ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

"Қ. И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті"
коммерциялық емес акционерлік қоғамы

М. Тынышбаев атындағы көлік инженериясы және логистика мектебі
«Логистика» білім беру бағдарламасының бағыты

Олжабаев Нұрсәт Саматұлы

Деректерді қорғау және көлік логистикасы саласындағы киберқауіпсіздікті қамтамасыз ету

ДИПЛОМДЫҚ ЖҰМЫС

6В11301 - Көлік қызметтері

Алматы 2025

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

"Қ. И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті"
коммерциялық емес акционерлік қоғамы

Көлік инженериясы және логистика мектебі

«Логистика» білім беру бағдарламасының бағыты

ҚОРҒАУҒА ЖІБЕРІЛДІ
«Логистика» білім беру
бағдарламасының
басшысының міндетін
атқарушы, т.ғ.к., доцент
Бектилевов А.Ю.
«05» 06 2025 ж.

ДИПЛОМДЫҚ ЖҰМЫС

Деректерді қорғау және көлік логистикасы саласындағы киберқауіпсіздікті қамтамасыз ету

6В11301 - Көлік қызметтері

Орындаған Олжабаев Н.С

Рецензент:
"Almaty Management University"
"Логистика" БЫҒ
PhD, қауымдастырылған профессор
Уалиева А. Б.
«05» мая 2025 ж.

Ғылыми жетекшісі:
Т.ғ.к., қауымдастырылған
профессор
Альтаева Ж.Ж
«04» 06 2025 ж.

Алматы 2025

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

"Қ. И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті"
коммерциялық емес акционерлік қоғамы

Көлік инженериясы және логистика мектебі

«Логистика» білім беру бағдарламасының бағыты

БЕКІТЕМІН
«Логистика» білім беру
Бағдарламасының
басшысының міндетін
атқарушы, т.ғ.к., доцент
Муханова Г.С.
«03» 02. 2025 ж.

ТАПСЫРМА
дипломдық жұмысты орындауға

Білім алушыға Олжабаев Нұрсәт Саматұлы
Тақырыбы: Деректерді қорғау және көлік логистикасы саласындағы киберқауіпсіздікті қамтамасыз ету
Басқарма мүшесі – академиялық мәселелер жөніндегі проректор Р. К. Ускенбаеваның 29.01.2025 ж. № 26-Ө / Ө бұйрығымен бекітілген
Аяқталған жобаны тапсыру мерзімі «30» мамыр 2025 ж.
Дипломдық жұмыстың алынған деректері: қосымшада Della.kz логистикалық платформасының деректері, Қазақстандағы кибершабуылдарға қатысты Kaspersky мен Positive Technologies мәліметтері, NurCrypt платформасына арналған аналитикалық шолулар және 2020–2024 жылдар аралығындағы кибершабуыл статистикасы біріктірілген.
Дипломдық жобада әзірлеуге жататын мәселелер тізімі:
а) Көлік логистикасында цифрландырумен бірге киберқауіптер артуда
б) Негізгі мақсат – қауіптерді азайтып, деректерді қорғау
в) Есептік бөлімде Della.kz жүйесінің осал тұстары мен шешім құны есептелді
г) NurCrypt секілді заманауи қорғаныс платформалары қарастырылды
д) Кибершабуылдардың нақты мысалдары мен салдары талданды
Графикалық материалдың тізімі: 3 кестеде және 6 кестеде көрсетілген.
Ұсынылатын негізгі әдебиеттер:

1 CISA (Cybersecurity and Infrastructure Security Agency). https://www.cisa.gov
2 Veracrypt программасы. https://veracrypt.io/ru/Home.html
3 Positive Technologies сарапшылары. https://ptsecurity.com/ru-ru/

дипломдық жұмысты дайындау

КЕСТЕСІ

Бөлімдер атауы, әзірленетін сұрақтар тізбесі	Ғылыми жетекшіге ұсыну мерзімдері	Ескертпе
Логистикадағы киберқауіпсіздік цифрлық трансформация мен киберқауіптер	11.03.2025	Орындалды
Della.kz платформасындағы киберқауіпсіздік кемшіліктері және оларды шешу жолдары	05.04.2025	Орындалды
Nurcrypt – логистикалық компаниялар үшін ақылды деректер қауіпсіздігі платформасы	17.04.2025	Орындалды

Аяқталған дипломдық жұмыс үшін, оған қатысты бөлімдердің жұмыстарын көрсетумен, кеңесшілер мен норма бақылаушының қойған **қолдары**

Бөлімдердің атауы	**Кеңесшілер, (аты-жөні, тегі, ғылыми дәрежесі, атағы)**	**Қол қойылған күні**	**Қол**
Нормобақылаушы	Болатқызы С., э.ғ.к., қауымдастырылған профессор	02.06.2025	

Ғылыми жетекшісі: _____ Ахметова Ж.Ж

Білім алушы тапсырманы орындауға алды _____ Олжабаев Н.С

Күні "25" 02 2025 ж

АҢДАТПА

«Деректерді қорғау және көлік логистикасы саласындағы киберқауіпсіздікті қамтамасыз ету». Логистиканы цифрландыру тиімділікті арттырғанымен, кибершабуылдарға деген қауіп-қатерді де көбейтеді. Бұл жұмыста жүйелердің осал тұстары, деректерді қорғау және киберқауіпсіздікті қамтамасыз ету шаралары талданады. NurCrypt сынды заманауи шешімдерге, қызметкерлерді оқытуға және нормативтік талаптарды сақтауға ерекше назар аударылады. Мақсаты – негізгі тәуекелдерді анықтап, логистикалық процестердің тұрақтылығын қамтамасыз ететін тиімді қорғаныс шараларын ұсыну.

АННОТАЦИЯ

«Защита данных и обеспечение кибербезопасности в сфере транспортной логистики». Цифровизация логистики повышает эффективность, но одновременно усиливает риски кибератак. Работа посвящена анализу уязвимостей логистических систем, защите персональных и коммерческих данных, а также мерам по обеспечению кибербезопасности. Рассматриваются современные подходы, такие как NurCrypt, а также важность обучения персонала и соблюдения нормативных требований. Цель – определить ключевые риски и предложить эффективные меры защиты для устойчивости логистических процессов.

ABSTRACT

«Data protection and cybersecurity in the field of transport logistics». While digitalization enhances the efficiency of logistics, it also increases the risk of cyberattacks. This paper analyzes system vulnerabilities, data protection, and cybersecurity measures. Special attention is given to modern solutions such as NurCrypt, employee training, and compliance with regulatory requirements. The main goal is to identify key risks and propose effective measures to ensure the resilience of logistics processes.

МАЗМҰНЫ

КІРІСПЕ

Өзектілігі – көлік логистика саласындағы деректерді қорғау мен киберқауіпсіздікті қамтамасыз ету қажеттілігі соңғы жылдары цифрландырудың өсуі, күрделі жеткізу тізбектерінің пайда болуы, кибершабуылдардың көбеюі, реттеу талаптарының күшеюі және бәсекелестік себепті айтарлықтай артты. Логистикада ақпараттық технологиялардың кеңінен қолданылуы мен процестерді автоматтандыру тиімділікті арттырса да, бұл кибершабуылдарға осалдықтар ашты. Күрделі тізбектер мен кибершабуылдар саланы қорғауды қажет етеді. Жаңа реттеу нормалары мен бәсекелестік жағдайында компаниялар киберқауіпсіздікке назар аудармауы клиенттерінің сенімін жоғалтуына әкелуі мүмкін. Сонымен қатар, жаңа технологиялар мен инновациялар киберқорғаудың жаңа тәсілдерін талап етеді.

Мақсаты – көлік логистикасы саласында деректерді қорғау және киберқауіпсіздікті қамтамасыз ету мақсаты: құпия ақпаратты қорғау, деректердің тұтастығын қолдау, кибершабуылдардың алдын алу, бизнес-процестердің үздіксіздігін қамтамасыз ету, реттеуші талаптарды сақтау, қызметкерлерді оқыту мен хабардар ету, серіктестермен ынтымақтастық орнату.

Бұл мақсаттар көлік логистикасының тиімді жұмысын қамтамасыз етуге, клиенттердің сенімін арттыруға және саладағы қауіптерді азайтуға ықпал етеді.

Тапсырмалар:

– Жеке ақпаратты қорғау.

– Клиенттер мен қызметкерлердің жеке деректерін қорғау.

– Компанияның ішкі құжаттары мен коммерциялық ақпаратының қауіпсіздігін қамтамасыз ету.

– Көлік жүйелерінің қауіпсіздігін қамтамасыз ету.

– Көлік басқару жүйелерін кибершабуылдардан қорғау.

– Жүкті бақылау жүйелерінің қауіпсіздігін қамтамасыз ету.

– Киберқатерлерді мониторингтеу.

– Аномалияларды анықтау жүйелерін енгізу.

– Инциденттерге жауап беру протоколдарын әзірлеу.

– Қызметкерлерді оқыту.

– Киберқауіпсіздік бойынша тренингтер өткізу.

– Қауіптер туралы хабардарлықты арттыру.

– Нормативтік талаптарды сақтау.

– Деректерді қорғау стандарттарына сәйкестікті қамтамасыз ету.

– Ішкі қауіпсіздік саясаттарын сақтау.

– Жеткізу тізбегін қорғау.

– Жеткізу тізбегіндегі тәуекелдер мен осалдықтарды бағалау.

– Серіктестермен киберқауіпсіздік бойынша ынтымақтастық.

– Инцидент-менеджмент.

– Киберқауіпсіздік инциденттеріне дайындық жоспарын әзірлеу.
– Инфрақұрылымды қорғау.
– Бағдарламалық қамтамасыз етуді жаңарту және патчтау.
– Деректерді шифрлеу.
– Заманауи технологияларды енгізу.
– Жасанды интеллект және машиналық оқыту негізіндегі шешімдер.
– Блокчейн технологиясын қолдану.

Бұл міндеттер көлік логистикасындағы киберқауіпсіздік стратегиясын тиімді түрде қалыптастыруға мүмкіндік береді, деректерді қорғауға және қауіптерді минимизациялауға ықпал етеді.

Зерттеу нысаны. Сайт Della.kz – Қазақстандағы жүк тасымалдау қызметтерін ұсынатын онлайн алаң. Бұл платформа жеке және заңды тұлғаларға жүк тасымалдаушыларды іздеуге, тасымалдау шарттарын келісуге және жүк жөнелтушілер мен тасымалдаушылар арасындағы байланысты жеңілдетуге мүмкіндік береді.

Негізгі мүмкіндіктері. Жүк іздеу және орналастыру: Пайдаланушылар өз жүктерін орналастырып, тасымалдаушылардан ұсыныстар ала алады. Тасымалдаушылардың ұсыныстары: Тасымалдаушылар өз қызметтерін ұсынады, ал жүк жөнелтушілер ең тиімді ұсынысты таңдай алады. Құжаттар мен лицензиялар: Барлық тасымалдаушылар міндетті тіркеуден өтіп, қажетті мемлекеттік құжаттарды ұсынады. Бағалар мен қашықтықтар: Сайтта тасымалдау бағалары мен қашықтықтар көрсетілген, бұл пайдаланушыларға шығындарды жоспарлауға көмектеседі.

Зерттеу пәні. Della.kz сияқты онлайн жүк тасымалдау платформалары – ақпараттық инфрақұрылымның бір бөлігі болып табылады. Олар тасымалдаушылар мен жүк жөнелтушілерді байланыстыратын цифрлық орта болғандықтан, белгілі бір деңгейде кибершабуылдарға осал болуы мүмкін.

1 ЛОГИСТИКАДАҒЫ КИБЕРҚАУІПСІЗДІК ЦИФРЛЫҚ ТРАНСФОРМАЦИЯ МЕН КИБЕРҚАУІПТЕР

1.1 Кибершабуылдар қаупі жоғары аймақтар

Логистикадағы киберқауіпсіздік цифрлық трансформация мен киберқауіптер жағдайында логистика секторының болашағын анықтауда өте маңызды. Бүгінгі таңда әртүрлі логистикалық процестер, соның ішінде материалдарды іздеу, сақтау, тасымалдау және тұтынушыларға жеткізу компьютерлік және интернет-басқаруға көшті. Бұл мақала логистикадағы киберқауіпсіздіктің маңыздылығын зерттейді, оның нені білдіретініне жарық түсіреді және тасымалдау кезінде деректерді қорғау стратегияларын ұсынады.

Логистикадағы киберқауіпсіздік: логистика өнім көзінен бастап соңғы тұтынушыға дейінгі барлық процестерді қамтиды. Киберқауіпсіздік осы логистикалық процестердің әр кезеңінде киберқауіптерден қорғауды қамтамасыз етуге бағытталған. Логистикадағы киберқауіпсіздік компаниялар үшін өз қызметін қолдау және тұтынушылар туралы ақпаратты қорғау үшін маңызды қажеттілік болып табылады.

Тасымалдау және деректерді қорғау стратегиялары: шифрлау Технологияларын қолдану: деректердің қауіпсіздігін қамтамасыз ету үшін Күшті шифрлау алгоритмдерін қолдану қажет. Тұтынушы туралы ақпарат, түгендеу деректері және басқа да құпия ақпарат шифрлау арқылы қорғалуы керек. Зиянды бағдарламалар мен шабуылдарды анықтау жүйелері. Логистикалық компаниялар зиянды бағдарламалар мен кибершабуылдарды анықтау және алдын алу үшін сенімді қауіпсіздік бағдарламалық жасақтамасы мен жүйелеріне инвестиция салуы керек. Бұл жүйелер ықтимал қауіптерді анықтауға және жедел араласуды қамтамасыз етуге көмектеседі. Оқыту және Хабардарлық: әлеуметтік инженерия тактикасы туралы хабардарлықты дамыту, күшті құпия сөздерді пайдалану және қауіпсіздік саясатын ұстану киберқауіптерден қорғауды құрудың маңызды құрамдас бөлігі болып табылады [1].

