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

Для укрепления киберустойчивости критически важных инфраструктур в Казахстане, страна активно разрабатывает и внедряет национальные стандарты кибербезопасности, нацеленные на повышение уровня защиты от киберугроз. Важным аспектом является обучение и повышение осведомленности сотрудников о методах противодействия кибератакам, что включает в себя разработку программ обучения и кампаний по повышению кибергигиены. Кроме того, Казахстан активизирует усилия в области межведомственного и международного сотрудничества для обмена информацией о киберугрозах и совместной разработки мер по их нейтрализации, что позволяет стране интегрировать мировой опыт и лучшие практики в национальную систему кибербезопасности.

Использование современных технологий защиты, включая системы обнаружения вторжений и многофакторную аутентификацию, играет ключевую роль в защите критической инфраструктуры. Разработка и тестирование планов реагирования на инциденты кибербезопасности также являются важной составляющей общей стратегии защиты, позволяя организациям эффективно реагировать на кибератаки и минимизировать их последствия.

На международном уровне Казахстан принимает активное участие в различных инициативах и сотрудничает с международными организациями, такими как ОБСЕ, Интерпол и Глобальный альянс по кибербезопасности. Это сотрудничество позволяет стране обмениваться опытом, знаниями и информацией о киберугрозах, повышая тем самым эффективность национальных мер по обеспечению кибербезопасности.

Таким образом, Казахстан реализует комплексный подход к защите критически важных инфраструктур от киберугроз, включая разработку и внедрение стандартов и нормативных актов, повышение осведомленности и компетенций сотрудников, укрепление международного сотрудничества, а также применение современных технологий и методик защиты. Эти меры направлены на создание устойчивой и эффективной системы кибербезопасности, способной противостоять современным и будущим киберугрозам.

Список использованной литературы

1. Льюис Дж.А., Нойнек Г. "Кибербезопасность и защита критически важной инфраструктуры: сравнительный анализ международных подходов" // Журнал по безопасности родины и управлению чрезвычайными ситуациями, 2015.

2. Агентство Европейского Союза по кибербезопасности (ENISA) "Обзор угроз для критической инфраструктуры" // Агентство Европейского Союза по кибербезопасности (ENISA), 2020.

3. Кшетри Н. "Киберпреступность и кибербезопасность в глобальном Юге" // Palgrave Macmillan, 2013.

4. Ассанте М.Дж., Тоби Д.Х. "Усиление кибербезопасности критически важной инфраструктуры" // IEEE Безопасность и конфиденциальность, 2011.

5. Ван В. и др. "Искусственный интеллект для кибербезопасности: обзор" // Журнал науки и технологий в области компьютеров, 2019.

6. Государственная техническая служба Республики Казахстан "Кибердайджест за год" [Электронный ресурс] // Государственная техническая служба Республики Казахстан, 2022. https://sts.kz/wp-content/uploads/2023/01/year-2022-digest.pdf

7. Позитив Технологии "Кибербезопасность в Азии: аналитический обзор" [Электронный ресурс] // Позитив Технологии, 2023. https://www.ptsecurity.com/ru-ru/research/analytics/asia-cybersecurity-threatscape-2022-2023

УДК 004.056.5

БІЛІМ БЕРУ ПОРТАЛДАРЫНА SQL-ШАБУЫЛДАРЫН ЗЕРТТЕУ ӘДІСТЕМЕСІ

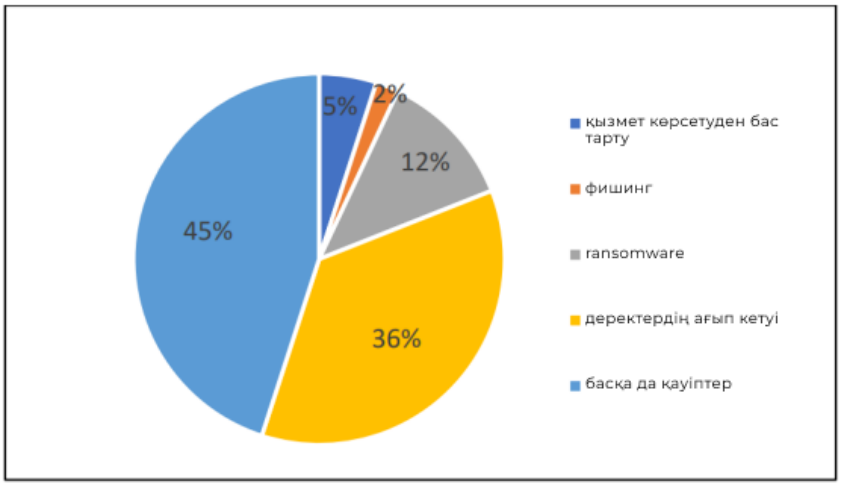
Тұрсынова Әселя Ғалымжанқызы
tursynova-2021@mail.ru

