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

Список использованных источников:

1. Фатьянов А.А. Правовое обеспечение безопасности информации в РФ: учебное пособие / А. А. Фатьянов. М.: Юрист, 2001. - 412 с. URL: https://b.eruditor.link/file/776585/ (дата обращения: 21.03.2024 г.)
2. Effros M. Claude Shannon: His Work and Its Legacy // EMS Newsletter. – 2017. URL: https://www.itsoc.org/resources/Shannon-Centenary/shannon-work-legacy-paper (дата обращения: 21.03.2024 г.)
3. Сулейманова Ш.С. Эффективность информационного обеспечения государственной политики: проблемы и перспективы // Коммуникология. 2018. №1. URL: https://cyberleninka.ru/article/n/effektivnost-informatsionnogo-obespecheniya-gosudarstvennoy-politiki-problemy-i-perspektivy (дата обращения: 21.03.2024).
4. Информационная политика: [Электронный ресурс]. URL: https://www.gov.kz/memleket/entities/mangystau-uvp/activities/3580?lang=ru (дата обращения: 14.02.2024).
5. Карягина А.В. Современная информационная правовая политика в РФ: теоретико-правовой аспект // Вестник ТИУиЭ. 2012. №2. URL: https://cyberleninka.ru/article/n/sovremennaya-informatsionnaya-pravovaya-politika-v-rf-teoretiko-pravovoy-aspekt (дата обращения: 22.03.2024).

ӘОЖ 327.7

ЕУРОПАЛЫҚ ОДАҚТЫҢ КИБЕРТЕРРОРИЗМГЕ ҚАРСЫ КҮРЕС ТЕТІКТЕРІ

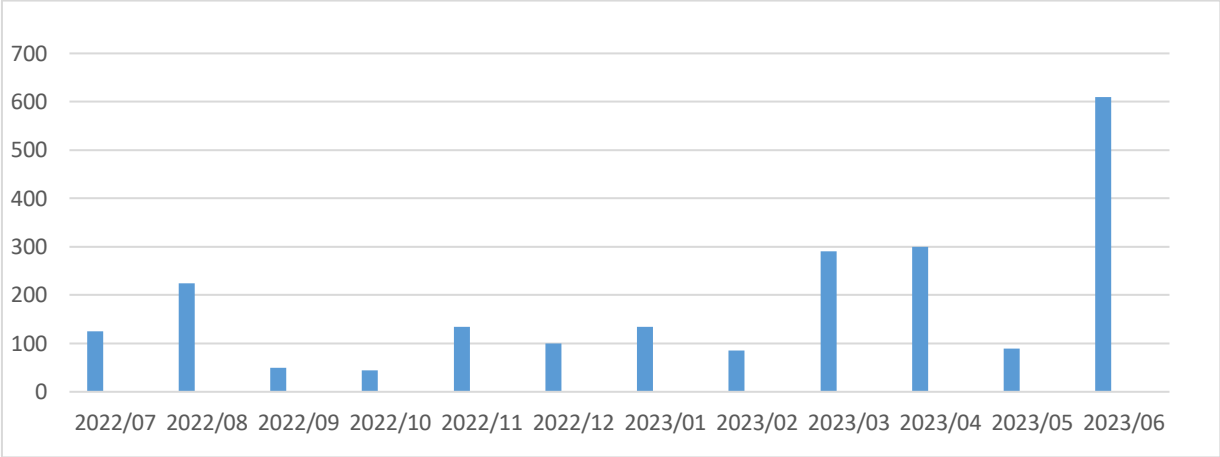
Сөкен Гүлназ Ақанқызы
soken.ga@mail.ru
Л.Н.Гумилев атындағы ЕҰУ,
Халықаралық қатынастар факультетінің магистранты, Астана, Қазақстан
Ғылыми жетекшісі - А.А. Тұрынтаева

Соңғы екі онжылдықта киберқауіпсіздік халықаралық қатынастардың ажырамас бөлігіне айналды. Адамдар жеке және кәсіби қарым-қатынасты сақтау үшін Интернеттегі қатысуын арттырды, ал киберқылмыскерлер бұл жағдайды, атап айтқанда, электрондық коммерция және электрондық төлем кәсіпорындарын, сондай-ақ денсаулық сақтау жүйесін нысанаға алу арқылы пайдаланады. Көлік, энергетика және денсаулық сақтау, телекоммуникация, қаржы, қауіпсіздік, демократиялық процестер, ғарыш және қорғаныс, көбінесе, өзара байланысты болатын желілер мен ақпараттық жүйелерге тәуелді. Желілер мен ақпараттық жүйелердің жұмыс істеуі өз кезегінде электр энергиясының тұрақты жеткізілуіне байланысты секторaралық өзара тәуелділіктер өте күшті. Қосылған құрылғылар қазірдің өзінде планетадағы адамдарға қарағанда көбірек және 2025 жылға қарай олардың саны 25 миллиардқа дейін өседі, соның ішінде олардың төрттен бірі Еуропада деп болжануда [1]. ЕО-дағы өнеркәсіптік ландшафт барған сайын цифрлық және өзара байланысты болып келеді; бұл сонымен қатар кибершабуылдар салалар мен экожүйелерге бұрынғыдан да көбірек әсер етуі мүмкін дегенді білдіреді.

