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

©Л.Н. Гумилев атындағы Еуразия ұлттық университеті, 2024

5. Gupta B. B. et al. A novel approach for phishing URLs detection using lexical based machine learning in a real-time environment //Computer Communications. – 2021. – Т. 175. – С. 47-57.

6. Hidayat R. et al. Similarity measure fuzzy soft set for phishing detection //International Journal of Advances in Intelligent Informatics. – 2021. – Т. 7. – №. 1. – С. 101-111.

7. Barraclough P. A., Fehringer G., Woodward J. Intelligent cyber-phishing detection for online //computers & security. – 2021. – Т. 104. – С. 102123.

8. Stobbs J., Issac B., Jacob S. M. Phishing web page detection using optimised machine learning //2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). – IEEE, 2020. – С. 483-490.

Wei W. et al. Accurate and fast URL phishing detector: a convolutional neural network approach //Computer Networks. – 2020. – Т. 178. – С. 107275.

ИНТЕРНЕТ ЗАТТАРЫ (IOT) ЖЕЛІСІНДЕГІ ҚАУІПСІЗДІК АУДИТІ

Жайлаухан Әсел Сардарбекқызы
asel.zhaylaukhan@mail.ru
Л.Н.Гумилев атындағы ЕҰУ Ақпараттық технологиялар факультетінің Ақпараттық қауіпсіздік кафедрасының 4 курс студенті, Астана, Қазақстан
Ғылыми жетекші – Сисенов Н.М., Жарасхан Н.Ж.

Интернет заттары (IoT) – бұл физикалық объектілердің, құрылғылардың, көлік құралдарының, ғимараттардың және басқа да нәрселердің интернет арқылы өзара байланыста болатын желісі. Бұл объектілер ұсынылатын деректерді жинақтап, талдап, және басқару функцияларын атқара алады. IoT технологиясының өсуімен, қауіпсіздік мәселелері де күн тәртібіне қойылуда. Осыған байланысты, IoT жүйелерінде қауіпсіздік аудиті өте маңызды рөл атқарады.

IoT құрылғыларының көптігі және олардың әртүрлілігі, сондай-ақ кең ауқымды қолданыстары қауіпсіздікке қойылатын талаптарды күрделендіреді. Қауіпсіздік аудиті арқылы ұйымдар бұл құрылғылар арқылы туындайтын мүмкін қауіптерді анықтап, оларды басқару стратегияларын жасай алады.

Қазақстан технология саласында жаһандық даму үрдістеріне белсенді түрде қосылып келеді. Интернет заттары желісі (IoT) сондай-ақ, өнеркәсіп, ауыл шаруашылығы, қалалық инфрақұрылым және тұтынушылық қызметтер сияқты көптеген салаларда қолданыс табуда.

Қазақстанның мұнай-газ секторы және тау-кен өндірісі IoT технологияларын белсенді қолдануда. Бұл арқылы олар өндірістік процестерді оптимизациялай алады, қауіпсіздік стандарттарын күшейтеді және тиімділікті арттырады.

Ауыл шаруашылық технологияларында IoT құрылғылары ауа райын бақылау, өсімдіктердің өсуін бақылау және жер қорын тиімді пайдалану сияқты маңызды ақпараттарды жеткізеді.

Алматы және Астана сияқты ірі қалалар қауіпсіздік және жол көлік инфрақұрылымын жақсарту үшін IoT шешімдерін қолдануда. Мысалы, бақылау камералары, жол белгілерінің автоматтандырылған жүйелері және ақылды жарықтандыру жүйелері.

Қазақстандағы көптеген үйлер мен кеңселерде ақылды үй жүйелері қолданылады, олар жылу, жарық және энергияны басқаруда тиімділікті арттырады.

Қазақстан IoT технологияларын дамытуға инвестиция салып, ұлттық инновациялық жоспарларда оған ерекше көңіл бөлінеді. Дегенмен, қауіпсіздік мәселелері – әлі де басым тақырып болып табылады. Қауіпсіздікті арттыру жолдарына қатысты заңнамалық базаны жетілдіру және технологиялық нормативтерді бекіту қажет.

Қазақстанда IoT технологияларының қолданысы кеңейіп келеді және бұл бағыттағы даму үрдістері жалғаса береді. Алайда, инфрақұрылымдық жаңартулар мен қауіпсіздік шараларын қолға алу арқылы бұл технологиялардың тиімділігін арттыруға және

қолданыстағы қауіптерді азайтуға болады. Қазақстандағы болашақтың IoT дамуы ұлттық инновациялық стратегияларға тікелей байланысты болмақ.