Касперскийдан болек компаниялар жадынамалар. Кибершабуылдар саны бойынша деректер Алматыда, Kaspersky cybersecurity Weekend халықаралық конференциясында айтылды. Іс-шарада компания сарапшылары бизнеске, өнеркәсіптік кәсіпорындарға және мемлекеттік ұйымдарға бағытталған ірі киберқауіптерді талқылады, сондай-ақ болашақта киберқауіпсіздік жағдайына әсер ететін үрдістерді болжады [11].

2023-те көлік саласы әлемдегі ең көп хакерлер шабуыл жасаған ондыққа кірді. Шабуылдардың негізгі әдістері:

2024 жылдың ақпан айының соңында ақпараттық қауіпсіздік бағдарламалық жасақтамасын әзірлеуге маманданған Positive Technologies көлік саласындағы киберқауіпсіздік жағдайын қарастыратын зерттеу шығарды. Есепте хакерлер 2023 жылы теміржол, авиация, теңіз және автомобиль көлігі операторларының ақпараттық технология жүйелерін бұзуға

тырысып, зиянды бағдарламаларды (жағдайлардың жалпы санының 35%), осалдықтарды пайдалануды (18%) және жеткізу тізбегіне шабуылдарды (8%) жиі қолданған.

Positive Technologies мәліметтері бойынша, көлік 2023 жылы кибер шабуылдарға жиі ұшырайтын 10 саланың қатарына кірді. Мұндай шабуылдардың салдары нарыққа қатысушы үшін өте ауыр болуы мүмкін, мысалы:

– Теміржол сегментінде – бұл жүк тасымалының бітелуі, сондай-ақ тасымалданатын жүктің (мысалы, мұнай мен көмір) зақымдануы немесе жойылуы болуы мүмкін.

– Авиацияда – қарапайым брондау жүйелері, багажды басқару жүйесінің істен шығуы және навигация құралдарының жұмысының бұзылуы.

– Теңіз тасымалы үшін – жанармай қоймаларын басқару процестеріне араласу, тиеуді басқару жүйелеріне шабуыл жасау, үлкен кеменің балласты басқару жүйесін басып алу, оның әсерінен ол құлап, батып кетуі мүмкін.

– Қалалық жол инфрақұрылымы мен автокөлік үшін-ақпараттық таблолардың, бағдаршамдардың, таксилерді брондау жүйелерінің және көлікті басқару жүйелеріне шабуылдың жұмысын бұзу.

Positive Technologies сарапшыларының бағалауы бойынша, 2023 жылы әлемдегі көлік компанияларына жасалған сәтті кибершабуылдардың саны 2022 жылмен салыстырғанда 36%-ға өсті. Ransomware вирустары қараңғы желіде жалға алу үшін ұсынылады [15].

Кибершабуылдың зияны 50 миллион долларға жетуі мүмкін. АҚШ және одан да көп. Бұл туралы 2021 жылдың 15 қыркүйегінде BCG хабарлады. ТиЛ секторындағы ықтимал кибершабуылдарды қамту артып, тәуекел сипаты барған сайын әртүрлі болғанымен, бұзу шығындары айтарлықтай төмендеді. Сонымен қатар, осалдықтардың негізгі көзі жүйелер емес, адамдар. ТиЛ салаларындағы киберқауіптерге қарсы тұру үшін үш бағыт бойынша белсенді шаралар қабылдау қажет: технологиялар, реттеу, сондай-ақ адамдар мен процестер. 2020 жылы акт бос жұмыс орындарының саны 4 миллионға жетті

Цифрландыру көлік және логистика саласындағы компаниялар арасында кең таралып, саладағы процестердің бүкіл циклін жетілдірді. Бұл кіріс арналарын кеңейтуге бағытталған бұрын-соңды болмаған тиімділікке ықпал етті [3].

Бұл оң жағы. Минус-цифрландыру компанияларында оларды кибершабуылдарға өте осал ететін бірқатар мәселелерді анықтады. Бұл теңіз, теміржол, автомобиль көлігі, логистика және сәлемдемелерді жеткізуді қоса алғанда, саланың әрбір секторына әсер етеді. Мұның салдары қымбатқа түседі, бұзылады және қаржылық жауапкершілікке әкелуі мүмкін, әсіресе клиенттер туралы құпия ақпараттың ағып кетуіне жол берілсе.

Көлік пен логистиканың осалдығының көптеген факторлары бар. Біріншіден, компанияларының цифрлық экожүйелерімен тікелей байланысты операциялық технологияларды, жаңа байланыс және сымсыз арналарды кеңінен қолдану компанияларды хакерлер үшін оңай нысанаға айналдырады.

Екіншіден, бұл Ақпараттық технология саласындағы ескірген реттеулер мен стандарттар, киберқауіпсіздік туралы хабардарлықтың жеткіліксіздігі және ең маңызды фактор – қорғауды қамтамасыз ете алатын білікті кадрлардың жетіспеушілігі.

Логистика секторындағы кибершабуылдар бұрын бірнеше жылда бір рет болатын. Енді олардың біреуі-екеуі ай сайын ұйымдастырылатын сияқты. Олардың кейбіреулері ауқымды. Мысалы, 2021 жылғы мамырдағы кибершабуыл АҚШ-тың шығыс жағалауының жартысына жуығы мұнай өнімдерін жеткізетін Colonial Pipeline компаниясының жұмысын шамамен бір аптаға тоқтатты. Компания қызметтің бұзылуына байланысты сатып алу мен жоғалту сомасы 50 миллион долларға немесе одан да көпке жетуі мүмкін деп мәлімдеді. Басқа кибершабуылдар, тіпті бірнеше рет зардап шеккен ірі көлік компанияларына бағытталған, баспасөздің назарын аз аударады, бірақ көбінесе электрондық пошта мен логистикалық жүйелерді ұйымдастыруды қамтиды.

Сонымен қатар, хакерлер транспорт және логистика индустриясын жаңарту және дамыту үшін өте маңызды желілерде сақталған деректерді ұрлауға тырысуда, өйткені олар тұтынушыларға тиімдірек және сапалы қызмет көрсетеді. Бұл желілер автоматтандырылған тапсырыстар, жүктерді бақылау және тіркелгі ақпаратына қол жеткізу сияқты цифрлық жақсартуларды енгізуге мүмкіндік береді. Клиент үшін мұндай артықшылықтар өте құнды болғанымен, олар қатаң киберқауіпсіздік хаттамаларының болмауына байланысты ең сенімсіз арналардың бірі болып табылатын онлайн платформалар, телефон қосымшалары және басқа мобильді құрылғылар арқылы жиналған үлкен көлемдегі құпия ақпаратты сақтауды талап етеді.

Транспорт және логистика секторындағы ықтимал кибершабуылдарды қамту артып, тәуекел сипаты барған сайын өзгеріп отырса да, бұзу шығындары айтарлықтай төмендеді.

Мәселенің өзектілігін ескере отырып, Boston conculting group саланың кибершабуылдарға осал болу себептерін зерттеді. Boston conculting group компаниялары осы тәуекелдердің әсерін азайту және олардан қорғаудың өміршең және сенімді әдістерін жасау үшін қолдана алатын бірқатар интеграцияланған шешімдерді әзірледі.

Транспорт және логистика компанияларының алдында тұрған қиындықтарға ең оңай тәсіл-олардың осалдық факторларын үш санатқа бөлу: технология, реттеу, адамдар мен процестер. Осы санаттардың әрқайсысын мұқият зерделеу қажет, бұл сала тұтастай алғанда жаңа қауіп-қатерлерге тап болады.

Транспорт және логистика саласының әр сегментінде кибершабуылдар бетінің кеңеюі айқын көрінеді. Мысалы, теңіз тасымалдаушылары арасында салыстырмалы түрде қарапайым апаттар туралы ескерту және қауіпсіздік жүйелері халықаралық теңіз ұйымының электрондық навигация бағдарламасы сияқты бұлтқа негізделген толыққанды жергілікті желілермен ауыстырылды. Бұл желілер хакерлер үшін тартымды мақсат болып табылады, өйткені олар кемелердің жағдайын, жүк деректерін, техникалық мәселелерді және

мұхиттық ортаға қатысты мәселелердің толық спектрін бақылау үшін борттық ақпаратты үнемі жинайды, біріктіреді және талдайды.

Операциялық жүйелерін серверлер, Компьютерлер және мобильді құрылғылар сияқты ішкі ат жабдықтарымен байланыстыратын және хакерлерге шабуыл жасаудың жаңа жолдарын ұсынатын бұл таратылатын желілер кейде кибершабуылдан қорғаудың маңыздылығын түсінбегендіктен одан да осал болады. жеткізушілер ретінде, сондықтан транспорт және логистика компаниялары. Кейбір жағдайларда, жеткізушілер қашықтан қол жеткізу, бақылау және ақаулықтарды жою үшін олардың жабдықтарына ықтимал осал басқару интерфейстерін енгізуді талап етеді. Сонымен қатар, компанияларының компьютерлік жабдықтары қатаң қауіпсіздік хаттамаларына сәйкес сирек жаңартылады.

Компаниядан жеке жеткізушілермен қарым-қатынастан басқа, транспорт және логистика өз жеткізушілерімен және дистрибьюторларымен тиімді және технологиялық серіктестіктер құратыны да алаңдатады, олар желілік байланыстарға көбірек тәуелді. Бұл серіктестердің киберқауіпсіздік хаттамалары әдетте бақыланбайды, бұл транспорт және логистика компанияларына олардың интеграцияланған экожүйелеріне байланысты тәуекелдің өсіп келе жатқандығы туралы ақпарат бермейді.

Көлік және логистика секторының коммерциялық және операциялық аспектілері көптеген аймақтарда реттелгенімен,киберқауіпсіздікке қатысты ережелер салыстырмалы түрде аз. Сектор қызметінің жаһандық сипатына қарамастан – немесе, мүмкін, осыған байланысты – реттеушілер қай жерде жұмыс істесе де, компаниялары сақтауы керек киберқауіпсіздік нормаларының кешеніне келісу немесе назар аудару қиынға соғады. Бұл кешен болмаған жағдайда, киберқауіпсіздікке инвестициялар ұйымдарға тәуекелдің жалпы әсерін азайту үшін оңтайландырылмаған.

Дегенмен, әлемдік сауда мен экономикалық тұрақтылық үшін транспорт және логистика саласына ауқымды кибершабуылдың ықтимал қауіптілігін мойындай отырып, реттеушілер неғұрлым белсенді позицияны ұстана бастайды және компаниялар желілерінің көбірек қорғалуын талап етеді. Ұсынылған немесе қазірдің өзінде қабылданған реттеу құралдарына ЕО-ның желілік және ақпараттық қауіпсіздік директивасы және жақында күшіне енетін

CLC/TS 50701 және EN 50126 теміржол көлігі стандарттары, сондай-ақ халықаралық теңіз ұйымы енгізген теңіз көлігі ережелері кіреді. Әр түрлі дәрежеде бұл реттеу шаралары компаниялардың маңызды деректері мен процестерін, әсіресе клиенттер туралы мәліметтер мен жүк тасымалы туралы ақпаратты қорғау үшін минималды нормаларды сақтауға бағытталған.

Адамдар мен процестер. Киберқауіптер үнемі дамып отырады, бірақ кейбір осал аймақтардың ортақ ерекшелігі – адамдар. Мысалы, фишингтік хатты тани алмайтын қызметкерлерді шабуылдың бастапқы кезеңінде хакерлер оңай қолдана алады. Шын мәнінде, шабуыл тізбегіндегі алғашқы қадам әдетте зардап шеккендердің әрекеттері болады деп айтуға болады,

өйткені деректердің бұзылуының жартысынан көбін қызметкерлердің ұйымдық процестері мен құзыреттеріндегі кемшіліктерді немесе олардың кибершабуылдар туралы білімдерінің жетіспеушілігін тікелей байқауға және анықтауға болады.

Киберқауіпсіздік мамандарының орасан зор және өсіп келе жатқан жаһандық кадр тапшылығы жағдайды нашарлатады. Isc2 ақпаратты қорғау жөніндегі салалық топтың мәліметтері бойынша 2020 жылы акт маманы ретінде төрт миллион лауазым бос болды. Жақсы дайындалған кибер мамандардың жетіспеушілігі ішінара киберқауіпсіздік саласындағы жоғары білімнің салыстырмалы түрде жас құбылыс екендігіне байланысты, тек он жылға жуық уақыт болды.

Біздің ақпаратымыз бойынша, бұл жетіспеушілік қарастырылып отырған салада, әсіресе Азия-Тынық мұхиты аймағында қатты сезіледі, өйткені киберқауіпсіздік біліктілігі бар түлектер мен осы салада жұмыс істейтін тәжірибелі мамандар әдетте тасымалдау мен логистиканы мансап құрудың таңдаулы саласы ретінде қарастырмайды.

Бұл ішінара қабылдау мәселесі. Лауазымға үміткерлердің көпшілігі транспорт және логистика компанияларын инновациялық жұмыс орындары ретінде қарастырмайды, мұнда технология мамандары роботтандыру және автоматтандыру, деректерді талдау, блокчейн, өзін-өзі басқаратын көліктер және т.б. сияқты салаларға ауыса алады. Киберқауіпсіздік жұмысын тартымды етудің орнына-жақсырақ жалақы мен әлеуметтік пакеттерді ұсыну және инновацияларды ынталандыру – көптеген транспорт және логистика компаниялары киберқауіпсіздікті қатаң бюджеттік шеңберге сәйкес келетін шығын бірлігі ретінде қарастырады.