Уақыт өте келе ЕО мен оның елдері үшін киберқауіптер деңгейі айтарлықтай өсті. Соңғы жылдары мемлекеттер мен хакерлік топтар немесе кибертеррористік ұйымдар сияқты бақыланбайтын акторлардың кибершабуылдарының саны мен күрделілігінің артуы байқалды. Еуропалық Одақтың киберқауіпсіздік агенттігінің (ENISA) мәліметтері бойынша, 2020 жылы Еуропадағы негізгі секторларға айтарлықтай зиянды шабуылдар 2019 жылғыға қарағанда екі есе өсті – 146 оқиғадан 304 оқиғаға дейін [2]. Ауруханалар мен басқа да медициналық мекемелерге жасалған кибершабуылдар саны 47%-ға өскен болатын және бұл көрсеткіштер жыл сайын көбеюде *(1-кесте)*. 2020 жылы киберқылмыстан жалпы әлемдік экономикаға жыл сайынғы

шығын 5,5 трлн еуроны құраған болатын, бұл 2015 жылмен салыстырғанда екі есе көп [3]. Бұл жаһандық есірткі саудасынан гөрі тарихтағы экономикалық байлықтың ең үлкен трансферін білдіреді. Кибершабуылдың ең зардапты оқиғаларының бірі, 2017 жылы WannaCry төлем бағдарламасының шабуылы әлемдік экономикаға 6,5 миллиард еуродан астам шығын келтірген болатын. 2019 жылы қаржы және энергетика сияқты маңызды еуропалық инфрақұрылымдармен байланысты 450-ге жуық киберқауіпсіздік оқиғалары болды [3].

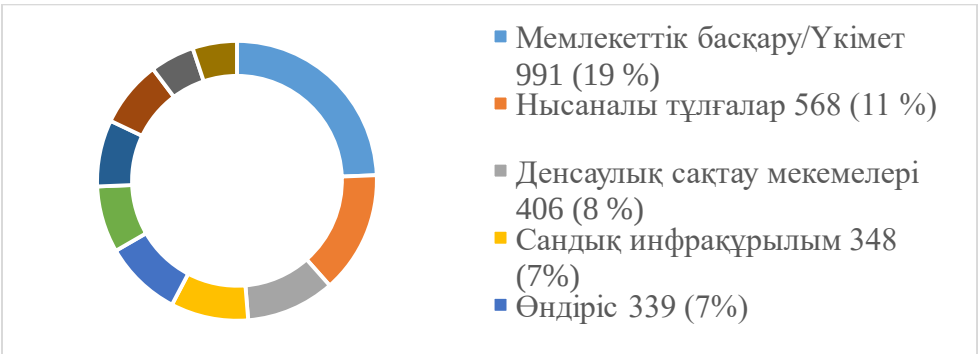
1-кесте. Еуропалық Одақтағы кибершабуылдар хронологиясы.



Дереккөз: ENISA Киберқауіптер ландшафты (2023)

Ал осы 2023 жылы жасанды интеллект (AI) және технологияның жаңа түрлерінің пайда болуының нәтижесінде әлеуметтік инженерлік шабуылдардың саны айтарлықтай өсті. CISA (Киберқауіпсіздік және инфрақұрылымдық қауіпсіздік агенттігі) директоры Джен Истерли Atlantic Council-де ChatGPT сияқты танымал жасанды интеллект құралдарын көрсете отырып, "осы ғасырда кездесетін ең үлкен мәселе" екендігін атап өткен болатын [4]. "Жасанды интеллект осы ғасырдың ең қуатты технологиялық мүмкіндігі және қаруы. Бізде оларды қауіпсіз және тиімді жүзеге асыруға мүмкіндік беретін құқықтық режимдер немесе реттеу жүйелері жоқ. Біз мұны жақын арада анықтауымыз керек", - деп мәлімдеді. Жасанды интеллекттің қарқынды дамуы киберқауіпсіздік нарығында шабуыл құралдары мен қорғаныс құралдары арасындағы жарысты жаңа деңгейге шығарғанын байқаймыз.

