МАЗМҰНЫ / СОДЕРЖАНИЕ / CONTENT

Мақала туралы мәлімет

Конференция атауы	«Жастар және ғылым: бүгіні мен болашағы» жас ғалымдардың халықаралық ғылыми-тәжірибелік конференция материалдар жинағы
Сборник	«Молодежь и наука: настоящее и будущее». Сборник материалов Международной научно-практической конференции молодых ученых
Conference	The collection of materials from the International Scientific and Practical Conference of Young Scientists «Youth and Science: Present and Future»
Өткізілген күні	7 сәуір 2025, Атырау
ISBN	978-601-262-587-5
Жинақтағы жариялану №	109
Жинақтағы беттері	511-514
ӘОЖ/УДК/UDC	ӘОЖ 002:004.056
Секция	Секция IV. II Адам құқығын қорғау – құқықтық және әділ мемлекет құрудың кепілі/ / Защита прав человека – залог создания правового и справедливого государства
Автор(лар)	Мүстекенов К.Т.
Мәртебесі	Студент
Ғылыми жетекші	Ғылыми жетекшісі, з.ғ.м. Аманжол Ж.М.
Мақала атауы	КИБЕРҚЫЛМЫС ЖӘНЕ ДЕРЕКТЕРДІҢ ҚАУІПСІЗДІГІ

безопасности Республики Казахстан. Научные труды Академии финансовой полиции. Выпуск 3. Астана: Фолиант, 2002. – 496 с.

3 Актуальные вопросы взаимодействия науки, законотворчества и.Диссертационная работа Байзакова Д. 2018 год Академия государственного управлениянри Президенте РК.

ӘОЖ 002:004.056

КИБЕРҚЫЛМЫС ЖӘНЕ ДЕРЕКТЕРДІҢ ҚАУІПСІЗДІГІ

Мүстекенов К.Т.
karimbek.m@mail.ru
«Құқықтану» білім бағдарламасының 1 курс студенті
Қ.Жұбанов атындағы Ақтөбе Өңірлік Университеті, Ақтөбе қ, Қазақстан Республикасы
Ғылыми жетекшісі, з.ғ.м. Аманжол Ж.М.

Киберқылмыс және деректердің қауіпсіздігі – ақпараттық технологиялардың қарқынды дамуы мен кеңінен қолданысқа енуімен бірге өзекті мәселеге айналды. Қазіргі таңда интернет пен цифрлық технологиялар қоғамның барлық саласына терең енді. Алайда, бұл процестің бірге келетін қауіптері де аз емес. Киберқылмыскерлер түрлі әдістермен жеке тұлғалар мен ұйымдардың құпия ақпараттарына қол жеткізуге тырысып, экономикалық және reputациялық шығындар әкеліп отыр.Мақалада киберқылмыстың негізгі түрлері, оның ішінде фишинг, зұлымдық бағдарламалар (вирус, троян, шпиондық бағдарламалар) мен денсаулық сақтау, қаржы секторы сияқты маңызды салаларға жасалатын шабуылдар туралы айтылып, олардың қоғам мен бизнеске тигізетін зияны талданады. Сонымен қатар, деректердің қауіпсіздігін қамтамасыз ету үшін қолданылатын заманауи әдістер мен құралдар, оның ішінде криптография, көпфакторлы аутентификация, брандмауэрлар мен желі мониторингі туралы ақпарат беріледі. Мақалада деректерді қорғау бойынша мемлекеттік және жеке секторлар арасындағы ынтымақтастық, киберқылмысқа қарсы халықаралық заңдар мен нормалар және цифрлық қауіпсіздік мәдениетін қалыптастырудың маңызы қарастырылады. Цифрлық қауіпсіздікті қамтамасыз ету тек техникалық шаралармен шектелмей, қоғамның әр мүшесінің осы мәселеге қатысты жауапкершілігін арттыруды талап етеді.

Бұл тақырып ақпараттық қауіпсіздік саласындағы жаңа технологиялардың дамуына, сондай-ақ киберқылмысқа қарсы күрес жүргізу бойынша қабылданатын шаралардың өзектілігіне тоқталатын маңызды мәселе болып табылады.