Транспорт және логистика компаниялары киберқауіпсіздік бағдарламасын олардың жабдықтары мен IT және IT бағдарламаларындағы киберқауіпсіздік деңгейін бағалаудан бастауы керек. Әрі қарай, олар ең маңызды және осал қолданбалар мен желілерде қорғаныс шараларын қолдана алады. Кибершабуылдар қаупі жоғары аймақтарды анықтау және қорғаныс портфолиосын әзірлеу киберқауіптерді басқару және оларды сандық бағалау бағдарламасы сияқты модельдер мен құралдардың көмегімен жеңілдетілуі мүмкін. Компаниялар өздерінің осалдық факторларын тәуекелдік тәсіл негізінде бағалауы керек, Мұнда негізгі активтер үшін киберқауіптерді жүзеге асырудың ықтималдығы мен салдарына басымдық беріледі. Содан кейін жобаларды әрқайсысының шығындарды ескере отырып, тұрақтылықты арттыру және осылайша киберқауіпсіздікке инвестициялау бюджеттерін оңтайландыру қабілетіне қарай бағалауға болады.

Осы сақтық шараларын қабылдағаннан кейін, транспорт және логистика компаниялары нөлдік сенім архитектурасы сияқты киберқорғаныстың неғұрлым жан-жақты тұжырымдамаларын жүзеге асыруға назар аударуы керек. Бұл әдістеме желімен өзара әрекеттесуге тырысатын барлық құрылғылар, пайдаланушылар немесе қолданбалар ықтимал қауіп екенін білдіреді. Нөлдік сенім стратегиясын ұйым ішіндегі және одан тыс

байланыстар бақыланатын қатаң бақыланатын ортаны қамтамасыз ететін DMZ (демилитаризацияланған аймақ) технологиясын қолдана отырып, желілерді сегменттеу және бөлу арқылы жүзеге асыруға болады. Ақпаратқа немесе активтерге қол жеткізуді қамтамасыз етпес бұрын пайдаланушылардың, бағдарламалардың және соңғы құрылғылардың түпнұсқалығын тексеруді қоса алғанда, мүмкіндігінше ішкі процестерді қатаң бақылау үшін де сол қағиданы ұстану керек. Транспорт және логистика компаниялары өздерінің ішкі киберқауіпсіздік дағдыларын жетілдіру үшін үш әрекет жасай алады.

Біріншіден, корпоративтік мәдениетте назардан тыс қалудан киберқауіпсіздік мәселелеріне қауіп-қатерлермен күресудің шұғыл қажеттілігін мойындауға көшу керек. Әрбір бөлімшеде бүкіл ұйым бойынша киберқауіпсіздікті нығайту идеясы айқын және негізгі аспект болуы керек. Киберқауіпсіздік туралы хабардарлық деңгейін арттыратын жиі тренингтер тәуекелдерді білетін ұжымның қалыптасуына айтарлықтай ықпал етуі мүмкін. Құпия сөздерді қорғау және компания желілеріндегі күдікті әрекеттерге назар аудару сияқты хакерлерден қорғауды қамтамасыз ету үшін жеке қызметкерлер қабылдауы мүмкін шараларды атап өту керек.

Екіншіден, бұл кибер тәуекелдерді басқаруға көбірек көңіл бөлу университеттер мен жеке сектордан киберқауіпсіздік мамандарын тарту үшін пайдаланылуы керек. Ұйымның мақсаты киберқауіпсіздік саласында уақыт көшбасшысы болу екенін мәлімдеңіз. Компаниялар Киберқауіпсіздік бойынша ең жақсы мамандарды тарта алады, оларға киберқауіпсіздік бағдарламаларын нөлден бастап, соңғы технологияларды қолдана отырып және ескірген жүйелерді ауыстыра алатындықтарын айтадЕкіншіден, бұл кибер тәуекелдерді басқаруға көбірек көңіл бөлу университеттер мен жеке сектордан киберқауіпсіздік мамандарын тарту үшін пайдаланылуы керек. Ұйымның мақсаты киберқауіпсіздік саласында уақыт көшбасшысы болу екенін мәлімдеңіз. Компаниялар Киберқауіпсіздік бойынша ең жақсы мамандарды тарта алады, оларға киберқауіпсіздік бағдарламаларын нөлден бастап, соңғы технологияларды қолдана отырып және ескірген жүйелерді ауыстыра алатындықтарын айтады. Сондай-ақ, ұйымдар өз технологияларын сатуға ұмтылмайтын ашық жабдықты жеткізушілерден кеңес алу мүмкіндігін қарастыруы мүмкін.

Соңында, компанияның технологиялық қызметкерлерінің арасынан киберқауіпсіздік бастамаларына дайын және табысты үміткерлерге қажетті негізгі қабілеттерін көрсеткен адамдарды табу керек. Бұл қызметкерлердің біліктілігін арттыру және оларға өтемақы ұсыну, сондай-ақ талап етілетін дағдыларды меңгергені үшін лауазымға негізделген ынталандыру шаралСоңында, компанияның технологиялық қызметкерлерінің арасынан киберқауіпсіздік бастамаларына дайыне табысты үміткерлерг қажетті негізгі қабілеттерін көрсеткен адамдарды табу керек. Бұл қызметкерлердің біліктілігін арттыру және оларға өтемақы ұсыну, сондай-ақ талап етілетін дағдыларды меңгергені үшін лауазымға негізделген ынталандыру шаралары til

компанияларына киберқауіпсіздікте жетіспейтін жұмыс күшінің кем дегенде бір бөлігін тез толтыруға мүмкіндік беруі мүмкін.

Көптеген компаниялары киберқауіпсіздік тәуекелдерін азайту үшін қабылдануы керек шаралар өте ауыр болып көрінуі мүмкін. Ақпараттық технология желілері және олардың әлсіз жақтары туралы ашықтық пен хабардарлықты арттыруға арналған практикалық кеңестердің бірі киберақпараттық өңдеу орталығын құру болуы мүмкін. Бұл орталық киберқауіпсіздікке қатысты басқару, қызмет, аналитика, процестер мен технологияларды қадағалауға, ұйымдастыруға және қадағалауға, киберқауіпсіздіктерді анықтау және жою үшін процестің негізгі қатысушылары арасында деректер мен мәліметтерді таратуға мүмкіндік береді.

Сонымен қатар, кибер ақпараттарды өңдеу орталығы басқару мен ақпараттарды басқару және т.б. басқару жүйелерін біріктіру арқылы қызметті оңтайландырады. Орталықта ат және т.б. мамандардың тәжірибесі мен білімі біріктірілуі керек, бұл интернеттегі және ішкі жүйелердегі кез – келген стандартты емес әрекеттерді бақылауға мүмкіндік береді – немесе, ең бастысы, осы екі жүйенің бірігу нүктесінде-кибершабуыл туралы уақытында сигнал бере алады.

Тәуекелді тиімді басқару үшін транспорт және логистика компаниялары жоғары стандарттарға сәйкес келетін кибер тұрақтылық деңгейлерін құруы, серіктестік жеткізу тізбегін қорғау. Тәуекелді тиімді басқару үшін компаниялар жоғары стандарттарға сәйкес келетін кибер тұрақтылық деңгейлерін құруы, серіктестік жеткізу тізбегін қорғауы және қауіпсіздік құралдарын әзірлеу кезінде тәуекелге бағытталған тәсілді ұстануы керек. Компанияларға өз ұйымдарының дамуына және технологиядан реттеуге және процестерден қызметкерлерге дейінгі бірнеше өлшем

Көлік және логистика. Ірі бизнесті шартты теміржол операторы және шағын көлік компанияларын бөлу қажет. Ірі бизнестің проблемалары үшінші тарап ұйымдарымен деректер алмасатын көптеген интерфейстер мен арналарға қызмет көрсету қажеттілігінен туындайды. Бұл деректер тек қаржылық сипатта ғана емес, сонымен қатар желідегі қозғалыс пен трафиктің сипаттамаларына байланысты болуы мүмкін. Бұл интерфейстерге шабуылдар жасалады. Ішкі қауіпсіздік қызметтері қарқынды жұмыс істейді, периметрді қорғау және бақылау, үшінші тарап ұйымдарының қолданбалы ландшафттың "сезімтал" компоненттеріне қол жеткізуін бақылау құралдарын үнемі жаңартып отырады.

Кіші логистика – егер ол алдағы мәселеге толығымен дайын болмаса, онда соққы, оның мақсаты мен салдары қай жағынан келетінін түсіну қиын. Бөлшек сауда басшыларының ақпараты бойынша, кибер шабуылдаушылардың әртүрлі зиянды әрекеттерінен туындаған жеткізілімдердің айтарлықтай төмендеуінің өсуі диагноз қойылған. Әрекеттер өте алуан түрлі – қарапайым бопсалаудан бастап, клиенттер, жеткізілімдер және т. б. туралы деректерді ұстауға дейін.

Хакерлікті "монетизациялау" схемасы қандай жүзеге асырылатыны әлі анық емес, бірақ, әдетте, зиянкестер басқа адамдардың қаражатын, қызметтері мен тауарларын өндіру әдістерінде өте тапқыр.

Ақпараттық қауіпсіздік саласындағы кадрлардың тапшылығы әрдайым болған және тек күшейе түседі, өйткені жұмыс істейтін шешімдерді құруға қабілетті жаңа формациядағы мамандарға деген қажеттілік тез өсуде. Тек регламенттерді жаза алатындар үшін мұндай проблемалар тіске сәйкес келмейді.

Қолда бар кадрлық аштық пен кибершабуыл деңгейінің өсуі жақсы қорғалған қызметтердің (бұлттық платформалар мен шешімдер сияқты) және қорғаныс қызметтерінің өсуіне әкелуі мүмкін, олар да бұлтқа жақын тәсілмен қамтамасыз етілуі қисынды – CyberSec as a Service. Ат жүйелерін және бағдарламалық жасақтаманы әзірлеуге байланысты ат жобаларын іске асыру тәсілдерін қайта қарастыру қажет.

Классикалық DevOps – тен DevSecOps тәсіліне көшкен жөн, ол әзірлеушілер тобын қамтамасыз етеді және cybersec-тің барлық процестерге-дизайннан бастап әзірлеуге, тестілеуге және сүйемелдеуге дейінгі сараптаманы тиісті мөлшерде қолдайды. Қазір мұндай мамандар жергілікті нарықта бірлік.

Мәселенің көлемін және сіздің бизнесіңізге әсер етпегенін түсіну үшін бағдарламалық жасақтама жүйелері мен инфрақұрылымнан бастап бақылау мен қорғауға дейін кешенді ат аудитін жүргізіп, бірнеше пентесттерді (penetration tests) орындау қажет.

Дегенмен, техникалық мәселелер "іске асыруды"қажет ететін барлық үлкен экономиканың бір бөлігі ғана. Осалдықтардың негізгі көзі жүйелер емес, адамдар.

Әлеуметтік инжиниринг, ақпараттық қауіпсіздік ережелерін сақтаудың маңыздылығын түсіндіру, тұрақты тренингтер және т. б. бойынша іс-шаралар қажет. Ақпараттық технология жүйелері мен қызметтеріне "өнім тәсілдері" тілін қолдана отырып, cybersec қасиеттері мен сипаттамаларын сіздің ұйымыңыз қолданатын немесе дамытатын барлық қызметтер мен өнімдерге "ендіру" туралы қамқорлық қажет [4].

1.2 Киберқауіпсіздік мамандарының кадр тапшылығы

Ірі transnet логистикалық компаниясына хакерлер шабуыл жасады. 2021 жылдың шілде айының ортасында Transnet-те кибершабуылмен байланысты оқиға туралы ақпарат пайда болды, нәтижесінде Оңтүстік Африканың Кейптаун портындағы контейнерлік операциялар бұзылды. Сахараның оңтүстігіндегі Африкадағы ең көп жүретін кеме терминалы Дурбан да зардап шекті.

Transnet ресми сайты 2021 жылдың 22 шілдесінде қате туралы хабарлама жіберіп, жұмыс істемеді. Оңтүстік Африканың ірі порттарын, соның ішінде

Дурбан мен Кейптаунды, сондай-ақ минералдар мен басқа да тауарларды экспортқа тасымалдайтын үлкен теміржол желісін басқаратын Компания өзінің ақпараттық технология инфрақұрылымының бұзылғанын және олардың себебін анықтағанын ресми түрде растады.

Компания кибершабуылдың бұзылуына себеп болды ма, жоқ па деген түсініктеме беруден бас тартты, бірақ баспасөзбен сөйлесуге рұқсат етілмегендіктен олардың атын атамауды сұраған дереккөздер шабуыл 2021 жылдың 22 шілдесінде таңертең ерте болғанын хабарлады.

2021 жылдың шілде айының басында мемлекеттік компания бірнеше күндік тәртіпсіздіктер мен елдің кейбір аудандарындағы зорлық-зомбылықтан кейін порттары мен ұлттық жүк теміржол желісінде үлкен үзілістерге тап болды.