Л.Н.Гумилев атындағы ЕҰУ, «Ақпараттық технологиялар» факультетінің 4-курс студенті, Астана, Қазақстан
Ғылыми жетекшісі – «Ақпараттық қауіпсіздік» кафедрасының аға оқытушысы Г.И.Аймичева

Қазіргі цифрлық қоғамда білім беру ортасы үшін киберқауіпсіздік мәселесі өзекті және маңызды болып отыр. Білім беру ортасында қауіпсіздікті қамтамасыз ету студенттердің, оқытушылардың және әкімшілік қызметкерлердің жеке деректерінің құпиялылығын қорғап қана қоймайды, сонымен қатар оқу барысының үздіксіздігін қамтамасыз етеді, білім беру ұйымдарына және олардың беделіне елеулі зиян келтіруі мүмкін ықтимал кибершабуылдардың алдын алады. Бұл мақалада білім беру ортасы үшін киберқауіпсіздіктің маңыздылығы және білім беру порталдарының қауіпсіздігінің маңыздылығын қарастырамыз. Білім беру саласы үшін көптеген статистикалар қарастырылып, оларға жасалатын шабуылдарға тоқталып кеттік.

Білім беру саласын қамтыған ақпараттық революцияның артықшылықтарының бірі - электрондық оқыту немесе цифрлық білім беру. Көптеген ғалымдар білім беру саласындағы киберқауіпсіздік мәселелерін мұқият зерттеп жатыр, соның ішінде Массачусетс технологиялық институтынан (MIT) Джонатан Либовиц, Мадридтегі Карлос III университетінен Мариана Делгадо-Реституто. Бұл мәселеге белсене араласқан елдердің бірі – АҚШ. Массачусетс технологиялық институты (MIT), Стэнфорд университеті және Карнеги Меллон университеті сияқты жетекші университеттер мен зерттеу орталықтары білім берудегі киберқауіпсіздікке қатысты зерттеулер жүргізіп, инновациялық тәсілдерді әзірлеуде.

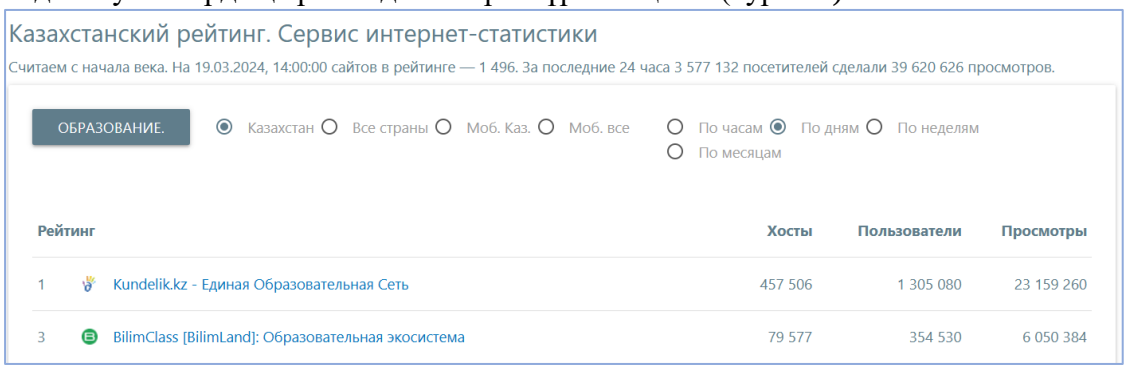
Жалпы білім беру ортасы үшін 2020 жылдан бастап Ddos шабуылдарының 2019 жылмен салыстырғанда айтарлықтай саны артқан [1].



Сурет-1. білім беру саласындағы кибершабуылдар [2].