Ақпараттық технологиялардың қарқынды дамуы мен цифрлық әлемнің кеңеюі қазіргі заманғы қоғамды жаңа мүмкіндіктермен қамтамасыз етіп қана қоймай, көптеген күрделі қауіптер мен қиындықтарды да алып келді. Интернет пен цифрлық жүйелер қоғамның барлық салаларын бір-бірімен байланыстырған жаңа әлемнің негізін қалайды. Әлеуметтік желілер, электрондық банкинг, онлайн сауда, мемлекеттік қызметтер мен көптеген басқа онлайн қызметтер адамдардың күнделікті өмірінің ажырамас бөлігіне айналды. Алайда, осы өзгерістермен бірге ақпараттық жүйелердің қауіпсіздігі мен деректердің қорғалуы аса маңызды мәселеге айналды.

Киберқылмыс дегеніміз – цифрлық технологияларды, интернет желісін және компьютерлік жүйелерді пайдаланатын заңсыз әрекеттердің жиынтығы. Бұл өз кезегінде жеке тұлғалар мен ұйымдардың деректеріне зиян келтіріп, оларға экономикалық және репутациялық зиян келтіреді. (Айтқазиев, 2020). Соңғы жылдары киберқылмыс әрекеттері айтарлықтай күрделеніп, әртүрлі әдістермен жүзеге асырылады: фишинг**,** вирус**,** трояндық бағдарламалар**,** шпиондық бағдарламалар секілді зиянды бағдарламалар арқылы пайдаланушылардың жеке мәліметтері ұрланады. (Нұртаев, 2019). Бұл, әсіресе, қаржылық ақпараттың ұрлануы мен жеке деректердің заңсыз пайдаланылуына әкеледі. Бұл мәселелер тек жеке адамдарға ғана емес, бүкіл қоғам мен мемлекетке қатысты.

Киберқылмыстың негізгі түрлерін талдайтын болсақ, олардың арасында ең кең таралғандары мыналар:

Фишинг - бұл – электрондық пошталар немесе басқа да хабарламалар арқылы адамды сендіріп, олардың жеке ақпараттарын (құпиясөздер, банктік шот нөмірлері, кредит карталарының деректері) алдау жолымен ұрлау. Қазіргі заманғы фишинг схемалары өте жоғары деңгейде жасалады, сондықтан оларды тану кейде қиынға соғады.

Зиянды бағдарламалар - Бұл бағдарламалар жүйеге кіріп, ақпаратты жояды немесе ұрлайды. Атап айтқанда, вирус, трояндық аттар, шпиондық бағдарламалар, ransomware сияқты зиянды бағдарламалар жеке және корпоративтік деректерге қол жеткізуге мүмкіндік береді.

DDoS-шабуылдар – бұл түрі distributed denial-of-service (DDoS) деп аталады және оның мақсаты – белгілі бір жүйені немесе вебсайтты артық трафикпен «тоқтату». Бұл шабуылдар бизнес-операцияларды тоқтатып, компаниялар мен ұйымдар үшін үлкен шығындарға әкелуі мүмкін.

Әлеуметтік инженерия – әлеуметтік инженерия – адамдарды алдап, жүйеге кіруге рұқсат алу үшін қолданылатын әдістердің жиынтығы. Бұл әдістер психологиялық манипуляцияға негізделеді, мысалы, телефон арқылы немесе электрондық поштамен жұмыс істейтін адамдарға жүйелер мен деректерге кіру рұқсатын алу үшін жасалатын әрекеттер.

Криптовалюталық алаяқтықтар – Қазіргі кезде криптовалюталардың таралуы, сондай-ақ блокчейн технологиясының дамуы алаяқтардың жаңа схемаларға кіруіне мүмкіндік береді. Олардың арасында криптокрандар арқылы фишинг, инвестициялық алаяқтықтар, ICO (Initial Coin Offering) алаяқтықтары өте жиі кездеседі.

Құпия деректердің ұрлануы – бұл қылмыс жеке ақпараттарды немесе бизнеске қатысты құпия деректерді заңсыз жолмен алу арқылы жасалады. Ол қаржылық деректер, құжаттар, патенттер және басқа да интеллектуалдық меншіктің ұрлануына әкелуі мүмкін.

Киберқылмыскерлер жаңа әдістерді қолдана отырып, әрдайым жаңарып отырады. Бұл орайда, қазіргі таңда бірқатар ұйымдасқан киберқылмыстық топтар жасалған шабуылдарын кеңейтуде және жаңа тактикалар ойлап табуда. Мұндай қылмыстардың қайталану ықтималдығы жоғары және олардың салдары өте ауыр болуы мүмкін.