1-кесте – Соңғы бес жылдықта киберқауіпсіздік шабуылдары

Жыл	Шабуыл түрі	Шабуыл саны	Залал көлемі (млн $)	Негізгі салдары
2020	Ransomware (Блоктау)	3	12	Жеткізу тізбегінің бұзылуы, операция тоқтады
2021	Phishing (Алаяқ хаттар)	7	5	Қызметкерлер деректері ұрланды
2021	Data Breach (Дерек ұрлау)	2	18	Клиенттердің жеке деректері таралды
2022	DDoS (Серверге шабуыл)	4	3	Жүйе 48 сағатқа дейін істемей қалды
2023	Supply Chain Attack	1	25	Жеткізушілер арқылы ішкі жүйеге ену
2024	Zero-day Exploit	2	8	Қауіпсіздік жүйесінің әлсіз жері пайдаланылды
Ескерту – [5] дереккөздің негізінде автор құрастырған				

2021 жылдың шілде айының ортасында Transnet-те кибершабуылмен байланысты оқиға туралы ақпарат пайда болды, нәтижесінде Оңтүстік Африканың Кейптаун портындағы контейнерлік операциялар бұзылды. Сахараның оңтүстігіндегі Африкадағы ең көп жүретін кеме терминалы Дурбанда зардап шекті.

Ірі transnet логистикалық компаниясына хакерлер шабуыл жасады. Transnet ресми сайты 2021 жылдың 22 шілдесінде қате туралы хабарлама жіберіп, жұмыс істемеді. Оңтүстік Африканың ірі порттарын, соның ішінде Дурбан мен Кейптаунды, сондай-ақ минералдар мен басқа да тауарларды экспортқа тасымалдайтын үлкен теміржол желісін басқаратын Компания

өзінің ақпараттық технология инфрақұрылымының бұзылғанын және олардың себебін анықтағанын ресми түрде растады.

Компания кибершабуылдың бұзылуына себеп болды ма, жоқ па деген түсініктеме беруден бас тартты, бірақ баспасөзбен сөйлесуге рұқсат етілмегендіктен олардың атын атамауды сұраған дереккөздер шабуыл 2021 жылдың 22 шілдесінде таңертең ерте болғанын хабарлады.

2021 жылдың шілде айының басында мемлекеттік компания бірнеше күндік тәртіпсіздіктер мен елдің кейбір аудандарындағы зорлық-зомбылықтан кейін порттары мен ұлттық жүк теміржол желісінде үлкен үзілістерге тап болды.

Жобаларды басқару жүйелері: нарық ерекшеліктері, негізгі технотрендтер.

Транснеттегі кибершабуыл тәртіпсіздіктермен байланысты ма деген сұраққа жауап ретінде Үкімет өкілі мынаны айтты:

Біз тергеу жүргізіп жатырмыз және ол расталған немесе жоққа шығарылған кезде біз тиісті мәлімдеме жасаймыз. Қазіргі уақытта біз мұны тәртіпсіздіктермен байланысты емес оқиға ретінде қарастырамыз.

Соңғы сәтсіздік автокөлік бөлшектері бар контейнерлерді кешіктірді, бірақ тауарлар порттың басқа бөлігінде болғандықтан зардап шеккен жоқ.

Transnet өзінің контейнерлік терминалдарының жұмысы бұзылғанын айтты, бірақ сонымен бірге компания айналысатын басқа тасымалдау жолдары зардап шекпегенін атап өтті: жүк теміржол, құбырлар.

Glencore және Barrick Gold сияқты тау-кен компаниялары жұмыс істейтін Конго Демократиялық Республикасы мен Замбияда өндірілген мыс пен кобальттың көп бөлігі Африкадан жүктерді жөнелту үшін Дурбанды пайдаланады.

Киберқауіпсіздіктің күшті шаралары үшін императив біздің барған сайын цифрлық әлемде бұрын-соңды айқын болған емес. Ұйымдар дамып келе жатқан киберқауіптермен ландшафтты шарлайтындықтан, киберқауіпсіздіктің сенімді шаралары барған сайын сыни сипатқа ие бола түсуде.

40 нақты кейс-зерттеулердің бұл антологиясы жетекші жаһандық ұйымдардың өздерінің виртуалды активтері мен сезімтал деректерін қорғау үшін қабылдайтын сан алуан тәсілдерін көрсетеді.

Әрбір жағдай киберқауіпсіздік үшін жүргізіліп жатқан шайқас туралы баға жетпес мағлұматтар бере отырып, кибершабуылдардың ренішсіз тиынына қарсы цифрлық жүйелерді нығайту үшін қолданылатын күрделі стратегиялар мен проактивті шараларды егжей-тегжейлі қарауды ұсынады [5].

Киберқауіпсіздіктің күшті тәжірибесінің маңыздылығы біздің цифрлық технологияларға деген қазіргі сенімімізді көрсетеді. Компаниялар жеке және сыни жедел деректердің үлкен көлемін сақтайды, олар ымырасыз қорғалуы тиіс.

Бұған жауап ретінде кәсіпорындар киберқауіптерді болжау және алдын алу үшін озық технологиялар мен стратегиялық негіздерді пайдаланады. Бұл ұйымдар қауіптерді анықтаудың проактивті жүйелері, тәуекелдерді

басқарудың кешенді хаттамалары, сондай-ақ қауіпсіздік технологияларын үнемі жаңартып отыру арқылы әлеуетті осал тұстарды болдырмауға бағытталған.

Бұл жинақта PayPal, «Шеврон» және «IBM» сияқты салалық алпауыттардың киберқауіпсіздік саласындағы сын-тегеуріндерге берген жауаптарын егжей-тегжейлі баяндайтын егжей-тегжейлі баяндаулары ұсынылған. Мысалы, PayPal компаниясы қаржылық транзакцияларды қорғау мақсатында жасанды интеллект негізіндегі алаяқтықты анықтау жүйесін енгізіп, клиенттердің жеке деректерін шифрлау мен қауіпсіздіктің көпдеңгейлі әдістерін қолдану арқылы қауіпсіздік деңгейін едәуір арттырды.

Шеврон энергетика секторының маңызды инфрақұрылымдарын кибершабуылдардан сақтау үшін өнеркәсіптік басқару жүйелерін (ICS) қорғауға бағытталған арнайы киберқауіпсіздік бағдарламаларын іске қосты. Компания сондай-ақ қызметкерлер арасында ақпараттық қауіпсіздік мәдениетін қалыптастыру үшін тұрақты оқыту курстарын ұйымдастырды.

IBM болса, киберқауіпсіздік саласында жаһандық көшбасшылардың бірі ретінде, кибершабуылдарды модельдеуге және оған қарсы әрекет етуге арналған «X-Force Command Center» сияқты орталықтарды құрып, өз клиенттеріне кең ауқымды шешімдер ұсынып келеді. Сонымен қатар, IBM кванттық есептеулер дәуіріне бейімделіп, болашақ қауіп-қатерлерге қарсы тұра алатын криптографиялық алгоритмдерді зерттеуде.

Бұл баяндаулар әртүрлі секторлардағы ірі компаниялардың киберқауіпсіздікке қалай басымдық беретінін, жаһандық қауіптерге қалай ден қоятындығын және үздік тәжірибелер арқылы өз инфрақұрылымдарын қалай қорғайтынын көрсетуге бағытталған.

Кейс-зерттеулер киберқауіпсіздік стратегияларының практикалық қолданылуын және олардың бизнестің тұрақтылығы мен қауіпсіздігіне әсерін жарықтандырады, шифрлауды күрделі жөндеу және қауіп-қатерді барлаудың күрделі платформалары сияқты бастамаларды көрсетеді. Осы жағдайларды зерттей отырып, оқырмандар қазіргі заманғы цифрлық аренада киберқауіпсіздіктің маңызды рөлін нақты түсінетін болады және компаниялар өздерінің цифрлық шептерін қамтамасыз ету үшін маңызды шараларды қабылдауы тиіс.

2 DELLA.KZ ПЛАТФОРМАСЫНДАҒЫ КИБЕРҚАУІПСІЗДІК КЕМШІЛІКТЕРІ ЖӘНЕ ОЛАРДЫ ШЕШУ ЖОЛДАРЫ

2.1 Киберқауіпсіздік жүк тасымалы мен жеткізу тізбегі

Цифрлық технологиялардың қарқынды дамуы мен логистика саласының онлайн платформаларға көшуі жаңа қауіптер мен сын-тегеуріндерге жол ашты. Қазақстандағы танымал логистикалық порталдардың бірі – Della.kz, тасымалдаушылар мен жүк берушілерді байланыстыратын тиімді алаң болып табылады. Алайда, бұл платформадағы киберқауіпсіздік деңгейі кейбір аспектілерде осалдық танытады. Бұл дипломдық жұмыста Della.kz сайтындағы қауіпсіздік мәселелері талданып, оларды шешу жолдары ұсынылады.

Della.kz – көлік логистикасына арналған онлайн платформа, онда жүк тасымалы туралы хабарландырулар орналастырылады, тасымалдаушылар мен клиенттер байланыс орнатады. Платформада деректердің үлкен көлемі сақталады: байланыс нөмірлері, бағыттар, құжаттар, жеке аккаунттар, келісімдер және тағы басқа [2].

2-кесте – Della.kz кемшіліктері

№	Сипаттамасы	Қауіп түрі
1	Кейбір ішкі беттер https арқылы емес, бұл деректердің үшінші тарапқа берілу қаупін арттырады.	SSL сертификатының болмауы
2	Қолданушы аккаунттарын бұзу оңайырақ болады.	Екі факторлы аутентификация жоқ
3	Іздеу немесе форма өрістері енгізілген деректерді дұрыс тексермейді.	SQL Injection қаупі
4	Аккаунт деректері ашық түрде базаға сақталуы мүмкін.	Пайдаланушы деректерінің шифрланбауы
5	Жүктемені реттейтін жүйе жеткіліксіз.	DDoS шабуылына қарсы әлсіз қорғаныс
Ескерту – [2] дереккөздің негізінде автор құрастырған		

Салдарлары:

– Пайдаланушы деректерінің ұрлануы және алаяқтық фактілерінің көбеюі.

– Бизнес серіктестердің сенімсіздігі және репутациялық шығын.

– Қызметтің уақытша тоқтауы – шығын және бәсекелестерге жол беру.

– ҚР заңнамасын бұзу – ақпараттық қауіпсіздік заңдарына сәйкес жауапкершілікке тартылу.

3-кесте – Della.kz сайтына керек инвестициялар

Қадам	Шешім	Құн (шамамен)	Күтілетін нәтиже
1	HTTPS/SSL толық енгізу	50 000 ₸	Барлық беттердің қауіпсіздігі артады
2	Екі факторлы аутентификация (2FA)	100 000 ₸	Аккаунт қауіпсіздігі айтарлықтай жақсарады
3	SQL Injection сканерін қосу	70 000 ₸	Веб-қосымша қауіпсіздігі нығаяды
4	Шифрлау (AES-256) деректер базасына	120 000 ₸	Деректердің сыртқа шығуына тосқауыл
5	Cloudflare арқылы DDoS-тан қорғау енгізу	200 000 ₸	Жүйе жүктемесіне тұрақтылық
Ескерту – [5] дереккөздің негізінде автор құрастырған			

Della.kz платформасы – логистикалық саланың цифрлы дамуына елеулі үлес қосып жатқан жоба. Алайда, оның киберқауіпсіздігі заманауи талаптарға толық жауап бермейді. Жоғарыда көрсетілген осалдықтар нақты қауіп төндіреді және оларды жою үшін салыстырмалы түрде қарапайым техникалық шешімдер жеткілікті. Инвестиция көлемі айтарлықтай көп емес, бірақ қорғалмаған жүйеден келетін шығынмен салыстырғанда өте тиімді.

Киберқауіпсіздік ұйымдар мен логистикалық жүйелер үшін маңызды рөл атқарады. Cisco желілік трафиктегі аномалияларды анықтау үшін машиналық оқытуға негізделген болжамдық талдау жүйесін енгізіп, киберқауіптерге алдын ала жауап беру мүмкіндігін арттырды. Бұл шешім қауіпсіздікті жақсартып, операциялық тиімділікті көтерді. Microsoft шифрлау мен көп факторлы аутентификацияны қолдану арқылы деректерді қорғауды күшейтті, соның нәтижесінде ақпараттың бұзылу қаупі азайды және пайдаланушылардың сенімі артты. IBM Zero Trust архитектурасын енгізу арқылы желіге кіруді қатаң бақылауға алды. Бұл тәсіл қашықтан жұмыс істеу жағдайында осал тұстардан қорғануға мүмкіндік беріп, деректердің бұзылу ықтималдығын төмендетті. Palo Alto Networks жасанды интеллект пен машиналық оқытуға негізделген қауіпсіздік жүйесін енгізіп, күрделі шабуылдарды автоматты түрде анықтап, әрекет ету уақытын қысқартты. Google пайдаланушыларды нақты уақытта фишингтен қорғау үшін оқыту жүйесін іске қосты. Бұл пайдаланушылардың қауіп туралы хабардарлығын арттырып, фишинг шабуылдарының тиімділігін азайтты.

Киберқауіпсіздік жүк тасымалы мен жеткізу тізбегін де қорғайды. Контейнерлерді басқару жүйелеріне бағытталған шабуылдарда киберқауіпсіздік жүйелері осал тұстарды уақтылы анықтап, операциялардың

бұзылуына жол бермеді. Қауіпсіз бақылау жүйелері ұрлық пен алаяқтықты азайтып, күдікті әрекеттерді дереу тіркеуге мүмкіндік берді. Фишингке қарсы дайындық пен қызметкерлерді оқыту жалған төлемдер мен деректердің таралуының алдын алуға көмектесті. Көлік компаниялары шабуылдар кезінде сақтық көшірме мен әрекет ету жоспарлары арқылы шығындарды азайтты. Кеме компанияларында да алдын алу шаралары қауіптерді дер кезінде анықтап, навигацияға араласу қаупін жойды.

