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

- мемлекеттік қызметтің тұрақсыздануы;
- экономикалық зиян келтіру;
- ұлтаралық және конфессияаралық қатынастарды қиындату, ұлтаралық араздықты қоздыру;
- қасақана әскери қақтығыс тудыру;
- саяси жүйенің өзгеруі.

Ең жалпы көзқарас халықаралық қылмыстар мен халықаралық сипаттағы қылмыстарды қылмыстардың субъектісі мен объектісі тұрғысынан қарастыру болып табылады. Дәл осы критерийлер халықаралық қылмыстарды анықтауда іргелі болып табылады. Олардың көмегімен халықаралық қылмыстар мен терроризм қылмыстарын салыстыруға да болады.

Пайдаланылған әдебиеттер:

1. Еуропа Кеңесінің терроризмнің алдын алу туралы Конвенциясы (CETS N 196) (Варшава қаласында 16.05.2005 ж. жасалған).
2. Терроризмге, сепаратизмге және экстремизмге қарсы күрес туралы Шанхай конвенциясы (Шанхай, 15 маусым 2001 ж.).
3. Терроризмді қаржыландыруға қарсы күрес туралы халықаралық конвенция (БҰҰ Бас Ассамблеясының 1999 жылғы 9 желтоқсандағы 54/109 қарарымен қабылданған).
4. Тәуелсіз Мемлекеттер Достастығына қатысушы мемлекеттердің терроризмге қарсы күрестегі ынтымақтастығы туралы шарт (Минск, 4 маусым 1999 ж.).
5. Бомбалық терроризмге қарсы күрес туралы халықаралық конвенция (Нью-Йорк, 15 желтоқсан 1997 ж.).
6. Әуе кемелерін заңсыз басып алуға қарсы күрес туралы Конвенция (Гаага, 16 желтоқсан 1970 ж.) / / шет мемлекеттермен жасалған қолданыстағы шарттар, келісімдер мен конвенциялар жинағы, М., 1974 ж., т. б. XXVII.
7. Азаматтық авиация қауіпсіздігіне қарсы бағытталған заңсыз актілерге қарсы күрес туралы Конвенция (Монреаль, 23 қыркүйек 1971 ж.) / / КСРО шет мемлекеттермен жасасқан қолданыстағы шарттар, келісімдер мен конвенциялар жинағы, М., 1975 ж., т. XXIX.

ӘОЖ 343.3/.7

КИБЕРҚЫЛМЫСТЫЛЫҚ ЖӘНЕ ОНЫҢ ТҮРЛЕРІ ОЛАРДЫ АЛДЫН АЛУ ЖӘНЕ КҮРЕСУ ШАРАЛАРЫ

Қойлан Әлібек Серікұлы
alibek.koylan@bk.ru
Л.Н.Гумилев атындағы ЕҰУ, заң факультеті «Құқықтану» мамандығының 3 курс студенті
Астана, Қазақстан
Ғылыми жетекші - Э.А. Ашимова з.ғ.к., доцент,

Қазіргі уақытта «киберқылмыстылық» түсінігі «компьютерлік қылмыс» түсінігімен қатар қолданылып жүр және де осы ұғымдар синонимдер ретінде де жиі қолданылады.

Шын мәнінде осы ұғымдар мағынасы жағынан бір-біріне жақын болып келеді. Дегенмен, оларды синонимдес деп айтуға болмайды. Біздің пікіріміз бойынша, «киберқылмыстылық» түсінігінің (ағылшын нұсқасында - cybercrime) мағынасы

«компьютерлік қылмыстылық» ұғымымен (com¬puter crime) салыстырғанда анағұрлым кең және ақпараттық кеңістікте жасалатын қылмыс сияқты құбылыстың мәнін нақтырақ ашады. Мысалы, Оксфорд түсіндірме сөздігінде «cyber-» қосымшасы күрделі сөздің бір бөлігі ретінде анықталған. Ол «ақпараттық технологияларға, Интернет желісіне, виртуалдық шынайылыққа жататын» деген мағынаны білідреді. Кембридж сөздігінде де осыған ұқсас мағына берілген: «cyber-» сөзі «компьютерлерді пайдалануды қамтитын немесе компьтерлерге, әсіресе Интернет желісіне қатысты». Бұл ретте Кембридж сөздігінде мысал ретінде «cybercrime» - киберқылмыстылық (киберқылмыс) сөзі келтірілген [1]. Осылайша, «cybercrime» - бұл компьютерлерді пайдаланумен де, ақпараттық технологияларды және жаһандық желілерді пайдаланумен де байланысты қылмыстылық. Бұл ретте «computer crime» термині компьютерлерге немесе компьютерлік деректерге қарсы жасалатын қылмыстарға ғана қатысты болып келеді.

