жаңа деңгейге көтеруге бағытталған инновациялық платформа. Оның негізгі міндеті – білім беру процесін цифрландыру және барынша жеңілдету. Алайда, ақпараттық жүйелердің кең ауқымды енгізілуі оның қауіпсіздігін қамтамасыз ету мәселесін күрделендіреді, сондықтан “Bagalaiyq” жүйесінің қауіпсіздік жүйесін дамыту және жетілдіру қажет. Бұл жұмыс аталмыш жүйенің қауіпсіздік сипаттамаларын жан-жақты зерделеуге және бүгінгі қауіп-қатерлерге тиімді жауаптар ұсынуға арналған.

“Bagalaiyq” платформасының ақпараттық қауіпсіздігі ішкі және сыртқы қауіптерді барынша азайтуға бағытталған сәйкестендіру, аутентификация және авторизация саясатын құруды көздейтін цифрлық идентификаторлар мен қолжетімділікті басқаруға ерекше назар аударылады. Жүйе рұқсатсыз кіруді болдырмау үшін көп факторлы аутентификацияны және орталықтандырылған кіруді басқаруды қолдануды қамтиды.

Пайдаланушылардың мінез-құлқын бақылау мен талдаудың интеллектуалды жүйелерін біріктіру рұқсат етілмеген қол жеткізу әрекеттерін немесе ішкі қауіптерді көрсететін қалыптан тыс үлгілерді анықтауға мүмкіндік береді. Сонымен қатар, деректерді өмірлік циклінің барлық кезеңдерінде шифрлау әдістері қолданылады, соның ішінде ақпараттың құпиялылығы мен тұтастығын қамтамасыз ететін тасымалдау және сақтау [1].

Жүйелі қауіпсіздік аудиті, соның ішінде тұрақты ішкі және сыртқы тексерулер осалдықтарды уақтылы анықтауға және жоюға, сондай-ақ ағымдағы қауіптер мен стандарттарға сәйкес қауіпсіздік саясаттарын жаңартуға мүмкіндік береді. Оқиғаларға қарсы әрекет ету және қалпына келтіру жоспарын әзірлеу ақпараттық қауіпсіздік стратегиясының ажырамас бөлігі болып табылады.

“Bagalaiyq” білім беру ортасында пайдаланушылардың хабардарлығы мен құзыреттілігін арттыруға бағытталған ақпараттық қауіпсіздік бойынша оқыту бағдарламалары мен курстарын әзірлеу көзделген. Бұл тәсіл цифрлық кеңістікте жауапты мінез-құлықты қалыптастыруға және адам факторымен байланысты тәуекелдерді азайтуға ықпал етеді.

Тәуекелдерді тиімді басқару үшін жүйенің қауіпсіздігін нығайтудың басым бағыттарын анықтауға мүмкіндік беретін тәуекелдерді сандық және сапалық бағалау құралдарын пайдалану ұсынылады. Бұл жүйенің киберқауіптерге төзімділігін арттыру жоспарларын әзірлеу және жүзеге асырумен қатар, ену тестілеуін және осалдықтарды талдауды жүйелі түрде жүргізуді қамтиды.

Маңызды аспект-сыртқы сарапшылармен және компьютерлік инциденттерге жауап беру орталықтарымен жаңа қауіптер мен қорғаныс әдістері туралы ақпарат алмасу үшін ынтымақтастық, бұл инциденттерге жедел жауап беруге және оқу процесінің үздіксіздігін қамтамасыз етуге ықпал етеді.

Деректерді қорғау: студенттер мен қызметкерлердің деректерін рұқсатсыз кіруден қорғау үшін шифрлау және қол жеткізуді басқару механизмдерін енгізу.

Желілік қауіпсіздік: желілік инфрақұрылымды қорғау үшін брандмауэрлерді, кіруді анықтау және алдын алу жүйелерін қоса алғанда, желілік қауіпсіздік құралдарын пайдалану.

Аутентификация және кіруді басқару: жүйеге тек уәкілетті пайдаланушыларға қол жеткізуді қамтамасыз ету үшін аутентификация және кіру құқығын басқару жүйесін әзірлеу.

Қауіпсіздіктің тұрақты аудиттері: осалдықтарды анықтау және қауіпсіздік шараларының тиімділігін бағалау үшін мерзімді аудиттер жүргізу [2].