Ескере кететін жағдай Қазақстанда болған оқиғаны қарастырсақ болады. Ұлттық қауіпсіздік комитетінің Мемлекеттік техникалық қызметі (ҰҚК МТҚ) Қазақстандағы білім беру платформаларына хакерлік шабуыл жасалғаны туралы хабарлаған. Қазақстандық kundelik.kz және bilimland.kz білім беру порталдарына Ddos шабуылы жасалған. Ведомствоның хабарлауынша, kundelik.kz сайтындағы шабуылдарды тіркелгеннен кейін сегіз минуттан кейін bilimland.kz білім беру порталына DDoS шабуылдары жасалған. KZ-CERT қызметінің сарапшылары осы фактіге сүйене отырып, шабуылдар өзара байланысты және қашықтықтан оқыту кезеңінде білім беру порталдарының функционалдығын бұзуға бағытталған деген қорытындыға келді. Сонымен қатар, OnlineMektep.org білім беру платформасы үшін де Ddos шабуылдары жасалған. Платформаны әзірлеушілер шабуылды ұйымдасқан және пайдаланушы сеніміне нұқсан келтіруге бағытталған деп санайды. Жоба жетекшісі Санжар Кенжеханұлының айтуынша, бүгінде «OnlineMektep» Қазақстан Республикасы Ұлттық қауіпсіздік комитетінің Мемлекеттік техникалық қызметі көрсеткен

қорғаныстың арқасында шабуылға төтеп берген. Бүгінгі сыртқы DDoS шабуылы платформадағы жүктеменің он есе артуына әкеліп соқтырған ең ауыры болды. Бұл қазақ интернетінің бүкіл тарихындағы ең ірі цифрлық шабуылдардың бірі болған. Жалпы бұл білім беру порталдарына қазіргі таңда пайдаланушылар тарапынан сұраныс өте жоғары. Осы жағдайды ескере отырып бұл білім беру порталдары үшін киберқауіпсіздіктің маңызынң ескеруіміз қажет. Zero.kz сайтының 2024 жылғы статистикасы бойынша соңғы уақытта бұл сайттар пайдаланушылардың арасында жоғары сұранысқа ие (сурет-2).



Сурет-2. Қазақстандық білім беру порталдарын пайдалану статистикасы [3].

Бірақ та осы порталдарға көптеген кибершабуылдар жасалатынын ескере кету қажет және де олардың қауіпсіздік деңгейін жақсартқан дұрыс. Білім беру саласындағы шабуылдарға тоқталып кетсек [2]:

Фишингтік шабуылдар: киберқылмыскерлер сенімді дереккөздерді жасыру арқылы деректерге қол жеткізуге тырысуы мүмкін. Мысалы, олар логиндерді, құпия сөздерді немесе басқа құпия ақпаратты алу үшін білім беру мекемесінің қызметкері болып көрінетін электрондық хаттарды жіберуі мүмкін.

SQL инъекция: шабуылдың бұл түрінде шабуылдаушы зиянды SQL командаларды сұраулар ретінде енгізеді. Бұл веб-қосымшаның қауіпсіздік шараларын айналып өтуге және деректер базасының серверінен құпия мазмұнды алуға мүмкіндік береді.

Қызмет көрсетуден бас тарту (DoS): бұл шабуыл веб-сайтты немесе серверді тоқтатуға, оның ресурстарын тұтынушыларға қолжетімсіз етуге бағытталған. Мысалы, DoS шабуылы банктік веб-сайтты немесе электрондық почта қызметін бірнеше сағатқа, тіпті күндерге жауып, уақыт пен ақшаны жоғалтуы мүмкін. Жалпы білім беру саласында жасалатын шабуылдар түрі өте көп.

SQL шабуылының цифрлық ізін анықтаудың технологиялары мен әдістері.

SQL инъекция веб-қосымшалардағы ең көп таралған шабуыл әдістерінің бірі болып табылады, мұнда шабуылдаушылар дерекқорға рұқсатсыз кіру үшін пайдаланушы енгізуіне SQL кодтарын енгізеді. SQL шабуылдарының сандық іздерін анықтау үшін әртүрлі технологиялар мен әдістер бар. Олардың кейбіреулерін қарастырайық [4]:

IDS журнал файлдары: Көптеген заманауи IDS/IPS жүйелерінде дерекқор шабуылдарын, соның ішінде SQL инъекцияларын анықтау үшін қолтаңбалар бар. Олар желілік трафикті талдай алады және күдікті SQL сұрауларын анықтай алады, бұл шабуылдардың алдын алуға немесе олардың ықтимал пайда болуы туралы ескертуге мүмкіндік береді.

Веб-қауіпсіз сүзгілерді (WAF) пайдалану: WAF – кіріс HTTP трафигін сүзе алатын және ықтимал қауіпті SQL құрылымдары бар сұрауларды блоктай алатын веб-бағдарламаның қауіпсіздік құралдары. Оларды жалпы SQL инъекция үлгілерін тану және олардың орындалуын блоктау үшін конфигурациялауға болады.