Maersk компаниясы 2017 жылы NotPetya вирусының жойқын шабуылына ұшырады. Барлық жүйелер істен шықты, бірақ Африкадағы филиалдағы сақтық көшірме арқылы компания жұмысын қалпына келтіре алды. Бұл оқиға деректердің физикалық көшірмесінің және желіні оқшаулаудың маңызын көрсетті. Кеме қатынасындағы EDI жүйесіне шабуыл жасау әрекеті де тіркелді, онда маршруттар мен құжаттар бұрмалануға ұшырады. Бірақ электрондық қолтаңбалар, блокчейн негізіндегі есеп жүйелері мен SIEM арқылы бұл шабуыл дер кезінде тоқтатылып, жүктің қауіпсіздігі қамтамасыз етілді. Бұл оқиғалар киберқауіпсіздіктің тек IT жүйелер үшін емес, бүкіл бизнес тұрақтылығы үшін шешуші мәнге ие екенін дәлелдейді.

Ресейдегі кибершабуылдардың негізгі бағыты негізінен электрондық коммерцияға байланысты бөлшек саудаға, банк секторына және логистикаға бағытталған

«Касперский зертханасының» мамандары, егер 2022 жылдың бірінші тоқсанын 2023 жылдың ұқсас кезеңімен салыстырсақ, Қазақстандағы фишингтік шабуылдар санының жалпы өсімін 12%-ға атап өтті. Бұл ретте корпоративтік сектордағы фишингтік шабуылдар саны 120%-ға өсті. Компанияның есептеулері бойынша Қазақстан кибершабуылдар саны бойынша әлемде жетінші орында тұр.

Егер 2022 жылдың бірінші тоқсанын 2023 жылдың ұқсас кезеңімен салыстыратын болсақ, пайдаланушының іс-әрекетін бақылай алатын, оның желідегі мінез-құлқының статистикасын жинай алатын, дербес деректерді ғана емес, Қазақстанда 20%-ға жуық өсті.

Компания сарапшылары сонымен қатар 2022 жылдың сәйкес кезеңімен салыстырғанда 2023 жылдың бірінші тоқсанында трояндық банктік шабуылдардың қарқынды өскенін атап өтті. Қазақстанда шабуылға ұшыраған пайдаланушылар саны 92%-ға өсті.

Сарапшылардың болжауынша, 2023 жылы әлемде бұлтты есептеулердің қауіпсіздігін бұзу қаупі артады. Интернет заттарының (IoT) құрылғыларын қорғауды қамтамасыз ету туралы алаңдаушылық артып келеді-оларды ұйымдардың ішкі желілеріне бастапқы қол жеткізу және деректерді одан әрі бұзу үшін пайдалануға болады. Жасанды интеллект көмегімен кибершабуылдардың көбеюін де күтуге болады. Кибершабуылдар осалдықтарды анықтау және күрделі шабуылдар жасау үшін машиналық оқыту алгоритмдерін және басқа AI технологияларын қолдануға тырысады. It шешімдерінің жеткізу тізбегіне шабуылдар жиі орын алуда және бұл үрдіс 2023 жылы да жалғасады деп күтілуде. Зиянкестер клиенттердің желілері мен

деректеріне қол жеткізу үшін үшінші тарап сатушылары мен жеткізушілеріне шабуыл жасайды.

2.2 Бағдарламалық жасақтаманы жаңарту және әдістері

Жаһандық статистика деңгейінде жүктерді ұрлау көбінесе келесі аймақтарда орын алады:

Солтүстік Америка: әсіресе АҚШ-та жүк тасымалы жоғары және көптеген ірі компаниялары бар. Ұрлық автотұрақтарда, терминалдарда және қоймаларда болуы мүмкін.

Еуропа: Ұлыбритания, Германия және Нидерланды сияқты кейбір елдер, әсіресе ірі порт және көлік тораптарында жүк ұрлау мәселесіне тап болады.

Латын Америкасы: Бразилия мен Мексика сияқты елдерде белгілі бір аймақтарда қылмыстың жоғары деңгейіне байланысты жүк пен көлік ұрлығы жиі кездеседі [6].

Азия: кейбір аймақтарда, мысалы, Үндістанда және Оңтүстік-Шығыс Азия елдерінде, әсіресе нашар бақыланатын аймақтарда жүктерді ұрлау жағдайлары байқалады.

Бұл деректер қауіпсіздік деңгейі, экономикалық жағдай, инфрақұрылым және құқық қорғау органдарының болуы сияқты көптеген факторларға байланысты.

Көліктік логистика саласындағы деректерді қорғау және киберқауіпсіздік логистикалық жүйелердің тиімді және қауіпсіз жұмыс істеуінде маңызды рөл атқарады. Сауданың жаһандануын және технологияға тәуелділіктің артуын ескере отырып, компаниялар деректерді қорғау және киберқауіптердің алдын алу шараларына ерекше назар аударуы керек. 1. Деректерді қорғау:

1 Шифрлау: көлік құралдары, қойма кешендері және Орталық басқару жүйелері арасында берілетін деректер рұқсатсыз кіруді болдырмау үшін шифрлануы керек.

Қол жеткізуді басқару: көп деңгейлі аутентификацияны енгізу және ақпаратқа тек өз міндеттерін орындау үшін қажет қызметкерлерге қол жеткізуді шектеу қажет.

Құпиялылық саясатын әзірлеу: тұтынушылардың деректерін өңдеу мен қорғаудың тиімді саясаты заңнаманы сақтау (мысалы, GDPR) және тұтынушылардың сенімін арттыру үшін қажет.

2 Киберқауіпсіздік қызметкерлерді оқыту. Қызметкерлерге кибершабуыл белгілері туралы білуі және оларға қалай дұрыс жауап беру керектігін білуі үшін жүйелі түрде тренингтер өткізу.

Қауіп-қатерді бақылау және анықтау. Желіні күдікті әрекеттерге үнемі қадағалап отыру және ықтимал қауіптерге тез жауап беру маңызды.

Бағдарламалық жасақтаманы жаңарту: жүйелер мен қосымшаларды үнемі жаңартып отыру осалдықтарды жоюға және шабуылдардың жаңа түрлерінен қорғауға көмектеседі.

3 Деректердің сақтық көшірмесін жасау және қалпына келтіру. Сақтық көшірме жасау: деректердің сақтық көшірмесін үнемі жасау жүйенің шабуылы немесе істен шығуы кезінде ақпаратты қалпына келтіруге көмектеседі.

Қалпына келтіру жоспары: деректер мен маңызды жүйелерді қалпына келтірудің нақты жоспарын жасау бос уақыт пен ысырапты азайтуға көмектеседі.

4 Инновациялық технологиялар. IoT және көлікті басқару: Көлік құралдарында IoT құрылғыларын пайдалану киберқауіпсіздікке ерекше назар аударуды қажет етеді, өйткені олар шабуылдарға осал болуы мүмкін. Барлық қосылған құрылғылар мен жүйелерді қорғау қажет.

Блокчейн технологиясы: блокчейнді қолдану логистикадағы транзакциялардың ашықтығы мен қауіпсіздігін арттырып, деректерді бұрмалау қаупін азайтады

Компаниялар қолданатын список детали

SIEM-жүйелер (Security Information and Event Management):

Мысалдар: Splunk, IBM QRadar, ArcSight. Бұл жүйелер қауіпсіздік оқиғаларын жинауға, талдауға және оларға жауап беруге көмектеседі.

Зиянды бағдарламалардан қорғау жүйелері:

Мысалдар: McAfee, CrowdStrike, Trend Micro. Бұл шешімдер вирустардан және басқа зиянды бағдарламалардан қорғауды қамтамасыз етеді.

Брандмауэрлер және кірудің алдын алу жүйелері (IPS):

Мысалдар: Cisco ASA, Palo Alto Networks, Fortinet. Олар желілік трафикті басқарады және жүйелерге рұқсатсыз кірудің алдын алуға көмектеседі.

Деректерді шифрлау:

VeraCrypt немесе файлдық жүйе деңгейіндегі шифрлау қолданбалары сияқты маңызды ақпаратты шифрлау бағдарламалары.

Қол жеткізуді басқару және аутентификация:

Көп факторлы аутентификацияны (MFA) және кіруді басқару жүйелерін (мысалы, Okta, Microsoft Azure AD) пайдалану.

Қызметкерлерді оқыту:

Киберқауіптер мен жалпы киберқауіпсіздікке қатысты қызметкерлердің хабардарлығын арттыру бағдарламаларын іске асыру.

Осалдықтарды бағалау және ену сынағы:

Осалдықтарды үнемі бағалау үшін Nessus немесе Qualys сияқты құралдарды пайдалану.

Оқиғаларға жауап беру жоспарлары: инциденттерге жауап беру жоспарларын әзірлеу және тестілеу.

Дұрыс шешімді таңдау үшін тәуекелдерді талдау, қолданыстағы инфрақұрылым мен бизнес қажеттіліктерін бағалау маңызды.

Технологияларды, процестерді және оқытуды біріктіретін кешенді тәсіл логистикада киберқауіпсіздікті қамтамасыз етуде ең тиімді болып табылады.

4-кесте – Шифрлардың еңгізілген түрлері

№	Логистикалық ұйым	Қолданылатын шифрлау әдісі	Шифрланған деректер түрі	Шифрлау дәрежесі	Енгізілген жыл
1	KAZLogistics	AES-256	Клиенттік деректер, төлем ақпараты	Жоғары	2020
2	TranZam Express	RSA-2048	API байланыс, ішкі құжаттар	Орташа	2019
3	RailTrans	TLS 1.3	Жеткізу кестелері, навигация	Жоғары	2021
4	KZ Freight Co.	Proprietary Encryption	Сервер журналдары	Төмен	2018
5	Qazaq Trans Group	AES-128	Электронды хат алмасу	Орташа	2022
Ескерту – [10] дереккөздің негізінде автор құрастырған					

Ransomware – бұл пайдаланушының файлдарын шифрлап немесе жүйеге кіруге тосқауыл қойып, оны қалпына келтіру үшін төлем талап ететін зиянды бағдарлама. Әдетте, жұқтыру электрондық поштадағы зиянды тіркемелер, зиянды сайттар немесе жүйедегі осалдықтар арқылы жүреді. Бағдарлама іске қосылған соң маңызды файлдарды шифрлап, пайдаланушыдан криптовалютада төлем жасауды сұрайды. WannaCry, REvil және LockBit секілді белгілі мысалдар бар. Ransomware-ден қорғану үшін тұрақты резервтік көшірме жасау, бағдарламаларды жаңарту, антивирустар мен фаерволдарды пайдалану және желіні сегменттеу қажет [7].

Фишинг – бұл әлеуметтік инженерия әдісі, мұнда шабуылдаушылар пайдаланушыны алдап, құпия ақпаратты – логин, құпиясөз, банк деректері және т.б. алуға тырысады. Көп жағдайда шабуыл электрондық пошта, веб-сайт немесе хабарлама арқылы жүзеге асады, олар нақты ұйым немесе қызмет түрін (банк, пошта, мемлекеттік орган) еліктейді. Фишингтің түрлері: жалпы фишинг, нақты мақсаттағы spear phishing, басшыларға бағытталған whaling, телефон арқылы – vishing және SMS арқылы – smishing. Қорғану шараларына пайдаланушыларды оқыту, фишингке қарсы сүзгілер орнату, екі факторлы аутентификация және сілтемелерді мұқият тексеру жатады.

DDoS шабуылдары сайтты, серверді немесе қызметті бір мезетте көптеген сұраныспен толтырып, оны қолжетімсіз етуге бағытталған. Мұндай шабуылдарға шабуылдаушы ботнет деп аталатын, зиянды кодпен жұқтырылған құрылғылар желісін пайдаланады. Нәтижесінде сервер артық жүктемеге шыдамай жұмысын тоқтатады. Атака деңгейлері әртүрлі болуы

мүмкін: желілік (трафик арнасына жүктеме), транспорттық (TCP/UDP хаттамаларына шабуыл) және қолданбалы деңгей (нақты қолданушы әрекетін имитациялау). Қорғану тәсілдері: желілік сүзгілер, жүктемені теңгеру, бұлтты DDoS-қорғаныс жүйелері және трафикті тұрақты бақылау.

IoT құрылғыларына ену – бұл интернетке қосылған ақылды құрылғылар (мысалы, камералар, динамиктер, сенсорлар) арқылы жүзеге асатын қауіп. Мұндай құрылғылар жиі жаңартылмайды, әлсіз стандартты құпиясөздермен жабдықталады және кейде шифрлаусыз жұмыс істейді. Зиянкестер мұндай құрылғыларды желіге ену немесе ботнеттің бөлігі ретінде пайдалана алады. Мысалы, Mirai ботнеті жүздеген мың IoT құрылғысын жұқтырып, ауқымды шабуылдар ұйымдастырды. Қорғану үшін құрылғының стандартты құпиясөзін өзгерту, микробағдарламаларды жаңарту, IoT құрылғыларын негізгі желіден бөліп шығару және құрылғылар белсенділігін бақылау қажет.