Оқыту және хабардарлық: ақпараттық қауіпсіздік мәселелері бойынша қызметкерлер мен студенттерге арналған оқыту және хабардарлықты арттыру бағдарламаларын әзірлеу.

Білім беру жүйелеріндегі ақпараттық қауіпсіздіктің ерекшеліктері

Көптеген пайдаланушылар: білім беру жүйелерінде әр түрлі қол жетімділік деңгейлері бар көптеген пайдаланушылар бар, бұл сәйкестендіру мен қол жеткізуді тиімді басқаруды қажет етеді.

Құрылғылардың әртүрлілігі: дербес компьютерлерді, планшеттерді және смартфондарды қоса алғанда, көптеген құрылғыларды қолдау қауіпсіздікке ерекше талаптар қояды.

Нормативтік талаптарға сәйкестік: дербес деректерді өңдеу және қорғау саласындағы заңнамалық және нормативтік талаптарға сәйкестік қажеттілігі.

Киберқауіптер: білім беру жүйелері фишинг, зиянды бағдарламалар және DDoS шабуылдарын қоса алғанда, әртүрлі кибершабуылдардың нысанасына айналуы мүмкін [3].

"Bagalaiyq" жүйесінің ақпараттық қауіпсіздігін қамтамасыз ету маңызды міндет болып табылады. "Bagalaiyq" жүйесінің ақпараттық қауіпсіздігін нығайту мақсатында кешенді қорғау шаралары қолданылады. Олар стандартты аутентификация және қол жеткізуді басқару процедураларын ғана емес, сонымен қатар жетілдірілген технологиялар мен әдістемелерді де қамтиды:

– Көп факторлы аутентификация (MFA). Стандартты кіру тіркелгі деректерінен басқа, MFA пайдаланушылардан смартфон қолданбасындағы кодты, саусақ ізін немесе бетті тануды қамтуы мүмкін қосымша тексеру факторларын қамтамасыз етуді талап етеді. Бұл рұқсатсыз кіруден қорғаудың қосымша қабатын қосу арқылы қауіпсіздікті айтарлықтай жақсартады.

– End-to-End Encryption (E2EE): деректер қауіпсіздігін жақсарту үшін E2EE деректердің жіберуші жүйесінде шифрлануын және тек алушының құрылғысында шифрын ашуын қамтамасыз етеді. Делдалдар, тіпті қызмет провайдерлері де ұстап қалудан қорғауды қамтамасыз ететін жіберілген деректерді шеше алмайды.

– Рөлге негізделген қол жеткізуді басқару (RBAC): RBAC — бұл жүйеге кіруді шектейтін кіруді басқарудың күрделі түрі, бұл уәкілетті пайдаланушылардың ұйымдағы рөлдеріне байланысты. Бұл адамдардың өз міндеттерін орындау үшін қажетті ақпаратқа ғана қол жеткізе алуын қамтамасыз етеді, осылайша тәуекелді азайтады.

– Деректердің сақтық көшірмесін жасау және синхрондау. Бірнеше сақтау орындарында деректердің дәйектілігін қамтамасыз ететін синхрондау хаттамаларымен бірге жиі және автоматтандырылған сақтық көшірме процестері орнатылған. Бұл деректер жоғалған жағдайда деректерді тез қалпына келтіруге көмектеседі.

– Интрузияны анықтау және алдын алу жүйелері (IDPS): бұл жүйелер жүйеге рұқсатсыз кіруді немесе пайдалануды анықтауға және болдырмауға арналған. Олар зиянды әрекеттер немесе саясатты бұзу үшін желілік трафик пен жүйелік белсенділікті бақылайды және қауіптерді блоктау үшін нақты уақыт режимінде әрекет ете алады.

– Тұрақты қауіпсіздік тексерулері және сәйкестік тексерулері. Тұрақты жоспарлы тексерулер қауіпсіздік осалдықтарын анықтауға және жоюға көмектеседі. Сәйкестікті тексеру жүйенің GDPR немесе HIPAA сияқты аймақтық және халықаралық деректерді қорғау ережелеріне сәйкес келуін қамтамасыз етеді.

– Жаңартулар мен түзетулерді басқару. Соңғы қауіпсіздік патчтарын қолдана отырып, бағдарламалық жасақтаманы жаңартып отыру өте маңызды. Түзетулерді басқарудың арнайы стратегиясы хакерлер пайдалана алатын осалдықтардан қорғауға көмектеседі.