2-кесте. Оқиғалар саны бойынша мақсатты секторлар (2022 ж. шілде – 2023 ж. маусым).



Дереккөз: ENISA Киберқауіптер ландшафты (2023)

Технология физикалық әлемнен бөлінбейтін болғандықтан, кибершабуылдар халықтың ең осал топтарының өмірі мен әл-ауқатына қауіп төндіретіні белгілі. Жоғарыда келтірілген ENISA

агенттігі ұсынған соңғы көрсеткіштерден жалпы әлем бойынша біз мемлекеттік басқару (19%) және денсаулық сақтау (8%) секторларындағы ұйымдарға бағытталған көптеген әрекеттерді байқаймыз *(2-кесте)*. Оқиғалардың едәуір бөлігі цифрлық инфрақұрылымға (7%) және цифрлық қызметтерді жеткізушілерге (6%) бағытталған оқиғалардан тұрады. Бұл басқа секторлардың осы екі секторға тәуелділігіне байланысты бірнеше секторға әсер ететін оқиғалар. Сондай-ақ азаматтық қоғамға бағытталған және белгілі бір секторға міндетті емес оқиғалардың айтарлықтай санын көреміз (олар "нысаналы тұлғалар" ретінде белгіленген және байқалған оқиғалардың 11% құрайды) [5].

Кибертерроризмге қарсы іс-қимыл: заңнамалық аспектілері

Еуропалық инфрақұрылым қауіпсіздігі директивасының бастапқы жобасы 2008 жылы Көлік және энергетикалық инфрақұрылымға бағытталған еуропалық маңызды инфрақұрылым (ECI) директивасы қабылданған кезде дайындалды. Ол жалпы көзқарас тұрғысынан болашақ мәтіндердің негізін қалағанымен, киберқауіпсіздік тәуекелдерін қарастырмайды.

Жалпы киберқауіпсіздік саясатының негізі 2013 жылы Еуропалық одақ пен ұлттық заңнаманы байланыстыратын ЕО-ның алғашқы киберқауіпсіздік стратегиясы (EUCSS) қабылданған кезде қаланған болатын. Бұл сонымен қатар "киберқауіпсіздік" терминін ашық түрде қолданатын алғашқы мәтін болып табылады. Еуропалық киберқауіпсіздікті нығайту мақсатында EUCSS әрбір мүше мемлекетті Ұлттық компьютерлік төтенше жағдайларды жою тобын (CERT), сондай-ақ Бельгияның Киберқауіпсіздік орталығы (CCB) немесе Франциядағы ANSSI сияқты еуропалық деңгейдегі пікірталастарда елдің атынан қатысатын құзыретті киберқауіпсіздік органын құруға итермеледі.

3-кесте. Әлем елдерінің киберқауіпсіздік деңгейі.

	Мемлекет	Ұлттық киберқауіпсіздік индексі	Цифрлық даму деңгейі	Айырмашылық мөлшері
1	Бельгия	94.81	74.07	20.74
2	Литва	93.51	67.34	26.17
3	Эстония	93.51	75.59	17.92
4	Чех Республикасы	90.91	69.21	21.70
5	Германия	90.91	80.01	10.90
6	Румыния	89.61	59.84	29.77
7	Греция	89.61	64.02	25.59
8	Португалия	89.61	68.46	21.15
9	Ұлыбритания	89.61	79.96	9.65
10	Испания	88.31	72.21	16.10

Дереккөз: Ұлттық киберқауіпсіздік индексінің мәліметтері

Елдердің киберқауіптердің алдын алуға және оларды басқаруға дайындығын анықтайтын жаһандық индекс Ұлттық киберқауіпсіздік индексінің (NCSI) (нақты уақыт режимінде жаңартылады) соңғы деректері бойынша әлемдегі киберқауіпсіздік деңгейі ең жоғары 10 ел таңдап алынған болатын [6] *(3-кесте)*. NCSI киберқауіпсіздіктің 4 аспектісіне назар аударады:

1. Қолданыстағы заңнама – құқықтық актілер, ережелер, бұйрықтар және т. б.
2. Құрылған бөлімшелер – қолданыстағы ұйымдар, департаменттер және т. б.
3. Ынтымақтастық форматтары – комитеттер, жұмыс топтары және т. б.

4. Нәтижелер – саясат, технологиялар, веб-сайттар, бағдарламалар және т. б.