Интернеттің біздің күнделікті өмірімізге терең енуі жаңа мүмкіндіктерге, сонымен қатар жаңа қауіптерге әкелді. Олардың ішіндегі ең маңыздыларының бірі-интернеттегі алаяқтық. Қазіргі цифрлық әлемде ол жеке қауіпсіздікке де, қаржылық әл-ауқатқа да қауіп төндіретін біздің шындықтың ажырамас бөлігіне айналды.

Интернеттегі алаяқтық -бұл желі арқылы жүзеге асырылатын алаяқтық пен алдаудың кең спектрі[4]. Бұл фишингтік хаттар, кибершабуылдар, зиянды бағдарламалар, жалған веб-сайттар, криптовалютаны қолданатын алаяқтық схемалар және т.б. болуы мүмкін. Күн сайын миллиондаған адамдар жеке деректерін, қаржысын немесе тіпті бүкіл өмірлік жинақтарын жоғалтып, осындай қылмыстардың құрбаны болады.

Бұл мақалада біз интернеттегі алаяқтықтың әртүрлі түрлерін қарастырамыз, олардың негізгі белгілерін анықтаймыз және өзіңізді осындай шабуылдардан қалай қорғауға болатындығын білеміз. Біз бірге киберқылмыстың құрбаны болу қаупін азайту үшін интернетті саналы және қауіпсіз пайдалануға тырысамыз.

Ішкі істер органдары интернет алаяқтыққа қарсы қандай іс-шараларды қолға алуда? Алаяқтардың арбауына түсіп қалмау үшін не істеу қажет? Ел-жұрт неліктен қарапайым қауіпсіздік шараларын сақтай бермейді? Осы және өзге де сұрақтарға онлайн-брифинг барысында жауап берген ІІМ Криминалдық полиция департаменті бастығыны Қанат Нұрмағамбетов: «Интернет алаяқтықтың ең басты ерекшелігі – жалпақ жұрттың бәріне қатысты жасалатындығында», деп атап өтті.

Интернеттің мүмкіндігін қылмыстық іс-әрекеттерін жүзеге асыру үшін оңтайлы пайдаланып жүрген алаяқтардың әдіс-тәсілдері күн сайын өзгеріп, жаңарып отырады. «Уақыт талабынан олар да қалыс қалмай келеді», деген спикер ғаламтордағы әккілердің, әсіресе әлеуметтік желілерді ұтымды пайдаланып отырғанын мәлімдеді. «Әдетте алаяқтар әлеуметтік желілерге жалған интернет хабарландырулар орналастырады немесе аккаунт пен арнайы бет ашып, сайт жасап алады.

Интернеттегі алаяқтық: цифрлық әлемде өзіңізді қалай қорғауға болады? [6]

Қазіргі цифрлық әлем Байланыс, жұмыс және ойын-сауық үшін үлкен мүмкіндіктер ұсынады, бірақ ол сонымен қатар киберқылмыстың әртүрлі түрлеріне, соның ішінде интернет-алаяқтыққа арналған алаңға айналды. Бұл ұғым пайдаланушының жеке ақпаратына, қаржысына және басқа ресурстарына қол жеткізу мақсатында интернет арқылы жүзеге асырылатын алаяқтық пен алдаудың кең спектрін білдіреді. Бұл мақалада біз интернеттегі алаяқтықтың бірнеше түрін қарастырамыз және өзіңізді осы қауіптерден қорғаудың нақты стратегияларын ұсынамыз.

Интернеттегі алаяқтық түрлері:[4]

Фишингтік шабуылдар-бұл зиянкестер пайдаланушыларды алдау және олардың құпия сөздері, несие карталарының нөмірлері немесе әлеуметтік қауіпсіздік нөмірлері сияқты жеке ақпаратын алу мақсатында Заңды және сенімді болып көрінетін электрондық хабарламалар жібереді немесе веб-сайттар жасайды. Бұл шабуылдар банктерден, интернет-провайдерлерден, интернет-дүкендерден немесе пайдаланушылар күнделікті өзара әрекеттесетін басқа ұйымдардан жіберілген электрондық хаттар түрінде келуі мүмкін.

