Темірлан Нұрланұлы Умыржан – старший преподаватель кафедры «Техническая физика и теплоэнергетика»; Университет имени Шакарима города Семей, Республика Казахстан; e-mail: timirlan-95@mail.ru.

Жан Касенович Алдажуманов – старший преподаватель кафедры «Техническая физика и теплоэнергетика»; Университет имени Шакарима города Семей, Республика Казахстан; e-mail: jean1974@mail.ru.

Авторлар туралы мәліметтер

Михаил Вячеславович Ермоленко* – техника ғылымдарының кандидаты, «Семей қаласының Шәкәрім атындағы университеті» Қазақстан Республикасы;«Техникалық физика және жылу энергетикасы» кафедрасының аға оқытушысы; e-mail: tehfiz@mail.ru. ORCID: 0000-0002-1677-8023.

Ольга Александровна Степанова – техника ғылымдарының кандидаты, доцент, «Семей қаласының Шәкәрім атындағы университеті» Қазақстан Республикасы;«Техникалық физика және жылу энергетикасы» кафедрасының меңгерушісі; e-mail: aug11@mail.ru. ORCID: 0000-0001-5221-1772.

Николай Александрович Демин – «Теплокоммунэнерго» МКК техникалық директоры, Қазақстан Республикасы; e-mail: mailto:nik.dyomin87@mail.ru.

Темірлан Нұрланұлы Умыржан – «Семей қаласының Шәкәрім атындағы университеті» Қазақстан Республикасы;«Техникалық физика және жылу энергетикасы» кафедрасының аға оқытушысы;e-mail: timirlan-95@mail.ru.

Жан Касенович Алдажуманов – «Семей қаласының Шәкәрім атындағы университеті» Қазақстан Республикасы;«Техникалық физика және жылу энергетикасы» кафедрасының аға оқытушысы;e-mail: jean1974@mail.ru.

Information about authors

Mikhail Yermolenko* – Candidate of Technical Sciences, Senior Lecturer of the Department «Technical physics and heat power engineering »; Shakarim University of Semey, Republic of Kazakhstan; e-mail: tehfiz@mail.ru. ORCID: 0000-0002-1677-8023.

Olga Stepanova – Candidate of Technical Sciences, Associate Professor, Head of the Department « Technical physics and heat power engineering »; Shakarim University of Semey, Republic of Kazakhstan; e-mail: aug11@mail.ru. ORCID: 0000-0001-5221-1772.

Nikolay Demin – Technical Director of the State Enterprise «Teplokommunenergo», Republic of Kazakhstan; e-mail: mailto:nik.dyomin87@mail.ru.

Temirlan Umyrzhan – senior lecturer of the department «Technical physics and heat power engineering»; Shakarim University of Semey, Republic of Kazakhstan; e-mail: timirlan-95@mail.ru.

Jean Aldazhumanov – senior lecturer of the department « Technical physics and heat power engineering»; Shakarim University of Semey, Republic of Kazakhstan; e-mail: jean1974@mail.ru.

Материал поступил в редакцию 10.03.2023 г.

DOI: 10.53360/2788-7995-2023-1(9)-4

ҒТАХР: 50.49.37

Г.Е. Жидекұлова*, А.Д. Абдувалова, С.Б. Бекболатов
М.Х. Дулати атындағы Тараз өңірлік университеті
Тараз қаласы Сүлейменов көшесі, 7
*e-mail: gul2006@mail.ru

ӘЛЕУМЕТТІК ЖЕЛІЛЕРДЕН БОЛАТЫН ҚАУІПТЕРДІ БАҚЫЛАУ АРҚЫЛЫ ҚОРҒАНУ МҮМКІНДІКТЕРІ

Андатпа: *Қазіргі таңда әлем халқының екіден бірі Вконтакте, Whatsapp, Instagram,Skype, Periscope тағы да басқа әлеуметтік желілерде отырады. Ең жаманы, әлеуметтік желі адам өміріне де қауіп төндіру мүмкін. Көп жағдайларда есірткі және*

психотроптық заттардың заңсыз айналымы осы әлеуметтік желілер арқылы таралуы мүмкін, сондықтан виртуалды кеңістіктегі ақпаратқа сенім проблемаларын зерттеуге ерекше мән беру керек.