Қазақстандағы Интернет заттары желісінің (IoT) қауіптері бірнеше маңызды аспектілерді қамтиды. Бұл технологиялық өсу кезінде қауіпсіздік тәуекелдерін түсіну және шешу аса маңызды болып табылады. Мұнда IoT-ның Қазақстанда кездесетін негізгі қауіптерін қарастырамыз:

1. Физикалық шабуылдар. IoT құрылғылары көбінесе ашық ортада орналасқан, сондықтан олар физикалық шабуылдарға осал. Мысалы, ауыл шаруашылығы сенсорлары немесе қалалық мониторинг құрылғылары ұрлануы немесе бүлінуі мүмкін.

2. Әлсіз аутентификация. Көптеген IoT құрылғылары күшті аутентификация процедураларын қолданбайды, бұл оларды несие мәліметтерін жинайтын немесе жеке ақпаратты қорғайтын басқа құрылғыларға қарағанда айтарлықтай осал етеді. Бұл заңсыз кіруге жол ашады.

3. Желілік қауіпсіздік осалдықтары. IoT құрылғыларының желілік байланысы қауіпсіздік протоколдарының дұрыс орындалмауына байланысты осал болуы мүмкін. Бұл кибершабуылдаушыларға жүйеге кіріп, зиянды әрекеттер жасауға мүмкіндік береді.

4. Құпиялылықты бұзу. IoT құрылғыларының жинақтаған ақпаратының құпиялылығы бұзылуы мүмкін, өйткені көптеген құрылғылар жеткілікті деңгейде шифрланбайды. Бұл жеке және корпоративтік деректердің заңсыз пайдаланылуына алып келуі мүмкін.

5. Зиянды бағдарламалар және шпиондық, IoT құрылғылары зиянды бағдарламалардың немесе шпиондық құралдардың орналасуына осал. Олардың көпшілігінде зиянды кодты анықтау және жою мүмкіндіктері шектеулі, бұл киберқылмыскерлерге желілерге кіріп, деректерді бұрмалауға немесе жоюға мүмкіндік береді.

6. Жаңартулар мен патчтардың болмауы. Көптеген IoT құрылғылары жеткілікті жиілікпен жаңартылмайды, бұл оларды бағдарламалық қамтамасыз ету осалдықтарына ұшыратады. Өндірушілер жиі кездесетін немесе анықталған осалдықтарға түзетулер шығармайды.

Қазақстандағы IoT технологияларының дамуы бұл қауіптерге деген сақтық шараларын күшейтуді талап етеді, соның ішінде күшті аутентификацияны қолдану, желілік қауіпсіздікті арттыру және құрылғылардың үнемі жаңартылуын қамтамасыз ету арқылы болады.

Қазақстандағы Интернет заттары желісін (IoT) бағалау кезінде бірнеше маңызды аспектілерді қарастыру қажет. Бұл аспектілер әртүрлі секторлардағы IoT қолданымдарының кең ауқымын, инфрақұрылымдық дайындықты, технологиялық жетілдірулерді және қауіпсіздікке қатысты шараларды қамтиды.

Қазақстандағы интернет желісінің қолжетімділігі мен жылдамдығы соңғы жылдары айтарлықтай жақсарды, бұл IoT құрылғыларының тиімділігін арттырады. Қала орталықтарында және ірі аудандарда қолжетімді жоғары жылдамдықты интернет құрылғылар арасындағы байланыс қажеттіліктерін қанағаттандырады. Алайда, ауылдық аймақтарда интернет инфрақұрылымының дамымауы IoT шешімдерінің қолданылуына кедергі келтіруі мүмкін.

Өнеркәсіптік секторда, әсіресе мұнай-газ және тау-кен өнеркәсібінде, IoT технологияларының қолданылуы жоғары. Сенсорлар мен автоматтандырылған басқару жүйелері өндірісті басқаруда және тиімділікті арттыруда маңызды рөл атқарады. Бұл секторларда IoT шешімдерінің пайдаланылуы көлемі және тиімділігі жоғары деңгейде.

Ауыл шаруашылығы саласында IoT құрылғылары жер көлемін бақылау, суару жүйелерін басқару және өнімділікті арттыру үшін қолданылады. Бірақ, ауылдық аймақтардағы инфрақұрылымның шектеулілігі бұл технологиялардың толық көлемде қолданылуына кедергі жасайды.