Келтірілген мәліметтер бойынша, ондыққа кіретін елдердің барлығы дерлік (Ұлыбританиядан басқа) ЕО-тың мүшесі, бұл аймақтағы киберқауіпсіздік деңгейінің басқалардан неғұрлым жоғарылығын көрсетеді. Соның ішінде Германияда киберқауіпсіздік деңгейі мен цифрлық даму деңгейі өзара сәйкес келеді. Германия Еуропалық Одақ елдері арасында ең көп кибершабуылдарға ұшырады. Осыған байланысты елдің киберқауіпсіздік саясаты өзгере бастады. Германия киберкеңістіктегі қолданыстағы нормаларды, ережелерді қайта қарағаң болатын. Еуропалық киберқауіпсіздік орталықтарының Еуропалық желісі сияқты киберқауіпсіздік жобаларында жетекші рөл атқаратын ЕО мүшелерінің бірі - Бельгия. Бельгияда қуатты киберқауіпсіздік инфрақұрылымы құрылған, елде киберқауіпсіздікке инвестициялардың деңгейі жоғары. Эстонияның жетістігінің себебі мемлекеттік емес институттардың маңызды рөлінде, ал Германия үшін басты рөл мемлекеттік органдарға жүктеледі. Эстония аумағында НАТО-ның Таллиндегі кибер орталығы да орналасқан, бұл елордада жоғары деңгейдегі мамандардың үлкен шоғырлануын, олардың көмегімен киберсаясаты қалыптасуын және Эстонияның жоғары деңгейлі қорғанысының болуын түсіндіреді.

Кибертерроризмді ЕО шеңберінде реттеудің институционалдық тетіктері

Тұрақты халықаралық киберқауіпке тап болған ЕО терроризмге қарсы күресте барған сайын елеулі рөл атқарады. Киберқылмыспен күресу және қауіпсіздікті қамтамасыз ету үшін негізгі жауапкершілік мүше мемлекеттерде болса да, ЕО ынтымақтастық және үйлестіру құралдарын, сондай-ақ осы шекарасыз құбылыспен күресу үшін қаржылық қолдау көрсетеді. Сонымен қатар, даму мен тұрақтылық пен ішкі және сыртқы қауіпсіздік арасында байланыс бар деген болжам ЕО-ның өз шекарасынан тыс әрекеттерін анықтай бастады. ЕО-ның терроризмге қарсы іс-қимыл саласындағы шығындары жылдар өткен сайын өсті, бұл Еуропол (Еуропалық Одақтың полиция агенттігі) және Еуропалық желілік және ақпараттық қауіпсіздік агенттігі (ENISA) сияқты қауіпсіздік пен әділеттілікке жауапты ЕО органдарының ұлттық құқық қорғау органдары арасындағы жақсы ынтымақтастықты және күшейтілген қолдауды қамтамасыз етуге серпін берді.

Еурополдың Еуропалық киберқылмыс орталығының (EC3) киберқылмыстардың алдын алу және тоқтату шараларын жүзеге асырудағы негізгі тәжірибелеріне төмендегілерді атап өтсек болады:

– EC3 және J-CAT соңғы онжылдықтағы ең маңызды ботнеттердің бірі – EMOTE-ті жоюға қатысты [7].

– 2014 жылдың ақпанында Троэлс Эртинг 2013 жылы бөлімшенің жетістіктері туралы хабарлады. Олар интернетке негізделген төлемдерді ұстауды қамтыды, нәтижесінде 13 қамауға алынды. Олар сондай-ақ ботнеттерді қолдана отырып, банктерге зиянды шабуылдармен күресуге қатысты және Microsoft пен Германияның федералды қылмыстық полиция басқармасының сарапшыларымен бірлесіп ZeroAccess ботнетін жойды [8].

– 2014 жылы Onymous операциясының егжей-тегжейлері ашылды, ол PANDORA, Cloud 9, Hydra, Blue Sky, Topix, Flugsvamp, Cannabis Road, Black Market және Silk Road 2.0 сияқты бірқатар Darknet веб-сайттарды жойды [9].

– 2015 жылы американдық БАҚ EC3 көмегімен киберқылмыскерлерге арналған ең үлкен ағылшын тілді коммуникация және сауда платформасы Dark0de-ді жою үшін ФБР-дің үйлестірілген операциясы жүзеге асырылған болатын [10].

– EC3 және J-CAT төлем бағдарламаларымен күресуде, маңызды жетістіктерге жетті: TALPA операциясы, "Бесінші элемент" операциясы және "Алтын құм" ("Gold Dust") операциясы [11].

Сондай-ақ, EC3 жыл сайын онлайн режимінде ұйымдасқан қылмыс қаупін бағалауды (ACT) жариялайды, бұл киберқылмыс саласындағы негізгі тұжырымдар мен туындайтын

қауіптер мен өзгерістер туралы өзінің негізгі стратегиялық есебі.