Әлеуметтік желілерге талдау жасау бүкіл әлем бойынша қолға алынып жатқан бағыт болғандықтан, көптеген бағдарламалардың да шығуы таңғаларлық емес, сол сияқты біздің қоғамға керекті түрлі домендердегі мәтіндерді талдап, бүкіл виртуалды әлем бойынша бақылау жасауға өрекет ететін Python программалау тілін қолдану арқылы жүйе құру. Арнайы бағдарламаға керекті алгоритмдерді енгізу арқылы біз бұл мақсатқа жетуге болады.

Заңсыз әрекеттерді анықтау және алдын алу мақсатында әлеуметтік желілерді бақылауға арналған бағдарламалық жасақтама жасау арқылы, интернет арқылы ұйымдастырылатын қылмыстардың алдын алу және әлеуметтік желілерді бақылау мүмкіндіктерін ұйымдастыруды қарастырған.

Мақалада киберқауіптер түрлері мен олардан қорғану әдістері талқыланып және әлеуметтік желілерді бақылаудың программасы Python ортасында құрылған, оның нәтижелер көрінісі келтірілген. Алынған нәтижелер арқылы қауіп-қатер түрлерін анықтау арқылы алдын алу мүмкіндігін қарастырған.

Түйін сөздер: *компьютерлік жүйе, программа, қауіп-қатер,әлеуметтік желі, интернет, шабуылдар, IDS желілік, хост, шабуылдарды тану, Python.*

Кіріспе. Компьютерлік жүйелерге шабуыл жасау, бұл белгілі бір осалдықты іздейтін және қолданатын шабуылдаушының әрекеті. Осылайша, шабуыл жасай отырып қауіп төндіреді. Зиянды ниеті бар адамның қатысуымен жасалған іс-әрекет, қауіпті анықтауда кездесетін кездейсоқтықтың элементі деп қарауға болмайды, бірақ тәжірибе көрсеткендей, қасақана және кездейсоқ әрекеттерді ажырату мүмкін емес. Егер жақсы қорғаныс жүйесі болса, кез-келген қауіп-қатерлерге қарсы тұру мүмкіндігі жоғары болады.

Зерттеушілердің осы бағытқа деген қызығушылығының себебі ол бар әдістерден тыс түсіндірме модельдердің жаңа жиынтығы мен аналитикалық құралдарын ұсынады. Сонымен қатар, осы салада әлеуметтік өзара әрекеттесуі мен кез келген әлеуметтік жүйелерді сипаттайтын өте күрделі үлгілерді құруға мүмкіндік беретін жинақталған математикалық аппарат [1].

Желілердегі ақпарат ағындарын, әлеуметтік жағдайлардың даму жолдарын болжау, әлеуметтік рөлдерді орындау ерекшеліктерін түсіндіру, әлеуметтік алмасу процестерін талдау, әлеуметтік ұйымдардың құрылымдары мен олардың өзара әрекеттестігін игеру, экономикалық әлеуметтану, социометрия, бұқаралық коммуникация әлеуметтанулары және Интернет, тарих, саясат және халықаралық қатынастар мәселелерін шешу процестерін зерттеу және модельдеу үшін әлеуметтік желілерді талдау қолданылады [1].

Сонымен қатар, зерттеушілер әдетте қауіпсіздікке төнетін қатердің үш негізгі түрін ажыратады – бұл ашылу, тұтастық және қызмет көрсетуден бас тарту қаупінің болуы.

Ашылу қаупі, мұндай ақпарат ақпараттан хабары жоқ адамға белгілі болады. Компьютер қауіпсіздігі тұрғысынан қарағанда компьютер жүйесінде сақталған немесе бір жүйеден басқа жүйеге тасымалданатын құпия ақпаратқа қол жеткізген кезде ашылу қаупі туындайды. Оны кей уақытта "ашу" сөзінің орнына "ұрлық" немесе "ағып кету" сияқты терминдермен де қолданылады.

Тұтастықты қорғау есептеу жүйесінде сақталған немесе бір жүйеден екінші жүйеге тасымалданатын деректерді кез келген әдейі өзгертуді (өзгертуді немесе жоюды) қамтиды. Көбінесе мемлекеттік органдардың ашылу қаупіне, ал іскерлік немесе коммерциялық құрылымдар тұтастық қаупіне ұшырайды деп есептейді.