Деректердің ағып кетуі – бұл құпия ақпараттың рұқсат етілмеген түрде жария болуы. Мұндай оқиғалар хакерлік шабуыл, фишинг, бағдарламалық осалдық, ішкі қызметкерлердің әрекеті немесе адами қателіктер нәтижесінде орын алуы мүмкін. Көбіне желіге логиндер, құпиясөздер, карта нөмірлері, жеке және корпоративтік деректер түседі. Бұл беделге нұқсан келтіріп, айыппұлдар мен материалдық шығындарға әкеледі. Белгілі мысалдар - Yahoo, Equifax және Facebook деректерінің ағып кетуі. Қорғану үшін деректерді шифрлау, қолжетімділікті бақылау, қауіпсіздік аудитін жүргізу, пайдаланушылар әрекетін тіркеу және деректерді азайту қағидатын қолдану қажет. Кибершабуылдардың салдары кез келген көлемдегі бизнес үшін өте ауыр болуы мүмкін. Олар тек техникалық аспектілермен шектелмей, сонымен қатар бизнес-процестерге, беделге, қаржылық жағдайға және заңдық жауапкершілікке де әсер етеді.

Қаржылық шығындар – ең байқалатын салдардың бірі. IBM компаниясының 2023 жылғы есебіне сәйкес, бір кибершабуылдың орташа құны шамамен 4,2 миллион долларды құрайды. Бұл сомаға IT-инфрақұрылымды қалпына келтіру, оқиғаны тергеу, (ransomware болған жағдайда) төлем төлеу, заңгерлік шығындар, айыппұлдар, жұмыс уақытындағы үзілістер мен деректердің таралуынан немесе сатылымның тоқтауынан болған жоғалтулар кіреді. Ірі компаниялар үшін бұл сома әлдеқайда жоғары болуы мүмкін, әсіресе миллиондаған клиенттің деректері зақымданған жағдайда [10].

Жеткізу мен логистиканың тоқтауы – тағы бір маңызды салдар. Тасымалдау және логистикалық жүйелерге жасалған шабуылдар (әсіресе вирус-вымогатель немесе жойқын зиянды бағдарламалар арқылы) жеткізулерді тоқтатуға, маршруттар, қоймалар, жүктер және клиенттер туралы деректерге қол жеткізуді шектеуге әкеледі. Мысал ретінде 2017 жылы Maersk компаниясына NotPetya вирусының әсерін келтіруге болады – бірнеше күн бойы жаһандық логистика тоқтап қалды. Бұл тек компанияға ғана емес, оның жеткізу тізбегіндегі барлық серіктестеріне де әсер етті.

Құқықтық тәуекелдер деректерді қорғау және ақпараттық қауіпсіздік саласындағы заңнаманы сақтамаған жағдайда туындайды. Еуропалық Одақта GDPR (General Data Protection Regulation) ережесі қолданылады, ол ЕО азаматтарының жеке деректерін қорғауды және кез келген дерек ағып кету туралы хабарлауды міндеттейді. Бұл ережені бұзғаны үшін компания 20 миллион еуроға дейін немесе жаһандық жылдық табыстың 4%-ына дейін айыппұл төлей алады. ISO 27001 халықаралық стандарты ақпараттық қауіпсіздікті басқару жүйесін енгізуді талап етеді. Бұл талаптарды орындамау – сот істеріне, реттеуші тарапынан санкцияларға және келісімшарттардан айырылуға әкелуі мүмкін.

Клиент сенімінен айырылу – ұзақ мерзімді және көбіне қаржылай бағаланбайтын, бірақ бизнес үшін аса маңызды салдардың бірі. Деректердің таралуы жағдайынан кейін клиенттер, әсіресе банктер, сақтандыру, медицина ұйымдары немесе жеке мәліметтермен жұмыс істейтін платформалар, қызметтерден жаппай бас тартып жатады. Компанияның беделін қалпына келтіру – қосымша PR-жұмыстарды, инвестицияны және қауіпсіздік шараларын күшейтуді талап етеді.

Киберқауіптерге арналған сақтандыру сыйлықақыларының өсуі де айқын трендке айналып отыр. Көптеген компаниялар кибершабуылдардан сақтандыру полистерін сатып алады – оған деректердің таралуы, операциялардың тоқтауы, сот шығындары және жүйелерді қалпына келтіру кіреді. Алайда шабуылдардың жиілігі мен ауқымының артуына байланысты сақтандыру компаниялары полис құнын көтеруде, шарттарды күшейтуде немесе қауіпсіздік деңгейі төмен компанияларға сақтандырудан бас тартып жатады. Бұл бизнестің қаржылық жүктемесін арттырып, барлық деңгейде киберқауіпсіздікке байыппен қарауды талап етеді.

Логистика мен критикалық инфрақұрылымды қорғау – бұл киберқауіпсіздіктің ең маңызды тақырыптарының бірі болып табылады, себебі осы салаларға жасалған кибершабуылдар елдің экономикасы мен қауіпсіздігі үшін катастрофалық салдарға әкелуі мүмкін. Соңғы бірнеше жылда осы секторлардағы киберқатерлер айтарлықтай өсті, сондықтан бұл салалардағы киберқауіпсіздік маңызды орынға ие болды. Төменде осы мәселеге қатысты негізгі жайттар қарастырылған.

Логистика және жеткізілім тізбегі – логистикалық компаниялар, оның ішінде көлік, тауарларды тарату және қоймалау жүйелері, кибершабуылдарға көбірек ұшырап жатыр. Соңғы жылдары жеткізілім тізбегіне жасалған шабуылдар айтарлықтай өсті. Көптеген маңызды элементтер, мысалы, көлік басқару жүйелері, қоймалық автоматизация, жүк қадағалау және тіпті қаржылық транзакциялар, бағдарламалық қамтамасыз ету мен технологияларға тәуелді, бұл оларды хакерлер үшін қолайлы мақсат етеді [9].

Логистикадағы қауіпсіздік мәселелері:

Интернет заттары (IoT): Логистикада IoT-тің дамуы, мысалы, қоймаларда ақылды датчиктерді немесе көліктік құралдардағы GPS-

трекерлерді пайдалану, жаңа қатерлерді тудырады. IoT құрылғылары көбінесе жеткілікті қорғаусыз болады, бұл оларды шабуылдарға осал етеді.

Бағдарламалық қамтамасыз етудегі осалдықтар: Логистикалық процестерді басқару үшін қолданылатын бағдарламалық қамтамасыз ету жиі ескіріп, жаңартылмайды, бұл жүйені бұзушылар үшін ашық қалдырады.

Адам факторы: Логистикада көптеген қызметкерлер жұмыс істейді, бұл кездейсоқ немесе әдейі қауіпсіздік бұзушылықтары болу мүмкіндігін арттырады.

Критикалық инфрақұрылым дегеніміз – мемлекеттің және қоғамның өмірлік маңызды қызметтерін қамтамасыз ететін объектілер. Бұған энергетика, су жіберу, денсаулық сақтау, көлік, қаржы жүйесі және басқа да маңызды салалар жатады. Осы жүйелерге жасалған кибершабуылдар олардың жұмысына ауыр бұзылулар әкелуі мүмкін, бұл экономикалық және әлеуметтік салдарға соқтыруы ықтимал.

Критикалық инфрақұрылымға қауіптер:

Шифровальщик (ransomware): WannaCry және NotPetya сияқты шабуылдар көрсеткендей, шифровальщиктерді қолдана отырып жасалған шабуылдар критикалық инфрақұрылымның жұмысын тоқтатып, деректер мен маңызды жүйелерге кіруді бұғаттай алады.

SCADA жүйелеріне шабуылдар: SCADA (Supervisory Control and Data Acquisition) жүйелері – өнеркәсіптік процестерді бақылау және басқару жүйелері, олар энергетика, мұнай-химиясы және су жіберу сияқты салаларда қолданылады. SCADA жүйелеріне жасалған шабуылдар құралдардың бұзылуына, авариялар мен апаттарға әкелуі мүмкін.

Вирустар және трояндар: Бұл қатерлер өндірісті автоматтандыру және инфрақұрылымдарды басқару жүйелеріне енуі мүмкін.

Мемлекеттің рөлі және арнайы бағдарламалар

Соңғы жылдары көптеген елдер киберқорғаныстың маңыздылығын түсініп, осы салаларды қорғауға бағытталған көптеген заңнамалық және ұйымдық шараларды қабылдады.

Қорғау бағдарламалары:

CISA (АҚШ): Киберқауіпсіздік және инфрақұрылымдық қауіпсіздік агенттігі (CISA) АҚШ-тың критикалық инфрақұрылымдарын қорғауда маңызды рөл атқарады. CISA қауіп-қатерлерді талдау жүргізеді, киберқорғаныс бойынша ұсыныстар әзірлейді, жеке компаниялар мен мемлекеттік құрылымдар арасында үйлестіруді қамтамасыз етеді, сондай-ақ әлем бойынша серіктестермен бірге киберқатерлерден қорғану шараларын қолға алады.

CISA-ның мақсаттары:

– Киберқұрылымдардың сенімділігі мен тұрақтылығын қамтамасыз ету.

– Кибершабуылдардан қорғау және инциденттерге жедел жауап беру.

– Қауіпсіздік стандарттарын әзірлеу және инфрақұрылымды қорғау бойынша ұсыныстар беру.

NIS2 (ЕО): NIS2 директивасы (Network and Information Security Directive) – Еуропалық Одақтың киберқорғанысты нығайтуға арналған маңызды бастамасы, оның мақсаты – желілер мен ақпараттық жүйелердің қауіпсіздігін арттыру, бұл салада энергетика, көлік, денсаулық сақтау және логистика секілді маңызды секторлар да бар. Бұл директива аясында Еуропа елдері критикалық инфрақұрылымды қорғауға арналған ұлттық стратегиялар қабылдауы керек және кибершабуылдарды алдын алу мен жою бойынша үйлестірілген әрекеттер жүргізуге міндетті.

NIS2-нің негізгі талаптары:

– Критикалық секторларда қауіпсіздік бойынша міндетті стандарттарды енгізу.

– Киберқауіптер туралы уақытылы ақпарат беруді және есеп беруді міндеттеу.

– Қауіпсіздік талаптарының бұзылуына жауапкершілік, соның ішінде айыппұлдар мен санкциялар.

– Инциденттерге жедел жауап беру үшін механизмдер құру.

Қорғаныс технологиялық шешімдер: Қауіптер мен шабуылдардың өсуіне байланысты ұйымдар мен мемлекеттер критикалық инфрақұрылымды және логистиканы қорғауға арналған жаңа технологияларды енгізуде.

Мониторинг және қатерлерді анықтау:

Қауіпсіздікті бақылау жүйелері, олар аномалияларды нақты уақытта қадағалап, инциденттерге жедел жауап беру мүмкіндігін қамтамасыз етеді. Бұл жүйелерге SIEM (Security Information and Event Management), IDS/IPS (Intrusion Detection/Prevention Systems), сондай-ақ машиналық оқыту технологиялары кіреді.

Жеткізілім тізбегін қорғау (Supply Chain Security): Жеткізілім тізбегінің қауіпсіздігін арттыру үшін барлық серіктес жеткізушілердің қауіпсіздігін тексеру және әрбір жеткізу кезеңінде тәуекелдерді бақылаудың құралдарын енгізу.

Шифрлау және деректерді қорғау:

Деректерді шифрлау және қорғаудың заманауи әдістерін енгізу құпия ақпараттың сыртқа шығып кету тәуекелін азайтып, критикалық инфрақұрылымдағы операцияларды бұзушылардан қорғауды күшейтеді.

Желілерді бөлу және сегменттеу: Желілерді бөлу және критикалық жүйелерді изоляциялау принциптерін енгізу шабуылдардың салдарын азайтуға көмектеседі.

Логистика мен критикалық инфрақұрылымды кибершабуылдардан қорғау мемлекеттің қауіпсіздігі мен экономикасы үшін маңызды бөлікке айналды. Жаңа қатерлер мен күрделі шабуылдардың пайда болуымен киберқауіпсіздік одан әрі дамып келеді, ал CISA сияқты АҚШ-тың және NIS2 сияқты Еуропалық Одақтың бағдарламалары ең маңызды секторларды қорғау үшін маңызды рөл атқарады [8].

3 NURCRYPT – ЛОГИСТИКАЛЫҚ КОМПАНИЯЛАР ҮШІН АҚЫЛДЫ ДЕРЕКТЕР ҚАУІПСІЗДІГІ ПЛАТФОРМАСЫ

3.1 Деректерді бұзудан және ағып кетуден қорғау

Стартаптың атауы: NurCrypt – логистикалық компаниялар үшін ақылды деректер қауіпсіздігі платформасы

Бұл MVP құру және жобаны бірінші жылы іске қосу шығындарын бағалайтын негізгі бизнес-жоспар болады.

Өнім сипаттамасы.

NurCrypt – логистикалық компанияларға арналған платформа:

– Деректерді шифрлау (end-to-end).

– Сақтық көшірме (real-time & scheduled).

– AI – қауіптерді анықтау.

– Блокчейндегі әрекеттер журналы.

– TMS/WMS/CRM – мен интеграциялауға арналған API.

– Өнім архитектурасы (MVP).

– Қаржыландыру көздері.

NurCrypt – бұл логистикалық операторлар мен көлік компаниялары үшін нақты уақыттағы деректерді сенімді шифрлауды, сақтық көшірмелеуді және қалпына келтіруді қамтамасыз ететін бұлтты платформа. Ол жүктер, маршруттар, клиенттер мен жүргізушілер туралы сезімтал деректерді ағып кетуден, бұзудан және жоғалтудан қорғайды.

– Мақсатты аудитория.

– Логистикалық компаниялар (3PL және 4PL).

– Курьерлік қызметтер.

– Флоты бар компаниялар (жеткізу, бөлшек сауда, FMCG).

– Халықаралық тасымалдаушылар.

– Негізгі функциялар.