Қауіпсіздік аудиті: тұрақты веб-бағдарлама қауіпсіздік аудиттерін жүргізу ықтимал осалдықтарды, соның ішінде SQL инъекцияларын анықтай алады. Аудит барысында веб-қосымшалар талданады және инъекция үшін пайдаланылуы мүмкін осал деректерді енгізу нүктелерінің бар-жоғына сыналады.

SQL шабуылында қолданылатын жасыру әдістері [4].

Кибершабуылшылар веб-сайттардағы қауіпсіздік тетіктерін айналып өту үшін әртүрлі жасыру әдістерін пайдаланады. Олардың кейбіреулері төменде талқыланды:

1. Жолдық түсініктеме: Қауіпсіздік механизмдерін айналып өту үшін шабуылдаушылар шабуыл жасалған жолдардың ортасында кірістірілген түсініктемелерді пайдаланады.
2. Таңбаларды кодтау немесе қос кодтау: Кейбір WAF-тер он алтылық кодталған кіріс деректерін декодтайды және шабуылдың алдын алып, оларды сүзеді. Оларды айналып өту үшін кибершабуылдаушылар кіріс деректерін екі рет кодтай алады.
3. Регистрді ауыстыру: Кейбір қолданбалар кіші әріппен жазылған SQL кілт сөздерін блоктайды. Осындай жағдайда кибершабуылшылар осы қорғау механизмін айналып өту үшін айнымалы регистрде жазылған кодты пайдаланады. Кейбір желіаралық қалқандарда тұрақты өрнек сүзгісі (regex)/union\select/g бар. Сондықтан олар кіші әріптермен жазылған күдікті кодты сүзе алады.

Білім беру порталдарды киберқауіптерден қорғау үшін келесі шараларды қабылдау қажет:

- Қызметкерлер мен студенттерді оқыту: қызметкерлер мен студенттер үшін киберқауіпсіздік бойынша оқыту бағдарламаларын жүйелі түрде жүргізу маңызды. Олар әртүрлі шабуыл түрлерін және олардан қалай қорғану керектігін білуі қажет.
- Заманауи қауіпсіздік жүйелерін пайдалану: антивирустық бағдарламаларды, желіаралық қалқандарды, шабуылдарды анықтау жүйелерін және басқа қауіпсіздік шараларын орнату шабуылдардың алдын алуға көмектеседі.
- Қатаң қауіпсіздік саясаттарын жасау: білім беру мекемелері қол жеткізуді басқару, құпия сөздер, деректердің сақтық көшірмесін жасау және ақпаратты ортақ пайдалану бойынша қатаң саясаттарды әзірлеуі және енгізуі керек.

Білім беру саласы әрқашанда маңызды аспектілердің бірі екенінін біле отырып, оның қауіпсіздігін қамтамасыз етуді де басты мақсат ретінде қараумыз қажет. Білім беру саласындағы киберқауіпсіздікті қамтамасыз ету қызметкерлер мен студенттерді оқытудан бастап заманауи технологиялық шешімдерді енгізуге дейінгі шараларды біріктіруді талап етеді. Білім беру ұйымдарында қауіпсіздікті сақтау деректердің құпиялылығын қорғап қана қоймай, білім беру процесінің үздіксіздігін қамтамасыз етеді.

Пайдаланылған әдебиеттер тізімі

1. Yousif Yaseen, K. A. (2022). Digital Education: The Cybersecurity Challenges in the Online Classroom (2019-2020). Asian Journal of Computer Science and Technology, 11(2), 33–38. https://doi.org/10.51983/ajcst-2022.11.2.3450

2. Юсиф Ясин, К. А. (2022). Важность кибербезопасности в секторе высшего образования 2022. Азиатский журнал компьютерных наук и технологий, 11 (2), 20–24. https://doi.org/10.51983/ajcst-2022.11.2.3448

3. Қазақстандық білім беру порталдарының рейтингі https://zero.kz/cat_id_7-obrazovanie-nauka/?ysclid=lu5614cmt1913585664

4. Digital Forensics Essentials. EC-Council official curricula. EC-Council, 2021

УДК 512.647

АУТЕНТИФИКАЦИЯНЫ КҮШЕЙТУДЕГІ ИННОВАЦИЯЛЫҚ ТӘСІЛДЕР

Хамитов Алмат Рустемович

almat1001@mail.ru

Л.Н.Гумилев атындағы ЕҰУ Ақпараттық технологиялар факультеті «7М06306 – Ақпараттық қауіпсіздік жүйелері» білім беру бағдарламасының 1-курс магистранты**,** Астана, Қазақстан

Ғылыми жетекшісі – Ташенова Ж.М.