2004 жылы құрылған және 2019 жылғы ЕО киберқауіпсіздік туралы Заңымен күшейтілген ENISA – Еуропалық одақтың тәуелсіз органы, оның негізгі қызметі Еуропалық Одақтағы киберқауіпсіздікті қолдау және жетілдіру болып табылады. ENISA зерттеулер жүргізеді, кеңестер мен ұсыныстар береді және киберқауіпсіздік саясатын дамытуға және жүзеге асыруға көмектеседі.

Жыл сайынғы киберқауіпсіздік қаупі ландшафтының жағдайы туралы ENISA Threat Landscape (ETL) есебінің он бірінші басылымынан (2023) геосаясаттың киберқауіптің таралу аймағына тікелей әсер ету факторын көреміз [12]. Ресей мен Украина арасындағы қақтығыс қауіп-қатер ландшафтын өзгертті. Кейбір назар аударатын өзгерістер қатарында хактивистік белсенділіктің айтарлықтай өсуі, белсенді соғыс қимылдарымен бірлесіп операциялар жүргізетін кибершабуылдар, хактивистерді жұмылдыру, киберқылмыс және осы қақтығыс кезінде ұлттық мемлекеттер топтарының көмегі болды. Хактивизмнің жаңа толқыны әсіресе Ресей-Украина дағдарысы басталғаннан бері байқалады. Деструктивті шабуылдар мемлекеттік субъектілердің операцияларының маңызды құрамдас бөлігі болып табылады. Ресей – Украина қақтығысы кезінде кинетикалық әскери әрекеттермен бірге операциялар жүргізетін кибершабуылдар байқалды. Жалған ақпарат та – ақпарттық соғыстың құралы. Ол "физикалық" соғыс басталғанға дейін Ресейдің Украинаға басып кіруіне дайындық шарасы ретінде қолданылған болатын.

ЕО және оның елдері кибертерроризмге әртүрлі жауап береді, соның ішінде қауіпсіздік шаралары мен жауапты адамдар мен ұйымдарға қарсы санкциялар. 2017 жылы ЕО пен оның елдерінің киберқауіпсіздік қабілеттерін нығайтуға бағытталған ЕО-тың Киберқауіпсіздік жоспарын қабылданды. Жоспар киберқауіпсіздікке инвестицияларды ұлғайтуды ЕО-ға мүше елдер арасындағы ынтымақтастықты нығайтуды қамтиды.

Сонымен қатар, ЕО кибершабуылдарға қатысқан акторларға қарсы санкциялар қолдану тәжірибесін атап өтуге болады. 2019 жылдың 17 мамырында ЕО-тың Кеңесі кибершабуылдарды тежеу және оларға қарсы әрекет ету үшін шектеу енгізу механизмін құрған болатын. 2020 жылы ЕО кибершабуылдар жасады деп айыпталған алты адамға және үш ұйымға санкциялар енгізді [13]. Бұл санкцияларға елге кіруге және шығуға тыйым салу және активтерді тоқтату, сондай-ақ байланыс технологиялары мен қызметтерін ұсынуға тыйым салу кіреді.

Алайда, кибертерроризмге қарсы күрес күрделі міндет болып табылады, өйткені киберқауіптер үнемі дамып, өзгеріп отырады. Сондықтан ЕО және оның елдері өздерінің киберқауіпсіздік жүйелерін дамытуды жалғастыруда және кибершабуылдарға тиімді қарсы тұру мақсатында оқыту мен ақпарат алмасуды жүргізуде.

Ірі трансшекаралық кибершабуылдарға дайындық үшін Еуропалық Одақ Кеңесі ЕО құқық қорғау органдарының шұғыл әрекет ету хаттамасын қабылдады. Хаттама жоғарыда айтылған ЕСЗ-на орталық рөл береді және ЕО-ның ауқымды трансшекаралық инциденттер мен киберқауіпсіздік дағдарыстарына үйлестірілген әрекет ету жоспарының бөлігі болып табылады. Ол ЕО-ның құқық қорғау органдарын жедел бағалау, маңызды ақпаратты қауіпсіз және уақтылы бөлісу және олардың тергеулерінің халықаралық аспектілерін тиімді үйлестіру арқылы ірі трансшекаралық кибершабуылдарға жедел ден қоюды қамтамасыз ету құралы ретінде қызмет етеді.