Деректерді қорғаудың ең маңызды аспектілерінің бірі – оларды дұрыс шифрлау. Бұл деректердің қауіпсіздігін және құпиялылығын сақтауға, сонымен қатар ақпараттық жүйелердің бұзылуы мен оның ағып кетуінен қорғауға көмектеседі. Шифрлау деректерді тек белгілі бір кілтпен немесе аутентификацияланған пайдаланушымен ғана ашуға мүмкіндік береді, осылайша бұл процесс деректердің кез келген түрін қауіпсіз сақтауға мүмкіндік береді. "Ұшу кезінде" және тыныштықта деректерді шифрлау негізгі екі маңызды жағдайды қамтиды:

"Ұшу кезінде" шифрлау – деректер интернет немесе басқа желі арқылы жіберілгенде шифрланады.

Тыныштықта шифрлау – деректер сақталған кезде (қатты дискіде немесе серверде) шифрланады.

AES-256 (Advanced Encryption Standard - 256 бит) – қазіргі кезде ең қуатты және кең таралған симметриялық шифрлау алгоритмі. Бұл 256 биттік

кілт ұзындығын қолданады және деректерді өте жоғары деңгейде шифрлайды, осылайша оларды тек дұрыс кілтпен ғана ашуға болады. AES-256 шифрлауды көптеген ұйымдар деректерді сақтауда және жіберуде қолданады.

TLS 1.3 (Transport Layer Security) – интернет желісі арқылы деректерді қауіпсіз тасымалдау үшін қолданылатын криптографиялық хаттама. TLS 1.3 соңғы нұсқасы ең жоғары қауіпсіздік деңгейін қамтамасыз етеді, өйткені ол ескірген және осал протоколдардан арылған. Бұл хаттама деректердің ұшу кезінде шифрлануын қамтамасыз етеді, шифрлау кілттерін жаңартуды және жасырын ақпараттарды қорғауды оңтайландырады.

Деректерді бұзудан және ағып кетуден қорғау үшін ұйымдар көпқабатты қорғаныс стратегияларын қолданады. Бұған шифрлау, рұқсатнамаларды басқару, деректердің ағып кетуін бақылау және жүйелік журналдарды сақтауды енгізу кіреді. Деректерді қорғаудың осы әдістері бұзушылардың жүйеге кіруін немесе ақпаратты заңсыз пайдалануын қиындатады.

Шифрлау деректерді тек заңды пайдаланушыларға ғана қолжетімді етіп сақтайды.

Деректерді ағып кетуден қорғау ақпараттың дұрыс емес немесе рұқсат етілмеген жерге кетуіне жол бермейді.

Ақаулыққа төзімді бұлтта сақтау сақталған деректердің қауіпсіздігін қамтамасыз етеді, сонымен қатар оларды қалпына келтіру мүмкіндігін арттырады.

Деректердің үздіксіз қолжетімділігін қамтамасыз ету үшін нақты уақыттағы сақтық көшірме жасау маңызды. Бұл технология жүйедегі кез келген өзгерістерді немесе ақауларды бірден анықтап, сақтық көшірмесін жасауға мүмкіндік береді. Нақты уақыттағы сақтық көшірмелер деректердің жоғалуына немесе бұзылуына жол бермейді, өйткені әрбір маңызды өзгеріс тіркеліп, көшіру әрекеті орындалады.

CRM (Customer Relationship Management) және TMS (Transportation Management Systems) жүйелері көбінесе логистика мен клиенттермен қарым-қатынас орнатуда қолданылатын маңызды құралдар. Оларды бір-бірімен синхрондау деректерді тиімді түрде басқаруға, ақпараттарды уақытылы алуға және оларды қауіпсіз түрде сақтау мен қорғауды қамтамасыз етуге мүмкіндік береді. Синхрондау, әсіресе жеткізілім тізбегінде, өте маңызды, себебі ол ақпараттың дәлдігін қамтамасыз етеді және деректердің бұзылуына немесе қате өңделуіне жол бермейді [14].

Бұлтты сақтау жүйелері деректерді сақтау үшін тиімді шешім болып табылады, ал ақаулыққа төзімді бұлтты сақтау жүйелері екі негізгі қағидатқа негізделеді:

Қалпына келтіру: Деректер жүйе істен шыққан жағдайда немесе апаттық жағдайларда автоматты түрде қалпына келтірілуі керек.

Резервті көшіру: Деректер әртүрлі физикалық орындарда немесе бірнеше провайдерлерде сақталады, бұл жағдайда деректер жоғалғанда, оларды басқа жерде қалпына келтіруге болады.

Блокчейн технологиясы деректердің өзгерістерін тіркеу және қорғау үшін қолданылады. Бұл технология деректердің өзгергенін, қосылғанын немесе жойылғанын нақты уақыт режимінде бақылауға мүмкіндік береді. Әрбір транзакция немесе өзгеріс блокчейнде тіркеледі, бұл оны кейінгі тексеру мен растауға мүмкіндік береді. Бұл әсіресе қаржы және құқықтық салаларда маңызды, өйткені ол деректердің түпнұсқалығын және қауіпсіздігін қамтамасыз етеді.

Деректерге қол жеткізудің мөлдір журналы – бұл жүйеге кімнің, қашан және қандай деректерге қол жеткізгенін тіркейтін жүйе. Мұндай журналдар деректердің заңсыз қолданылуының алдын алу үшін маңызды болып табылады. Қол жеткізу әрекеттерінің журналын бақылау және тексеру арқылы күдікті немесе рұқсат етілмеген әрекеттерді анықтауға болады.

Жеткізу тізбегі – бұл тауарлардың немесе қызметтердің жеткізілу процесін бақылау жүйесі. Киберқауіпсіздік тұрғысынан жеткізу тізбегін бақылау үшін деректерді шифрлау, өзгерістерді бақылау және деректерді синхрондау әдістері қолданылады. Бұл өндірістік процестердің қауіпсіздігі мен тиімділігін қамтамасыз етеді, сондай-ақ жеткізілім тізбегі барысында деректердің қауіпсіздігіне кепілдік береді.

Жасанды интеллект қазіргі таңда киберқауіпсіздік саласында аномалияларды анықтау және қауіптерді бақылау үшін кеңінен қолданылады. AI жүйелері үлкен деректер жиынтықтарын талдай отырып, жүйелерде күдікті әрекеттерді немесе шабуылдарды анықтай алады. Бұл технология көмекші құрал ретінде жұмыс істейді, себебі ол деректердің аномальды қозғалыстарын байқап, автоматты түрде ескертулер мен іс-қимылдарды бастайды.

Компания ішінде күдікті әрекеттерді анықтау жүйелері қызметкерлердің жүйедегі іс-әрекеттерін бақылап, олардың әдеттен тыс немесе қауіпті әрекеттерін анықтайды. Бұл әдіс ішкі қауіптерді – мысалы, қызметкерлердің деректерді заңсыз пайдалануы немесе ұрлауы – анықтауға көмектеседі. Жүйе әдеттегі әрекеттерден ауытқуларды табу үшін мінез-құлықты талдауды пайдаланады.

Деректердің бұзылуы туралы ескерту жүйелері деректердің қауіпсіздігіне қатысты кез келген бұзушылықты дереу анықтап, тиісті шараларды қабылдауға мүмкіндік береді. Бұл жүйелер жиі мониторинг жүргізіп, деректердің тұтастығын бақылап, егер қандай да бір бұзылулар немесе рұқсат етілмеген әрекеттер орын алса, ескерту жасайды.

RBAC (Role-Based Access Control) – бұл деректерге қол жеткізуді басқарудың әдісі, онда пайдаланушылардың рөлдеріне негізделген қол жеткізу құқықтары беріледі. Бұл әдіс ұйымдағы әртүрлі қызметкерлердің белгілі бір деректер мен жүйелерге рұқсат алуын шектеуге мүмкіндік береді, яғни әрбір қолданушы тек өзінің жұмыс міндеттеріне сәйкес ақпаратқа қол жеткізе алады.

2FA (Two-Factor Authentication) – екі факторлы аутентификация әдісі, пайдаланушылардың жүйеге кіргенде қосымша қауіпсіздік қабатын қамтамасыз етеді. Бұл әдіс пайдаланушының логинін және паролін растап қана қоймай, екінші фактор ретінде мобильді құрылғы немесе биометрияны

пайдалануды талап етеді. Биометрия (саусақ ізі, бет тану және т.б.) жүйеге рұқсатты қосымша түрде тексереді, бұл қауіпсіздікті арттырады.

Деректерді қорғау үшін заманауи қауіпсіздік технологиялары мен әдістерін қолдану өте маңызды. Шифрлау, нақты уақыттағы сақтық көшірме жасау, блокчейн қолдану, күдікті әрекеттерді анықтау және басқа да әдістер деректердің қауіпсіздігін қамтамасыз ету үшін маңызды шаралар болып табылады. Технологияның дамуы мен қауіптерді басқару әдістерінің жетілдірілуі ұйымдар мен пайдаланушыларға деректерді сенімді қорғауға мүмкіндік береді [12].

Бизнес-модель:

- SaaS жазылымы (компанияның көлеміне және деректер көлеміне байланысты).

- Премиум қолдау + SLA.

- Қосымша модульдер (қолданыстағы TMS/WMS-пен API интеграциясы).

- Логистикада жүктер ғана емес, деректер де жоғалады, бұл қаржылық шығындар мен бедел тәуекелдеріне әкелуі мүмкін.

- Заңнамалық талаптар (GDPR, ISO 27001, және т.б.) күшейтіледі.

- Киберқауіптердің өсуі саладағы ақпаратты қорғау үшін жаңа шешімдерді қажет етеді.

- Өнім архитектурасы (MVP).Frontend: React немесе Angular, 2FA/SSO авторизациясы, Backend: Node.js / Python (FastAPI/Django), AI модулі, REST API, Сақтау: AWS / GCP / Azure, AES-256, PostgreSQL, Redis, Blockchain.

Өнім архитектурасы – бұл бағдарлама немесе жүйенің негізі болып табылатын компоненттердің құрылымы мен өзара әрекеттесуін сипаттайды. Өнімнің бастапқы нұсқасы (MVP, Minimal Viable Product) көбінесе ең негізгі функционалдығын іске қосып, тестілеуге және нарыққа шығуға дайын өнім болып табылады. Мұндай архитектура жүйенің тиімділігі мен тұрақтылығын қамтамасыз ету үшін әртүрлі технологиялар мен құралдарды пайдаланады.

Frontend (Алдыңғы бөлік): React немесе Angular, 2FA/SSO авторизациясы.

Frontend – бұл қолданушының өніммен өзара әрекеттесетін бөлімі. Оның мақсаты – пайдаланушының интерфейсі мен тәжірибесін оңтайландыру. Бұл компонент тексеріліп, қолданушы үшін қолайлы болуы керек [12].

React немесе Angular – Бұл екі танымал JavaScript фреймворк/библиотекасы фронтенд дамуында кеңінен қолданылады. Олар компоненттерге негізделген архитектураны ұсынады, бұл кодты жеңіл басқаруға және жаңартуға мүмкіндік береді.

React – бұл Facebook компаниясы жасаған кітапхана, ол бір бетке негізделген қосымшаларды жасауға ыңғайлы. React компоненттерді пайдаланады, бұл кодтың қайта қолданылуын қамтамасыз етеді.

Angular – бұл Google компаниясы жасаған толыққанды фреймворк, ол үлкен жобалар мен күрделі қосымшаларды дамыту үшін қолданылатын қуатты

құралдарды ұсынады. Angular модульдік архитектураға ие, бұл масштабтауды оңай етеді.

2FA (Two-Factor Authentication) және SSO (Single Sign-On) авторизациясы - Қауіпсіздікті қамтамасыз ету үшін 2FA және SSO әдістері жиі қолданылады.

2FA – қосымша қауіпсіздік деңгейін енгізеді. Пайдаланушыға тек құпиясөз ғана емес, сонымен қатар қосымша идентификация факторы қажет болады, мысалы, мобильді құрылғы арқылы келген бір реттік код.

SSO – бір рет кіру жүйесі болып табылады, онда пайдаланушы бірнеше қызметке кіру үшін тек бір рет тіркеледі. Бұл пайдаланушылардың жүйеге бірнеше рет кіру қажеттілігін жояды және қауіпсіздікті арттырады.

Backend (Кері бөлік): Node.js / Python (FastAPI/Django), AI модулі, REST API.

Backend – өнімнің логикасын, деректер базасын және жүйе жұмысын қамтамасыз ететін серверлік бөлігі. Бұл компоненттің басты мақсаты – деректерді өңдеу, қолданушының сұраныстарын қабылдау және өңдеу, сондай-ақ қауіпсіздікті қамтамасыз ету.

Node.js – бұл серверлік JavaScript орындаушы ортасы, ол әсіресе деректерді жылдам өңдеу және көптеген сұраныстарды бір уақытта өңдеу қажет болғанда тиімді. Node.js қосымшаларының жоғары өнімділігі және масштабталуы белгілі.

Python (FastAPI/Django). FastAPI – бұл Python тілінде жасалған жоғары жылдамдықты веб-фреймворк, RESTful API жасауға арналған. Ол асинхронды сұраныстарды тиімді өңдейді, әрі пайдаланушы интерфейсі мен сервер арасындағы байланыс жылдам әрі қауіпсіз болады.

Django – Python үшін толыққанды фреймворк болып табылады. Django өнімділікті арттыру үшін көптеген алдын ала дайын компоненттерді ұсынады, сонымен қатар қауіпсіздікке үлкен мән береді. Бұл фреймворк көбінесе үлкен және күрделі веб-қосымшаларды жасау үшін пайдаланылады.