Деректердің қауіпсіздігі — әртүрлі саладағы ұйымдар мен жеке тұлғалардың негізгі приоритетіне айналған маңызды мәселе. Әсіресе, цифрлық мәліметтермен жұмыс істейтін ұйымдар үшін ақпаратты қорғаудың маңызы зор. Мысалы, мемлекеттік органдардың немесе ірі кәсіпорындардың құпия ақпараттарын сақтау мен қорғау талаптары өте жоғары. Киберқылмыскерлер бұл ақпаратты ұрлап, заңсыз пайдалану арқылы ірі экономикалық шығын тудырып, бизнес пен қоғамның тұрақтылығына нұқсан келтіреді.[2]

Деректердің қауіпсіздігін қамтамасыз етудің негізгі шаралары:

Қауіпсіздік саясатын әзірлеу Әрбір ұйым өздерінің деректерін қорғау үшін нақты қауіпсіздік саясатын әзірлеуі тиіс. Бұл саясат ақпараттық қауіпсіздік шараларын, қорғалатын деректерді анықтауды, олардың қауіпсіздігін тексеруді, оқытуды және басқа да қауіпсіздік шараларын қамтуы тиіс.

Шифрлау – деректерді рұқсатсыз қолжетімділіктен қорғаудың ең тиімді әдісі болып табылады. Кез келген құпия ақпаратты шифрлау арқылы, ақпаратты тек рұқсат етілген пайдаланушы ғана аша алады. Бұл технология жеке адамдардың деректерін, сондай-ақ ұйымдардың ішкі құжаттарын қорғауға өте маңызды.

Мектеппен қызметкерлерді оқыту Әрбір қызметкердің киберқауіпсіздік бойынша сауаттылығын арттыру ұйым үшін маңызды. Олар фишингтік хаттарды тану, құпиясөздерді қауіпсіз сақтау және жүйеге рұқсатсыз кіру әрекеттерінен сақ болу туралы білімді болуы керек.

Қауіпсіздік бағдарламаларын қолдану Антивирустық бағдарламалар мен брандмауэрлер жүйеге сыртқы шабуылдарды болдырмауға көмектеседі. Бұл жүйелер зиянды бағдарламалардан қорғануды қамтамасыз етеді және қауіпсіздік шараларын арттырады.

Құпия деректерге рұқсатты шектеу Барлық ұйымдар құпия ақпаратқа рұқсатты шектеу жүйесін енгізуі керек. Бұл жүйе пайдаланушылардың қандай деректерге қолжетімділік

алатынын анықтауға мүмкіндік береді. Осылайша, тек қажетті адамдар ғана белгілі деректерге қол жеткізе алады.[4]

Қауіпсіздікке арналған резервтік көшіру Жүйелер мен деректерге кез келген шабуыл жасалған жағдайда резервтік көшіру өте маңызды болып табылады. Бұл шара деректердің жоғалуын болдырмайды және жүйенің қалыпты жұмысын сақтап қалуға мүмкіндік береді.

Цифрлық қауіпсіздікті қамтамасыз ету үшін заманауи құралдар мен әдістер қажет. Осы орайда, криптография**,** көпфакторлы аутентификация**,** брандмауэрлар **мен** желілік мониторинг сияқты технологиялар ақпараттың қауіпсіздігін қорғауға көмектеседі. Бірақ бұл құралдармен ғана мәселені шешу мүмкін емес. Қазіргі уақытта киберқылмыс пен ақпараттық қауіптерге қарсы күресу тек техникалық шаралармен шектелмейді, ол бүкіл қоғамның санасы мен жауапкершілігіне де байланысты.

Цифрлық қауіпсіздік мәдениеті — бұл қоғамның цифрлық кеңістіктегі қауіпсіздікті қамтамасыз етуге деген ұжымдық жауапкершілігін қалыптастыруға бағытталған процесс. Қоғамның әрбір мүшесі ақпараттық қауіпсіздікті қамтамасыз ету жолында белсенді түрде жұмыс істеуі қажет. Бұл үшін адамдарға интернеттегі қауіптер туралы түсінік беру, жеке деректерді қорғау жолдарын үйрету, сондай-ақ дұрыс онлайн әрекеттер жасау дағдыларын қалыптастыру керек. Сонымен қатар, жастар мен балалардың санасында цифрлық қауіпсіздік мәселелерін ерте жастан бастап дұрыс қалыптастыру өте маңызды.