Қауіпсіздік мәселелері IoT желісінің басты шектеулерінің бірі болып табылады. Қазақстанда киберқауіпсіздікке қатысты стандарттар мен заңнамалар жетілдіру қажет. IoT құрылғыларының көбісі жаңартылмайтын немесе қауіпсіздік осалдықтары бар бағдарламалық қамтамасыз етумен жұмыс істейді, бұл кибершабуылдар үшін осалдықтарды тудырады.

Қазақстандағы технологиялық даму және инновацияларды ынталандыру саясаты IoT секторын одан әрі дамытуға мүмкіндік береді. Мемлекеттік бағдарламалар мен қаржыландыру көмегімен жаңа технологияларды енгізу және тарату жеделдетілуі мүмкін.

Қазақстандағы IoT желісінің дамуы жоғары потенциалға ие, бірақ бірқатар шешімін таппаған мәселелер бар. Технологиялық инфрақұрылымды жетілдіру, қауіпсіздік стандарттарын күшейту және ауылдық аймақтарды қамту IoT саласындағы өсімнің негізгі драйверлері болып табылады.

Қазақстандағы Интернет заттары желісінің (IoT) қауіпсіздік саясатын жасау үшін төмендегідей маңызды аспектілерді қамтитын кешенді стратегия қажет. Бұл стратегия технологиялық осалдықтарды азайтуға, қауіпсіздік стандарттарын жақсартуға және инфрақұрылымды күшейтуге бағытталуы тиіс.

Заңнаманы қабылдау: IoT құрылғыларын өндіру, пайдалану және басқару үшін қатаң заңнамалық шеңбер құру қажет. Бұл заңнама құрылғылардың стандарттарын, деректерді жинау және сақтау тәсілдерін, сондай-ақ киберқауіпсіздік мәселелерін қамтуы тиіс.

Халықаралық стандарттарға сай келу: Еуропалық Одақтың GDPR сияқты халықаралық қауіпсіздік стандарттарына сәйкес келу арқылы деректерді қорғау мен жеке құпиялылықты сақтау.

Қауіпсіздік архитектурасын жасау: Барлық IoT құрылғылары мен платформалары үшін күшті, қабаттасқан қауіпсіздік архитектурасын әзірлеу. Бұл архитектура шифрлау, аутентификация, жүйелік қауіпсіздік және физикалық қауіпсіздікті қамтуы тиіс.

Желілік қауіпсіздікті күшейту: IoT желілері үшін күшті шифрлау және трафикті бақылау шешімдерін қолдану.

Тұрақты аудиттер: IoT инфрақұрылымдарының жүйелі аудиттерін жүргізу, олардың қауіпсіздігін бағалау және әлсіз жерлерін анықтау.

Тестілеу және сынақтар: Penetration testing (Pen-тестілеу) және басқа да қауіпсіздік тестілеулерін жүргізу арқылы осал жақтарды анықтау және түзету.

Хабардарлық пен оқыту бағдарламалары: Компаниялар мен жеке тұлғалар арасында IoT қауіпсіздігі туралы түсінікті арттыру үшін білім беру және хабардар ету бағдарламаларын іске асыру.

Техникалық дайындық: Техникалық мамандарды IoT қауіпсіздігі бойынша жоғары деңгейдегі оқыту курстарымен қамтамасыз ету.

Саясатты үнемі жаңарту: Технологиялық даму және жаңа қауіпсіздік тәуекелдеріне байланысты IoT қауіпсіздік саясатын үнемі жаңартып отыру.

Қазақстанда IoT қауіпсіздік саясатын осындай шаралар арқылы жүзеге асыру, елдің технологиялық инфрақұрылымын нығайтуға және халықаралық деңгейде бәсекеге қабілеттілігін арттыруға ықпал етеді.

Қазақстандағы Интернет заттары желісін (IoT) оқыту және хабардар ету бағдарламаларын іске асыру IoT технологияларының дұрыс және қауіпсіз пайдалануын қамтамасыз ету үшін маңызды.

Жоғары оқу орындарында IoT технологиялары бойынша курстар мен бағдарламаларды енгізу. Бұл курстар студенттерге теориялық білімді ғана емес, сонымен қатар практикалық дағдыларды меңгеруге көмектеседі.