AI модулі – Өнімнің жасанды интеллект (AI) модулі деректерді талдау, болжам жасау немесе пайдаланушының әрекеттеріне негізделген ұсыныстар беру сияқты функцияларды жүзеге асырады.

Бұл модуль алгоритмдер мен мәліметтерді пайдаланып, пайдаланушының қажеттіліктеріне бейімделген қызметтерді ұсынады. Мысалы, AI деректерді талдай отырып, аномалияларды немесе күдікті әрекеттерді анықтай алады.

REST API – Бұл веб-қосымшалардың арасында мәлімет алмасу үшін қолданылатын стандартты интерфейс. REST (Representational State Transfer) архитектурасы клиент пен сервер арасындағы деректерді жеңіл және түсінікті түрде жіберуге мүмкіндік береді. REST API арқылы өнімнің сыртқы жүйелермен және қосымшалармен өзара әрекеттесуі оңай әрі тиімді болады.

3.2 Қазақстандағы бір компанияға кибершабуылдан орташа залал

Сақтау: AWS / GCP / Azure, AES-256, PostgreSQL, Redis, Blockchain.

AWS (Amazon Web Services), GCP (Google Cloud Platform), Azure – бұл үш ірі бұлтты платформа, олар деректерді сақтау және есептеу ресурстарын ұсыну үшін қолданылады. Әрбір платформа түрлі құралдар мен қызметтерді ұсынады:

AWS – бұлттық есептеулер мен сақтау бойынша әлемдегі ең ірі қызметтердің бірі. AWS жоғары деңгейде масштабталатын және сенімді шешімдер ұсынады.

GCP – Google компаниясының бұлттық платформасы. Бұл қызмет машиналық оқыту және жасанды интеллект сияқты жоғары технологиялармен жұмыс істеуге ыңғайлы.

Azure – Microsoft-тың бұлттық қызметі, көбінесе корпоративтік шешімдер мен кәсіпорындардың жоғары деңгейдегі қажеттіліктерін қанағаттандыру үшін пайдаланылады.

AES-256 – бұл деректерді қорғау үшін қолданылатын ең қуатты шифрлау әдістерінің бірі. AES-256 шифрлауы деректердің қауіпсіздігін қамтамасыз етіп, оларды заңсыз қолжетімділіктен қорғайды. Бұл шифрлау әдісі көптеген халықаралық стандарттарға сәйкес келеді және деректерді сақтау мен беру кезінде қолданылатын қауіпсіздік хаттамаларының негізі болып табылады.

PostgreSQL – бұл жоғары өнімді, ашық бастапқы кодты реляциялық деректер базасы. Ол күрделі сұраныстар мен үлкен көлемдегі деректерді өңдеуге қабілетті.

PostgreSQL көбінесе корпоративтік деңгейде пайдаланылатын тұрақты шешім болып табылады.

Redis – бұл жадыдағы деректер базасы, ол деректерді жылдам сақтау және алу үшін қолданылады. Redis көбінесе кэштеу, сессияларды сақтау немесе деректердің жоғары жылдамдықты сұраныстарын өңдеу үшін пайдаланылады.

Blockchain – бұл деректерді сақтаудың және бақылаудың жаңа тәсілі. Blockchain технологиясы деректердің тұтастығын қамтамасыз ете отырып, транзакциялардың тексерілетін және өзгертілмейтін жазбаларын сақтайды. Бұл әдіс әсіресе қаржы жүйелерінде, смарт-келісімдерде және деректердің қауіпсіздігі жоғары салаларда тиімді қолданылады.

Өнімнің архитектурасы дұрыс құрылып, тиімді құралдар мен технологиялар пайдаланылған жағдайда, ол жоғары өнімді, қауіпсіз және масштабталатын болады.

Алдыңғы және кері бөлік үшін ең жаңа фреймворк және тілдер, деректерді қорғау үшін шифрлау әдістері мен бұлттық қызметтерді пайдалану өнімнің қауіпсіздігін, тұрақтылығын және тиімділігін қамтамасыз етеді.

5-кесте – Команда және жалақы (12 ай)

Рөлі	Саны	Айлық ($)	12 айға жалпы ($)
CTO / сәулетші	1	6000	72,000
Backend dev	2	4500	108,000
Frontend dev	1	4000	48,000
DevOps / SecOps	1	5000	60,000
Data Scientist (AI/ML)	1	5500	66,000
UI/UX дизайнері	1	3000	36,000
PM / Product Owner	1	4000	48,000
Sales & Partnerships	1	3500	42,000

Барлығы: $480,000

6-кесте – Басқа шығыстар (12 ай)

Санат	Сомасы ($)
Бұлтты ресурстар (AWS/GCP)	30,000
Сертификаттар, лицензиялар	5,000
Заңды рәсімдер (GDPR, ISO)	10,000
Маркетинг және сайт	20,000
Кеңсе / коворкинг	15,000
SaaS құралдары	5,000
Резервтік қор	10,000

Барлығы: $95,000
12 айлық бюджет (MVP + іске қосу)
Жалақы + шығындар = $575,000

7-кесте – Ықтимал кіріс

Жоспар	Баға ($/ай)	Клиенттер саны	Жылдық табыс ($)
Small	299	200	717,000
Medium	899	50	539,400
Enterprise	2,499	10	299,880

Жалпы болжамды табыс: $1.5M+ / жыл

Іске асыру кезеңдері:

1 ай: UI/UX, сұхбат, ТЗ

2-6 ай: Backend және AI әзірлеу

3-6 ай: Frontend әзірлеу

4-7 ай: Интеграция және DevOps

7-9 ай: Тестілеу және MVP ұшырылымы

9-12 ай: Маркетинг және сатылым

Қаржыландыру көздері:

– Тұқымға дейінгі инвестициялар ($600k дейін).

– Гранттар (логистика, киберқауіпсіздік).

– Мемлекеттік қолдау.

Үдеткіштер (Y Combinator, FRII т.б.)

Қаржыландыру көздері

Тұқымға дейінгі инвестицияларды тарту: 6 600k

Жеңілдікті гранттар (мысалы, логистикалық цифрландыру, киберқауіпсіздік).

Мемлекеттік ат қолдау бағдарламалары

Үдеткіштер (мысалы, Y Combinator, Starta, Free, FRII және т. б.)

Қолданба сипаттамасы:

Атауы: SafeNet KZ

Мақсаты: шағын және орта бизнесті фишингтен, зиянды бағдарламалардан және деректердің бұзылуынан қорғайды.

- Аудитория: қызметкерлер саны 100 адамға дейін жететін компаниялар.

- Жазылым: ұйымға айына 1 100.

- Клиенттер саны: 1,000 компания.

Есептеу үшін алғышарттар:

Қазақстандағы бір компанияға кибершабуылдан орташа залал * - жылына 1 10,000 (KZ-CERT деректері бойынша шағын бизнес фишингтен, вирустардан, DDoS және т. б. жиі зардап шегеді).

SafeNet KZ зиян келтіру қаупін 15% * төмендетеді:

Фишингтік сайттарды бұғаттау

Ағып кету мониторингі

Антивирустық сканер

1000 компания үшін үнемдеуді есептеу:*

Қолданбасыз зиян:

$10,000 × 1,000 компания = жылына 1 10,000,000

Залалды 15% төмендету кезінде үнемдеу:

$10,000,000 × 15% = жылына 1 1,500,000

Кезеңді үнемдеу:Кезең / Үнемдеу

1 жыл |$1,500,000 5 жыл |$7,500,000 10 жыл |$15,000,000

Егер қосымша уақыт өте келе 5,000 клиентке дейін кеңейсе, онда 10 жылдағы үнемдеу сол шарттарды сақтай отырып, 75 млн – нан асуы мүмкін.

ҚОРЫТЫНДЫ

Киберқауіпсіздік жаһандық логистикалық операциялардың аса маңызды құрамдас бөлігіне айналуда. Цифрлық платформаларын қорғауға инвестиция салған компаниялар тек тұрақтылыққа ғана емес, сонымен қатар клиенттер мен серіктестердің сеніміне де ие болады. Сенімді киберқорғаусыз цифрлық логистика өз құндылығын жоғалтады.

Della.kz платформасы – логистикалық саланың цифрлы дамуына елеулі үлес қосып жатқан жоба. Алайда, оның киберқауіпсіздігі заманауи талаптарға толық жауап бермейді. Жоғарыда көрсетілген осалдықтар нақты қауіп төндіреді және оларды жою үшін салыстырмалы түрде қарапайым техникалық шешімдер жеткілікті. Инвестиция көлемі айтарлықтай көп емес, бірақ қорғалмаған жүйеден келетін шығынмен салыстырғанда өте тиімді.

NurCrypt жүйесі жүктер, маршруттар, клиенттер, тапсырыстар және жүргізушілер туралы сезімтал ақпаратты қорғауға арналған. Ол тек деректердің ағып кетуін немесе бұзылуын болдырмайды, сонымен қатар компания ішіндегі күдікті әрекеттерді анықтап, нақты уақыт режимінде ескертулер жібереді. CRM және TMS жүйелерімен толық интеграциясы арқасында NurCrypt логистикалық бизнес-процестерге оңай бейімделеді және үздіксіз жұмысын қамтамасыз етеді.

Қазіргі таңда цифрлық логистикада қауіпсіздік - бұл артықшылық емес, қажеттілік. NurCrypt осы қажеттілікке жауап бере отырып, компанияларға клиенттердің сенімін сақтауға, бизнес-үдерістерін үздіксіз жүргізуге және цифрлық трансформацияны қауіпсіз түрде жүзеге асыруға мүмкіндік береді.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР

1 Ақпараттандыру саласындағы қатынастарды реттеу негіздері. Электрондық сілтеме:https://adilet.zan.kz/kaz/docs/Z1500000418
2 Ресми сайттан алынған бақылау деректері. Электрондық сілтеме: https://della.kz
3 Cloudflare ресми деректері. Электрондық сілтеме:https://cloudflare.com
4 “Cybersecurity for Logistics and Supply Chain Management”. Электрондық сілтеме:https://clck.ru/3MSWM8
5 CISA (Cybersecurity and Infrastructure Security Agency) Электрондық сілтеме:https://www.cisa.gov
6 ENISA (European Union Agency for Cybersecurity). Электрондық сілтеме: https://www.enisa.europa.eu
7 MIT Center for Transportation & Logistics. Электрондық сілтеме: https://ctl.mit.edu
8 SANS Institute – Supply Chain & OT Security. Электрондық сілтеме: https://www.sans.org
9 World Economic Forum-Cyber Resilience in Supply Chains. Электрондық сілтеме:https://www.weforum.org
10 Kaspersky блогы. Электрондық сілтеме:https://www.kaspersky.com/blog
11 Қазақстанды цифрландыру-көлікте ақпараттық қауіпсіздік бойынша материалдар. Электрондық сілтеме:https://cifravyekz.kz
12 Ақпараттық қауіпсіздік бойынша көптеген жобалары бар Технопарк, кейде-логистика. Электрондық сілтеме:https://astanahub.com
13 TMC басқару жүйесі. Электрондық сілтеме:https://www.4logist.com/chto-takoe-tms-sistema-upravleniya–transportom/
14 Positive Technologies сарапшылары. Электрондық сілтеме: https://ptsecurity.com/ru-ru/
15 Veracrypt программасы. Электрондық сілтеме:https://veracrypt.io/ru/Home.html
16 Standard.kz -жеткізу тізбегіндегі бақылау: киберқауіпсіздікті талдау. Электрондық сілтеме:https://standard.kz/ru/post/2024_10_proslezivaemost-v-cepockax-postavok-analiz-kiberbezopasnosti-306
17 STS Logistics-логистикадағы киберқауіптер: қиындықтар мен шешімдер. Электрондық сілтеме:https://stslog.com/press-center/blog/blog_22_10_2024
18 The Hartford – Cybersecurity in Logistics. Логистикалық компаниялар үшін қауіптер мен қорғаныс шараларына шолу). Электрондық сілтеме: https://www.thehartford.com/insights/cyber/cybersecurity-in-logistics
19 PwC – PricewaterhouseCoopers - Жеткізу Тізбегіндегі Киберқауіпсіздік). Электрондық сілтеме:

https://www.pwc.com/us/en/industries/industrial-products/library/cyber-supply-chain.html

20 Fortune Business Insights (2024) есебі. Электрондық сілтеме: https://medium.com/@guiretfuide593/decoding-the-distributed-ledger-a-deep-dive-into-the-blockchain-industry-ceacdf0ad664

21 Casper Labs сауалнамасы (2023)). Электрондық сілтеме: https://proveai.com/news/casper-labs-unveils-2023-enterprise-blockchain-report

22 PricewaterhouseCoopers болжамы (2023). Электрондық сілтеме:https://www.pwc.com/m1/en/media-centre/articles/the-triad-that-secures-blockchain.html

23 PricewaterhouseCoopers есебі (2020). Электрондық сілтеме:https://www.pwc.com.cy/en/issues/assets/blockchain-time-for-trust.pdf

24 Block Data есебі (2021). Электрондық сілтеме:https://cognizium.io/uploads/resources/Blockdata%20-%20Blockchain%20adoption%20by%20the%20wrolds%20top%20100%20public%20companiese%20-%20na.pdf

25 Кәсіпорындарға арналған Hyperledger Fabric блокчейн-платформасы. Электрондық сілтеме:https://hyperledger-fabric.readthedocs.io/en/latest/

26 Ақпараттық қауіпсіздік және жүйелік IT интеграциясы. Электрондық сілтеме: https://cyberfoxglobal.com/