2017 жылы бұрын-соңды болмаған WannaCry және NotPetya кибершабуылдары киберқылмыскерлердің тез өзгеретін жұмыс әдістеріне тиімді қарсы тұру үшін оқиғаға негізделген реакциялардың қаншалықты жеткіліксіз екенін анық көрсетті. "ЕО мен оның азаматтарын ауқымды кибершабуылдардан қорғау үшін кибернетикалық дайындықты арттыру өте маңызды", - деп мәлімдеді Уил ван Гемерт, Еуропол операциялары жөніндегі атқарушы директордың орынбасары. - "Құқық қорғау органдары зардап шеккендердің санын азайту және шабуылға жауапты адамдарды жауапқа тарту үшін қажетті дәлелдерді сақтау үшін төтенше жағдайларға жауап беруде маңызды рөл атқарады" [14].

Киберқауіптерді және оларды реттеу механизмдерін зерделей келе, ЕО-тың институттары және агенттіктері киберқауіптер туралы ұжымдық ситуациялық хабардарлыққа ие емес. Себебі ұлттық билік ЕО-дағы киберқауіпсіздік жағдайын бағалауға көмектесетін ақпаратты жеке сектордан алынған ақпарат сияқты жүйелі түрде жинамайды немесе бөліспейді. Мүше мемлекеттер оқиғалардың аз ғана бөлігі туралы хабарлайды және ақпарат алмасу жүйелі де, жан-жақты да емес; кибершабуылдар еуропалық қоғамдарға жасалған келісілген зиянды шабуылдардың бір ғана аспектісі болуы мүмкін. Қазіргі уақытта мүше мемлекеттер арасында шектеулі өзара жедел көмек бар және ауқымды трансшекаралық киберқауіптер немесе дағдарыс жағдайында мүше мемлекеттер мен ЕО институттары, агенттіктері мен ведомстволары арасында жедел механизм толықтай жасақталмаған.

Осы тұрғыда ENISA нормативтік және жұмыс тәжірибесінде ашықтық пен ынтымақтастыққа басымдық беруі маңызды. Ол сертификаттау схемаларын әзірлеуді жүзеге асыратын процестер де бірлескен болуы керек және ол әртүрлі мүдделі тараптармен, соның ішінде өнеркәсіппен, сауда қауымдастықтарымен, стандарттау органдарымен және мүше мемлекеттермен тиісті консультацияларды қамтамасыз етуі тиіс.

Кибертерроризммен күресте шетелдік тәжірибелерді де ескеру қажет. Шетелдердің тәжірибесін қолданудың бірнеше мысалдары мен мүмкіндіктері ретінде төмендегілер анықталды:

1. Жеке сектормен өзара іс-қимыл: ЕО, мысалы, киберқауіпсіздік және коммерция орталығы (NCCoE) бағдарламасы аясында АҚШ-та енгізілгенге ұқсас мемлекет пен жеке сектор арасындағы серіктестіктің сәтті модельдерін қолдана алады. Мұндай ынтымақтастық кибершабуылдардың алдын алу және оларға ден қою кезінде жеке сектордың техникалық ресурстары мен сараптамасын тиімдірек пайдалануға мүмкіндік береді. ЕО да мүшесі болып табылатыг НАТО және АҚШ киберқауіпсіздікке неғұрлым тиімді және жан-жақты жауап беру үшін жеке киберқауіпсіздік компанияларымен ынтымақтасады. Бұл жеке секторда әзірленген озық тәжірибелер мен технологияларды мемлекеттік қауіпсіздік жүйелерінде пайдалануға мүмкіндік береді. Жеке сектормен осындай ынтымақтастық ЕО-да жетекші IT-компаниялармен және киберқауіпсіздік мамандарымен серіктестік орнату арқылы жүзеге асырылуы мүмкін.

2. Киберспецназ және оқыту: АҚШ құқық қорғау органдарының қызметкерлеріне, соның ішінде киберқауіпсіздік мамандарына арналған оқыту және оқыту бағдарламаларын белсенді түрде әзірлеуде. 2018 жылға қарай USCYBERCOM пайда болды, ол АҚШ-тың кибертеррористерге қарсы іс-қимылдарды синхрондау, бағыттау және үйлестіру бойынша жауынгерлік қолбасшылығына айналды. Бұл бағдарламалар киберқауіптерге жауап беру және оқиғаларды талдау үшін арнайы бөлімшелер құруды қамтиды. ЕО-да киберспецназды нығайту және Киберқауіпсіздік бойынша білім деңгейін арттыру үшін осындай оқыту бағдарламалары мен білім беру бастамаларын енгізуге болады.