Студенттерді жаңа IoT шешімдерін зерттеуге және жобалауға тарту, оларды инновациялық жұмыстарға бағыттау.

IoT технологияларын пайдаланатын кәсіпорындар үшін арнайы оқыту семинарларын ұйымдастыру. Бұл семинарлар қауіпсіздік тәуекелдерін түсіндіру және құрылғыларды қолдану бойынша тәжірибелік білімдер беруі тиіс.

Қызметкерлердің біліктілігін жетілдіру және жаңа технологияларды меңгеруге мүмкіндік беретін жалғасымды оқыту бағдарламаларын қамтамасыз ету.

IoT технологияларының маңыздылығы мен қолданылу аясын түсіндіру үшін ақпараттық науқандар өткізу. Бұл науқандар арқылы қауіпсіздік саясатының негізгі аспектілерін хабарлау және кеңірек көпшіліктің санасына сіңіру мақсатында болады.

БАҚ арқылы IoT-ның Қазақстандағы дамуы туралы және оның қоғамға әсері туралы мәлімет тарату.

Университеттер мен зерттеу орталықтарында IoT технологияларын зерттеуге арналған арнайы лабораторияларды құру. Мұндай орындар жаңа идеяларды сынап көруге және тәжірибе жинақтауға мүмкіндік береді.

Жаңа технологияларды көрсету және олардың практикалық пайдасын түсіндіру үшін арнайы орталықтар ашу.

Қазақстандағы IoT-ны оқыту және хабардар ету бағдарламалары технологиялық инновацияларды ынталандыруға және қоғамның қауіпсіздікке деген сезімталдығын арттыруға көмектеседі, бұл болашақта технологиялық өзгерістерге бейімділікті және тұрақтылықты қамтамасыз етеді.

IoT құрылғыларының кең таралуы мен олардың әртүрлі қолданылуы қауіпсіздік аудитінің маңызын арттырады. Қауіпсіздік аудиті арқылы ұйымдар өздерінің желілері мен құрылғыларындағы мүмкін қауіптерді азайта алады және оларды тиімді басқара алады. Бұл процесс барлық құрылғылар мен желілерді қауіпсіз, сенімді және тұрақты етіп сақтауға көмектеседі.

Пайдаланған әдебиеттер тізімі

1. «Introduction to the Internet of Things» - Cisco Networking Academy.
2. Rajkumar Buyya, Amir Vahid. Internet of Things: Principles and Paradigms. 2016. 378 p.
3. Shancang Li, Li Da Xu. Securing the Internet of Things. 2017. 154 p.
4. Bruce Sinclair. IoT Inc: How Your Company Can Use the Internet of Things to Win in the Outcome Economy. 2017. 304 p.

УДК 004.056.5

КРИМИНАЛИСТИЧЕСКИЕ МЕТОДЫ АНАЛИЗА РЕЕСТРА WINDOWS ДЛЯ РАССЛЕДОВАНИЯ ИНЦИДЕНТОВ, СВЯЗАННЫХ С УТЕЧКАМИ ДАННЫХ

Жакиева Асел Нартаевна
aselzakieva0@gmail.com,
студент III курса образовательной программы 6B06306 «Системы информационной безопасности», Евразийский национальный университет им. Л.Н. Гумилева
Алимбетова Аида Арманқызы
aidalimbetova18@gmail.com
студент III курса образовательной программы 6B06306 «Системы информационной безопасности», Евразийский национальный университет им. Л.Н. Гумилева
Научный руководитель Аймичева Гаухар Ислямовна

В современном мире, с увеличением числа цифровых технологий и расширением присутствия в интернете, обеспечение безопасности данных становится приоритетом не только для отдельных лиц, но и для организаций и компаний. Несмотря на принятие самых строгих мер безопасности, не исключены случаи утечек информации. Проведение тщательного расследования подобных инцидентов играет важную роль в выявлении причин и предотвращении подобных ситуаций в будущем.

Исследование, проведенное IBM и Ponemon Institute, показало (рис.1), что средняя стоимость утечки данных в мире в 2022 году составит 4,4 миллиона долларов США по сравнению с 4,2 миллиона долларов США в 2021 году и 3,9 миллиона долларов США в 2020 году [1]. Эта цифра является тревожным сигналом о серьезности последствий таких инцидентов и подчеркивает важность расследования каждого случая утечки данных. Каждая утечка данных не только влечет финансовые потери, но и подрывает доверие клиентов и репутацию организации. Таким образом, расследование утечек данных становится