Көбінесе фишингтік электрондық пошталарда ұйымдардың ресми сайттарымен бірдей көрінуі мүмкін жалған веб-сайттарға сілтемелер бар. Пайдаланушылардан жеке деректерін енгізуді немесе тіпті пайдалы қолданба немесе файл ретінде жасырылған зиянды бағдарламалық құралды жүктеп алуды сұрауы мүмкін.

Фишингтік шабуылдар әдетте әлеуметтік инженерияны қолданатынын ескеру маңызды, яғни пайдаланушылардың эмоцияларын немесе сенімдерін манипуляциялау, оларды ұсынылған нұсқауларды орындауға сендіру. Мысалы, зиянкестер пайдаланушылар болжамды мәселелер мен қауіптерді болдырмау үшін өз деректерін ұсынудың шұғыл қажеттілігін сезінетін жағдайларды тудыруы мүмкін.

Өзіңізді фишингтік шабуылдардан қорғау үшін электрондық хаттарды, әсіресе күдікті сілтемелері бар немесе жеке деректерді беруді сұрайтындарды ашқанда абай болу керек. Ақпаратты енгізбес бұрын веб-сайттардың URL мекен-жайларын тексеріп, шабуылға ұшырау қаупін азайту үшін антивирустық бағдарламалық жасақтама және спам сүзгілері сияқты қорғаныс механизмдерін қолданыңыз. Сонымен қатар, шабуылдаушылар пайдалануы мүмкін осалдықтарды жою үшін құрылғылардағы бағдарламалық жасақтама мен операциялық жүйелерді үнемі жаңартып отыру керек.

Жалған веб - сайттар-бұл пайдаланушыларды алдау және олардың жеке ақпаратын немесе қаржылық деректерін алу мақсатында зиянкестер жасаған веб-беттер немесе сайттар. Бұл сайттар белгілі компаниялардың, банктердің немесе ұйымдардың ресми домендеріне өте ұқсас жалған домендік атаулармен жасалуы мүмкін. Жалған веб-сайттардың мақсаты көбінесе пайдаланушылардан логиндер, парольдер, несие карталарының нөмірлері және басқа да сезімтал ақпаратты алу болып табылады.

Көбінесе жалған веб-сайттар танымал банктерге, онлайн-дүкендерге, төлем жүйелеріне немесе басқа танымал онлайн қызметтерге еліктеу үшін жасалуы мүмкін. Олар мүмкіндігінше сенімді көріну үшін түпнұсқа сайттың дизайнын, логотиптерін және интерфейсін имитациялай алады.

Әдетте, пайдаланушылар жалған веб-сайттарға электрондық пошта сілтемелері, әлеуметтік медиа хабарламалары, жарнамалар немесе іздеу жүйелері арқылы бағытталуы мүмкін. Мысалы, шабуылдаушылар электрондық поштаны жібере алады, онда пайдаланушылардан өз деректерін жаңарту үшін веб-сайтқа сілтеме жасауды сұрайды және бұл веб-сайт олардың ақпаратын ұрлау үшін жалған болады.

Өзіңізді жалған веб-сайттардан қорғау үшін интернетте шарлау кезінде абай болу керек. Сезімтал ақпаратты енгізбес бұрын веб-сайттардың URL мекенжайларын тексеріңіз. Веб-сайттың қауіпсіз қосылымды (HTTPS) пайдаланатынына және жарамды қауіпсіздік сертификаты бар екеніне көз жеткізіңіз. Сонымен қатар, егер Сізге жеке ақпарат немесе қаржылық деректер ұсынылса, электрондық пошта немесе жарнама сілтемелеріне өтпей, компанияның немесе ұйымның ресми веб-сайтына тікелей хабарласқан дұрыс.

Кибершабуылдар - бұл компьютерлік жүйелерге, желілерге немесе құрылғыларға рұқсатсыз кіруге, ұрланған деректерге қол жеткізуге, зиян келтіруге немесе тіпті шабуылға ұшыраған нысанды бақылауға бағытталған мақсатты әрекеттер.

Кибершабуылдар вирустар, трояндық бағдарламалар, құрттар, DDoS шабуылдары (қызмет көрсетуден бас тарту шабуылдары) және т.б. сияқты әртүрлі әдістерді қамтуы мүмкін. Кибершабуылдардың мақсаттары қаржылық бопсалаудан бастап құпия ақпаратты ұрлауға немесе жай вандализмге дейін болуы мүмкін.