Оның үстіне, киберқылмысты жеңу үшін халықаралық ынтымақтастық та өте маңызды рөл атқарады. Интернет кеңістігіндегі қылмыстар көбінесе елдер шекарасын елемей жүзеге асады, сондықтан халықаралық деңгейде ортақ заңдар мен реттеуші шараларды қабылдау қажет. Әрбір мемлекет өз ішінде киберқылмысқа қарсы заңдар мен нормативтерді күшейтсе, әлем бойынша ақпараттық қауіпсіздікті қорғаудың тиімділігін арттыруға мүмкіндік береді. Киберқылмысқа қарсы халықаралық ұйымдар мен коалициялар құру, бірлескен күш-жігер арқылы ақпараттық кеңістікті қорғау шараларын жүзеге асыру өте маңызды.

Цифрлық қауіпсіздік тек техникалық құралдар мен заңдармен шектелмейді. Қазіргі қоғамда ақпараттық қауіпсіздікті қамтамасыз ету үшін әрбір адам, ұйым және мемлекет өздерінің цифрлық қауіпсіздікке деген жауапкершілігін сезініп, бірігіп жұмыс істеуі керек. Цифрлық мәдениет пен қауіпсіздік — бұл тек ақпараттық технологиялардың мамандары ғана емес, барлық қоғам мүшелері қатысуы тиіс кешенді мәселе. Осы тұрғыда, цифрлық сауаттылықты арттыру**,** киберқылмысқа қарсы күресті жүзеге асыру, жаңа технологияларды қорғаудың тиімді жолдарын табу – қазіргі қоғамның алдында тұрған басты міндеттер болып табылады.[3]

Бұл мақалада киберқылмыстың негізгі түрлері, олардың қоғам мен бизнеске тигізетін зияны, деректерді қорғаудың заманауи әдістері мен құралдары, сондай-ақ цифрлық қауіпсіздікті қамтамасыз ету үшін мемлекеттік және халықаралық деңгейдегі ынтымақтастықтың маңызы қарастырылады. Сонымен қатар, киберқылмысқа қарсы күресте цифрлық қауіпсіздік мәдениетін қалыптастыру, қоғамның цифрлық сауаттылығын арттыру және құқықтық реттеу мәселелері де талқыланады. Осы мәселелерді шешу үшін тек техникалық шаралар жеткіліксіз, бүкіл қоғамның санасы мен әрекеті маңызды рөл атқарады. Әр азаматтың цифрлық жауапкершілігі, ұйымдардың қауіпсіздікті қамтамасыз етуі және халықаралық ынтымақтастықтың күшеюі біздің заманымызда цифрлық әлемдегі қауіпсіздікті қорғаудың басты құралы болуы тиіс.

Қазіргі цифрлық дәуірде ақпараттық қауіпсіздік пен киберқылмыс мәселелері қоғамның барлық деңгейінде өзекті бола түсті. Интернеттің кеңеюі мен ақпараттық технологиялардың дамуы жаңа мүмкіндіктер әкелсе де, олармен бірге сан түрлі қауіптер мен қатерлер де пайда болды. Киберқылмыс әлемнің түкпір-түкпірінде жеке тұлғалар мен ұйымдарға зор экономикалық және репутациялық зиян келтіріп, ақпараттық қауіпсіздікке қатысты жаңа талаптарды қойды. Осыған байланысты деректердің қауіпсіздігі маңызды әрі өзекті мәселеге айналды.

Киберқылмысқа қарсы күрес тек техникалық құралдар мен құқықтық шаралармен шектелмейді. Бұл бүкіл қоғамның жауапкершілігіне қатысты мәселе болып табылады. Құпия

ақпараттарды қорғау, жеке деректердің қауіпсіздігін қамтамасыз ету және киберқылмыстың алдын алу үшін әрбір азамат цифрлық қауіпсіздікке қатысты білімді болуға тиіс. Сондай-ақ, цифрлық қауіпсіздік мәдениетін қалыптастыру және ақпараттық кеңістікті қорғауға бағытталған халықаралық ынтымақтастықтың маңызы зор. Әрбір мемлекет өз ішіндегі заңнамаларды күшейтіп, халықаралық деңгейде бірлескен күш-жігерді ұйымдастыру қажет.