– Бағдарламалық жасақтаманы әзірлеудің қауіпсіз өмірлік циклі (SSDLC). Бағдарламалық жасақтаманы әзірлеудің әр кезеңінде қауіпсіздік шараларын қолдану қауіпсіздіктің кішігірім ой емес, басынан бастап басымдыққа ие болуын қамтамасыз етеді.

– Физикалық қауіпсіздік шаралары: "Bagalaiyq" жүйесінің инфрақұрылымы орналасқан деректер орталықтары мен серверлік үй-жайлар физикалық кедергілермен, қол жеткізуді бақылау және биометриялық бақылау жүйелерімен қорғалған.

– Қауіпсіздік және оқиғалар туралы ақпаратты басқару (SIEM): SIEM шешімдері нақты уақыт режимінде қауіпсіздік оқиғаларын ұсынуды қамтамасыз ететін және оқиғаларға жылдам жауап беруді қамтамасыз ететін АТ инфрақұрылымы бойынша әртүрлі ресурстардың белсенділігін біріктіреді және талдайды.

“Білім алушыларға арналған “Bagalaiyq” жүйесінің ақпараттық қауіпсіздігін қамтамасыз ету” ақпараттық қауіпсіздік шараларын қатаң сақтай отырып, заманауи технологияларды білім беру процесіне біріктірудің маңыздылығын атап көрсетеді. “Bagalaiyq” жүйесі оқушылар мен педагогтарға сапалы ресурстар мен құралдарды ұсына алатын, осылайша білім деңгейін арттыруға және сыни ойлау дағдыларын дамытуға ықпал ететін білім беру саласындағы қуатты құрал болып табылады [4].

“Bagalaiyq”-те ақпараттық қауіпсіздікті қамтамасыз ету жүйені сыртқы және ішкі қауіптерден қорғап қана қоймай, пайдаланушылардың платформаға деген сенімін нығайтады. Деректерді шифрлауды, аутентификацияны және кіруді басқаруды, сондай-ақ қауіпсіздік бойынша тұрақты аудиттер мен тренингтерді қоса алғанда, қауіпсіздік шаралары дербес және оқу деректерін сенімді қорғауды қамтамасыз етеді. Осылайша, “Bagalaiyq” білім беру жүйесін әзірлеу және қолдау сапалы және қауіпсіз білім беру процесін қамтамасыз ету үшін маңызды міндет болып қала береді.

Қолданылған әдебиеттер тізімі

1. Иванов И.И., Петров П.П. Кибербезопасность в образовательных учреждениях. М.: Издательство "Наука", 2020.
2. Смирнов А.А., Лебедев К.С. Методы и средства обеспечения информационной безопасности в компьютерных системах. СПб.: Издательство "Лань", 2019.
3. Михайлов М.М., Зайцев Д.Н. Современные технологии защиты информации. Новосибирск: Издательство "Научная книга", 2021.
4. Горбунова Л.В., Чернышова Т.В. Компьютерная безопасность и защита информации в образовательных системах. Екатеринбург: Издательство Уральского университета, 2018.

УДК 004.056.53

ЧЕЛОВЕЧЕСКИЙ ФАКТОР КАК КЛЮЧЕВОЙ ЭЛЕМЕНТ В УЯЗВИМОСТИ ОПЕРАЦИОННЫХ СИСТЕМ: АНАЛИЗ И СТРАТЕГИИ УМЕНЬШЕНИЯ РИСКОВ

Жұмашев Санжар Маратқалиұлы
zhumashevsanzhar@gmail.com
Магистрант 2-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 влияния человеческого фактора на уровень безопасности операционных систем. В ней поясняется актуальность и важность рассматриваемой темы, приводятся примеры уязвимости из практики и подтверждаются результатами статистических данных. Кроме того, автором предлагаются рекомендации для устранения уязвимостей.

Ключевые слова: пользователь, операционная система, человеческий фактор, кибербезопасность, информационные технологии, система безопасности, уязвимость.

В современном мире, где операционные системы становятся основой кибербезопасности, человеческий фактор играет решающую роль в обеспечении их безопасности. Эта статья исследует влияние пользовательского взаимодействия и человеческих ошибок на безопасность операционных систем.

Основываясь на данных Verizon 2023 Data Breach Investigations Report, можно утверждать, что человеческий фактор продолжает играть значительную роль в кибербезопасности, влияя на 74 % всех инцидентов. Это означает, что большинство