Қорытындылай келе, Еуропол жыл сайын осы ұйымның мамандары интернетте ұйымдасқан қылмыс қаупін бағалайды. Атап айтқанда, 2022 жылдың соңында жүргізілген соңғы бағалаудың нәтижелері бойынша киберқылмыстың негізгі тенденциялары оның үнемі жетілуі болып табылатындығында, сондай-ақ қақтығыстардың күшеюі аясында ең тиімді және жаһандық мақсаттарды таңдауға баса назар аударылады. Сонымен қатар, бопсалау жағдайлары желіде негізгі қауіп болып қала береді. Осыған байланысты Еуропол болашақта Еуроодақ аумағында мүмкін болатын заңсыз көріністер туралы ескерту сияқты фактілерді қарастыру қажет деген тұжырымға келеміз.

Кибершабуылдарды анықтау және алдын алу үшін жасанды интеллектті дамыту – ең ықтимал шаралардың бірі. Машиналық оқыту алгоритмдерін үлкен көлемдегі деректерді талдау және желілердегі заңсыз әрекеттерді тану үшін пайдалануға болады. Жасанды интеллект негізінде шабуылды анықтау жүйесін (Intrusion Detection Systems - IDS) енгізу ұсынылады. Бұл желідегі күдікті әрекеттерді автоматты түрде анықтауға және оларға жауап беруге мүмкіндік береді.

AI негізіндегі кибершабуылдарды анықтау жүйесінің жұмысына келетін болсақ, ол келесі қадамдарды қамтиды:

1. Деректерді жинау: AI жүйесі желілік белсенділіктің толық бейнесін алу үшін әртүрлі дереккөздерге, соның ішінде желілік белсенділік журналдарына, антивирустарға, брандмауэрлерге және басқа көздерге қол жеткізуі керек.

2. AI моделін оқыту: ауытқулар мен күдікті әрекеттерді тануды үйрену үшін жүйені үлкен көлемде оқыту керек. Ол үшін машиналық оқыту және терең оқыту алгоритмдерін қолдану қажет.

3. Шабуылдарды анықтау және алдын алу: оқытудан кейін жүйе ауытқуларды автоматты түрде анықтай алады және күдікті белсенділік туралы сигнал бере алады. Егер шабуыл анықталса, жүйе оның алдын алу үшін шаралар қолдана алады, соның ішінде кіруді бұғаттау немесе әкімшіге (администраторға) ескерту.

4. Оқиғаларды басқару және жауап беру жүйелері (SIEM): IDS AI кибершабуылдарды тиімді талдау және жауап беру үшін оқиғаларды басқару және жауап беру жүйесімен біріктірілуі мүмкін.

Мұндай AI негізінде шабуылды анықтау жүйесін іске асыру Еуропалық комиссия, ENISA, ұлттық үкіметтер арасындағы тығыз ынтымақтастықты көздейтіні анық. ENISA қазірдің өзінде Еуропалық одақтың киберқауіпсіздік жөніндегі негізгі агенттігі болып табылады және осы салада тәжірибесі бар. Олар шабуылдарды анықтау үшін AI жүйелерін енгізу стандарттары мен нұсқауларын әзірлеуге қатыса алады. Еуропалық комиссия ЕС Еуропалық Одақтағы шабуылдарды анықтау жүйелеріне жасанды интеллектті әзірлеу және енгізу жобасын қаржыландыруда және бастауда үлкен рөл атқара алады. Сондай-ақ, мемлекеттік деңгейде зерттеу жүргізуге, инфрақұрылымды құруға және киберқауіпсіздік бойынша кадрларды даярлауға қаражат бөлу секілді кешенді іс-қимылдар жүргізілсе, киберқауіптердің алдын алу мен тоқтатуда алға жылжу болар еді деп болжанады.

Халықаралық ынтымақтастықты күшейту кибертерроризм секілді жаһандық маңызы бар мәселеде ең негізгі ұстанымдардың бірі: киберқауіптер туралы ақпарат алмасу және ЕО елдері арасындағы іс-қимылды үйлестіру үшін еуропалық платформалардың нәтижелілгін бақылау маңызды. Бұл кибершабуылдарды тезірек анықтауға және жолын кесуге, сондай-ақ кибертерроризмнің әдістері туралы ақпарат алмасуға мүмкіндік береді. Елдер кибертерроризмге қарсы тұру үшін жаңа қауіптер мен шабуылдар туралы белсенді түрде ақпарат алмасуы керек.

Бұл шаралардың барлығы тез өзгеретін киберқауіпті ортаны және жаңа технологиялардың дамуын ескере отырып, әрине, кешенді түрде қолданылуы тиіс.