Осы тұрғыда, тек технологиялық шешімдер жеткіліксіз. Цифрлық сауаттылықты арттыру, қауіпсіздік туралы ақпараттандыру және жауапкершілікті арттыру арқылы цифрлық әлемдегі қауіптерге қарсы тұруға болады. Криптография**,** көпфакторлы аутентификация сияқты құралдар ақпараттық қауіпсіздікті қорғауға көмектескенімен, тек техника ғана емес, қоғамның әрбір мүшесінің санасы мен жауапкершілігі маңызды рөл атқарады.

Қорыта айтқанда, Қазіргі уақытта киберқылмыс пен деректердің қауіпсіздігі әлемдегі ең маңызды мәселелердің бірі болып отыр. Әлемдік цифрлық инфрақұрылымның қарқынды дамуы және ақпараттық технологиялардың үнемі өзгеріп отыруы бізді жаңа қауіптермен бетпе-бет келтіруде. Киберқылмыскерлер әртүрлі тәсілдер мен технологияларды қолданып, ұйымдар мен жеке тұлғалардың деректерін ұрлап, үлкен қаржылық және ақпараттық шығындарға алып келеді. Бұл өз кезегінде ақпараттық қауіпсіздік саласындағы шараларды одан әрі жетілдіру қажеттілігін туындатады.

Деректерді қорғау, кибершабуылдардың алдын алу, қауіпсіздік жүйелерін дамыту – қазіргі заманғы қоғамның басты міндеті. Бұған тек мемлекеттік органдар ғана емес, сондай-ақ жеке сектор мен әрбір азамат та жауапты болуы тиіс. Ақпараттық қауіпсіздік мәдениетін қалыптастыру, киберқауіптер туралы білім беру және күнделікті өмірде қауіпсіздік шараларын қабылдау, кибершабуылдардың алдын алудың ең тиімді жолдары болып табылады.

Киберқылмысқа қарсы күрестің маңызды аспектілерінің бірі – ақпараттық технологиялардың дамуына ілесу және оларды тиімді пайдалану. Қазіргі таңда ақпараттық қауіпсіздік жүйелерінің кешенді түрде қолданылуы, мысалы, шифрлау, аутентификация, антивирустық бағдарламалар, резервтік көшірмелер жасау сияқты шаралар маңызды орын алады. Әрбір ұйым мен жеке тұлға осындай шараларды тұрақты түрде қолданып, өз қауіпсіздігін қамтамасыз етуі керек.

Қоғамның ақпараттық қауіпсіздікке деген жауапкершілігі барынша жоғары болуы қажет. Әсіресе, киберқылмыскерлердің құралдары мен әдістері үнемі жаңарып, күрделене түсетіндіктен, олардан қорғанудың да тәсілдері үнемі жаңартылып отыруы тиіс. Бұл тұрғыда киберқұқық қорғау, халықаралық ынтымақтастық және құқықтық реттеу жүйелерін жетілдіру маңызды рөл атқарады.

Қазақстанда да киберқауіпсіздік мәселесіне үлкен көңіл бөлінуде. "Цифрлық Қазақстан" мемлекеттік бағдарламасы аясында көптеген бастамалар қолға алынып, жаңа технологиялар мен шешімдер енгізілуде. Осыған байланысты, киберқауіпсіздік саласында білім деңгейін көтеру, инновациялық шешімдер енгізу, заңнамалық деңгейде киберқылмыстарды қатаң бақылауға алу — еліміздің ақпараттық қауіпсіздігін қамтамасыз етудің негізгі жолдары.[5]

Ақырында, киберқауіпсіздік — бұл тек жеке немесе ұлттық деңгейде ғана шешілетін мәселе емес. Ол әлемдік деңгейде үйлесімді әрі жан-жақты күресуді қажет ететін құбылыс. Тек бірлескен күш-жігер мен халықаралық ынтымақтастық арқылы ғана біз киберқылмысқа қарсы тиімді қарсы тұра аламыз. Бұл орайда, әрбір адам мен ұйымның қауіпсіздікке деген көзқарасын өзгерту және жауапкершілікті арттыру — болашақтағы қауіпсіз цифрлық әлем құрудың басты факторларының бірі болып табылады.

Ақпараттық қауіпсіздікке қатысты ұстаным мен білімнің жоғары деңгейі ғана кибершабуылдар мен ақпараттық дағдарыстарды болдырмауға мүмкіндік береді. Тек осы тұрғыда үздіксіз жұмыс істей отырып, біз қауіпсіз цифрлық болашақты қамтамасыз ете аламыз.

Ұсыныстар:

1.Цифрлық қауіпсіздік мәдениетін қалыптастыру**:** Мектептер мен жоғары оқу