Зиянды бағдарламалар: малициозды бағдарламалық жасақтама немесе малвар деп те аталатын зиянды бағдарламалар-бұл компьютерлік жүйелерге немесе құрылғыларға еніп, зиян келтіруге арналған бағдарламалық жасақтама.

Бұл бағдарламаларға вирустар, трояндық бағдарламалар, құрттар, шпиондық бағдарламалар, руткиттер және деректерді ұрлау, зиянды бағдарламаларды орнату, пайдаланушылардың әрекеттерін бақылау және т. б. үшін пайдалануға болатын бағдарламалардың басқа түрлері кіруі мүмкін.

Зиянды бағдарламалар көбінесе вирус жұққан веб-сайттар, электрондық пошталар, зиянды сілтемелер немесе бағдарламалық жасақтаманың осалдықтары арқылы таралады. Олар пайдаланушыларды алдау және олардың құрылғыларын жұқтыру үшін пайдалы қолданбалар немесе файлдар ретінде ұсынылуы мүмкін.

Кибершабуылдар мен зиянды бағдарламалардан қорғау үшін сенімді антивирустық бағдарламалық жасақтаманы пайдалану, операциялық жүйелер мен бағдарламалық жасақтаманы үнемі жаңартып отыру, электрондық пошталардағы тіркемелерді және сенімсіз көздерден алынған сілтемелерді Мұқият ашу, веб-сайттарға кіріп, интернеттен файлдарды жүктеу кезінде мұқият болу маңызды. Сондай-ақ, зиянды бағдарламалық жасақтама сәтті шабуыл немесе оқиға болған жағдайда шығындарды азайту үшін маңызды деректердің сақтық көшірмесін үнемі жасау қажет

Өзіңізді қалай қорғауға болады:

1. Киберқауіпсіздік негіздерін үйрету: киберқауіпсіздік негіздерін үйрету ықтимал қауіптерді жақсырақ түсінуге және оларды тануды үйренуге көмектеседі.
2. Электрондық хаттарды ашып, сілтемелерді басқан кезде абай болыңыз: электрондық поштаны жіберушінің мекен-жайын және олардағы сілтемелерді нұқу немесе жеке ақпарат беру алдында мұқият тексеріңіз.
3. Күшті құпия сөздерді және екі факторлы аутентификацияны пайдаланыңыз: әрбір онлайн тіркелгіңіз үшін бірегей және күрделі құпия сөздерді пайдаланыңыз және қосымша қорғаныс қабаты үшін мүмкіндігінше екі факторлы аутентификацияны қосыңыз.
4. Бағдарламалық жасақтаманы үнемі жаңартып отырыңыз: құрылғылардағы амалдық жүйелер мен бағдарламаларды жаңарту зиянкестер қолдануы мүмкін осалдықтарды жабуға көмектеседі.

Интернеттегі алаяқтық-бұл барлық интернет қолданушылары үшін үлкен қауіп. Дегенмен, дұрыс білім мен практикалық сақтық шаралары арқылы сіз интернеттегі алаяқтықтың құрбаны болу қаупін азайта аласыз. Өзіңізді және деректеріңізді қорғау үшін онлайн ортада өзара әрекеттесу кезінде оқудың және сақтықтың маңыздылығын есте сақтаңыз.

Пайдаланылған әдебиеттер тізімі:

1. Cambridge AdvancedLearner's Dictionary [Electronic recourse]. — URL-дан қолжетімді: http://dictionarv.cambridge.org [Кіру күні: 29.12.2018жыл]
2. Қазақстан Республикасының Конституциясы https://www.akorda.kz/ru/official_documents/constitution
3. Мартин, Майкл А. " сандық шабуыл және одан қорғаныс." Butterworth-Heinemann, 2015.
4. Пискорская, Н. В. және т. б. "Интернет-алаяқтық: алдын алу және қорғау."Оқу құралы. 2019.
5. Сталлман, Ричард М. " тірі этикет: цифрлық әлемде қалай өмір сүруге болады." GNU Press, 2019
6. Стоунер, Марк. "Киберқауіпсіздік: ақпаратты, цифрлық деректерді және компьютерлік желілерді қорғау." Routledge, 2017.
7. Уайтхед, Нил, және Джон М. Фредрикс. "Киберқауіпсіздікке кіріспе." CRC Press, 2018.
8. Шнайер, Брюс. "Қауіпсіздік криптографиясы: принциптері мен практикасы." John Wiley & Sons, 2017.