Қолданылған әдебиеттер тізімі

1. GSMA телекоммуникациялық сауда қауымдастығы жүргізген бағалау. [Электронды ресурс]. – URL: https://www.gsma.com /iot/wpcontent/uploads/2018/08/GSMA-IoT-Infographic-2019 .pdf (қаралған күні: 10.09.2023)

2. Nick Paton Walsh. Serious cyberattacks in Europe doubled in the past year // CNN. [Электронды ресурс] – 2021. – URL: https://edition.cnn.com/2021/06/10/tech/europe-cyberattacks-ransomware-cmd-intl/index.html (қаралған күні: 10.09.2023)

3. ЕО-ның цифрлық онжылдықтағы киберқауіпсіздік стратегиясы (16 желтоқсан, 2020 жыл).

4. Curran J. Easterly Voices Urgent Need to Set AI Regulatory Landscape. [Электронды ресурс] // MeriTalk – 2023. – URL: https://www.meritalk.com/articles/easterly-voices-urgent-need-to-set-ai-regulatory-landscape/ (қаралған күні: 15.09.2023)

5. Cybersecurity: how the EU fights cyber threats? [Электронды ресурс] // Еуропалық кеңес ресми сайты. – 2023. – URL: https://www.consilium.europa.eu/en/policies/cybersecurity (қаралған күні: 15.09.2023)

6. Ұлттық киберқауіпсіздік индексі. – URL: https://ncsi.ega.ee/ncsi-index/?order=rank (қаралған күні: 24.09.2023)
7. Richard A. Clarke, Robert K. Knake. The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats // Penguin Press, New York. – 2019. – 384 б.
8. Joint Cybercrime Action Taskforce (J-CAT). [Электронды ресурс] // Europol ресми сайты. – URL: https://www.europol.europa.eu/operations-services-and-innovation/services-support/joint-cybercrime-action-taskforce (қаралған күні: 24.09.2023)
9. Ermert M. Chef der EU-Cybercops zieht Erfolgsbilanz. [Электронды ресурс] // Heise online. – 2014. – URL: https://www.heise.de/news/Chef-der-EU-Cybercops-zieht-Erfolgsbilanz-2110188.html (қаралған күні: 24.09.2023)
10. Patrick B. Behörden schließen Drogen-Plattformen im Dark Web. [Электронды ресурс] // Zeit. – 2014. – URL: https://www.zeit.de/digital/internet/2014-11/operation-onymous-silk-road-betreiber-festgenommen (қаралған күні: 24.09.2023)
11. Bull K. FBI Leads Darkode Takedown. [Электронды ресурс] // Homeland Security Today – 2015. – URL: http://www.hstoday.us/single-article/fbi-leads-darkode-takedown/e43083ab3d9cc040901de3a596ab1750.html (қаралған күні: 03.10.2023)
12. ENISA: Киберқауіптер ландшафты 2023. (қаралған күні: 03.10.2023)
13. Haruspex security. The first ever EU sanctions against cyber-attacks. [Электронды ресурс] // Medium. – 2020. – URL: https://medium.com/@haruspex.security/the-first-ever-eu-sanctions-against-cyber-attacksb07889e4e1c2#:~:text=On%20July%2030th%2C%202020%20the,‘NotPetya’%2C%20and%20‘Operation%20Cloud%20Hopper’ (қаралған күні: 03.10.2023)
14. Law enforcement agencies across EU prepare for major cross border cyber-attacks. [Электронды ресурс] // Europol. – URL: https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-agencies-across-eu-prepare-for-major-cross-border-cyber-attacks (қаралған күні: 07.10.2023)

UDC 327.8

RESHAPING CENTRAL ASIA: THE DYNAMICS OF CHINA'S INFLUENCE AND REGIONAL LANDSCAPE TRANSFORMATION

Supyaldiyarov Islam
islam.supyaldiyarov@sdu.edu.kz
PhD student, Faculty of International Relations,
L.N. Gumilyov Eurasian National University, Astana, Kazakhstan
Supervisor - S.K. Alieva

In the post-1991 global order, Central Asia is undergoing profound transformations and has become an arena where the interests of various powers intersect, leading to simultaneous processes of cooperation and competition among global and regional actors. As early as the beginning of the last century, British geographer Sir Halford Mackinder, often regarded as the founder of geopolitics, foresaw the end of European dominance and emphasized the growing significance of the central part of Eurasia in the new era, referring to this zone as the "geographical pivot of history." In his article "The Geographical Pivot of History," published in The Geographical Journal in April 1904, Mackinder outlined that the world is divided into distinct zones, each fulfilling its functions, and whoever controls the Heartland controls the World Island, and subsequently the entire world [1]. According to this theory, in the context of global geopolitical processes, the Eurasian continent lies at the heart of the world, with the Heartland being the part of Eurasia where vast land masses are concentrated [2]. Amidst the escalating