Қызмет көрсетуден бас тарту қаупінің болуы көп жағдайларда қызмет көрсету кезінде туындайды, нәтижесінде кейбір іс-әрекеттер бұғатталады, қатынаудағы есептеуіш ресурсы жүйесі блокталады. Шын мәнінде, блоктау тұрақты болып қалуы мүмкін, сондықтан сұралған ресурс ешқашан алынбайды немесе ол пайдасыз болып қалған кезде ресурстың кешігіп келуі мүмкін. Мұндай жағдайларда ресурс таусылды деп айтады [1].

Материалдар мен әдістер. Қазіргі әлемде киберқауіптер санының жылдам өсуі байқалады. Күнделікті әлемдік жаңалықтар лентасында жаңа оқиғалар туралы хабарлағанда, шабуылдардан құтылу амалдарын іздей бастайсың. Кәсіпорындар мен мемлекеттік органдар шабуылдарға төтеп беруге тырысуда, хакерлер қарапайым азаматтардың банктік шоттарын

босатып жатыр, сондықтан цифрлық әлемнің қауіптерінен сенімді қорғау негізгі қажеттілікке айналып отыр. Киберқауіпсіздіктің не екенін және оның әрқайсымыз үшін неліктен маңызды екенін түсінейік.

«Киберқауіпсіздік» және «ақпараттық қауіпсіздік» терминдері жиі синоним ретінде қолданып келеді. Алайда, негізінен, бұл терминдердің мағынасы өте әртүрлі және бірін-бірі алмастырмайды. Киберқауіпсіздік киберкеңістікте болатын шабуылдардан қорғауды білдірсе, ал ақпараттық қауіпсіздік аналог түрінде немесе цифрлық болсын, кез келген қауіп түрлеріне деректерді қорғауды білдіреді.

Интернет ортасында болатын қауіптерді атап кетейік:

– Интернетке тәуелді болу. Балаларда мұндай тәуелділік ойындарға деген шамадан тыс құмарлыққа байланысты болады. Бұл әсіресе көп ойын ойнайтын аудиториясы бар ойындарда кездеседі, мұнда ойыншылар бір-бірімен сөйлеседі, оқиға барысында өзара бір-бірімен өзара әрекеттестікте болады. Ойын баланың өмірінің ажырамас бөлігіне айналғанда дабыл қағу керек: ол тамақтан бас тартады, оқуға деген қызығушылығы болмайды, түнде ойнайды, ойнауға тыйым салынған жағдайда агрессия көрсетуге дейін барады. Балалардың интернетке тәуелділіктен шығуы өте қиынға соғады, сондықтан оның алдын-алу барысында ғана оның зияны аз болады.

– Кибербуллинг және троллинг. Желіде қарсыластарды нешетүрлі эмоцияға әкелетін жаппай агрессивті пайдаланушылары бар орта. Бұл ортада әркім лайықты жауап беріп, өзін-өзі қорғай алмайды. Қорқыту, келемеждеу, қорлау сияқты іс-әрекеттер баланың мінез-құлқының өзгеруіне қатты әсер етеді. Бұл жағдайларда бала тұйық, тітіркенгіш болады және өзіне,талантына деген сенімінен ажырайды. Ішкі дүниесіндегі уайымдар оқуына әсер етеді.

– Вирустары бар сайттар (фишинг, кеншілер). Зиянды вирус техникалық жабдықтарға зиян келтіріп, жұмысты баяулатады және жалпы құралдардың жұмыс істеу мүмкіндігін төмендетеді. Сонымен қатар, құрылғы ресурстарын криптовалюта өндеуге жұмсайтын майнер вирустары интернет-пайдаланушылардың компьютерлеріне енуі мүмкін. Бұдан басқа, желіде көптеген фишинг сайттар бар, олардың көмегімен желі алаяқтары пайдаланушылардың банк картасының нөмірлері, төлқұжат деректері және т.б. жеке деректерін ұрлайды:

– Терроризмді, нацизмді, агрессияны насихаттау қаупі. Жасөспірімдерді басқару өте оңай болу мүмкіндігін, шабуылдаушылар тез пайдаланады. Желіде адамдарды зорлық-зомбылықтың белгілі бір түрлеріне ашық түрде шақыратын сайттар табылады. Бұлар адамдарды шақырып қана қоймай неше түрлі қатыгездік пен кісі өлтіру көріністері бар бейнероликтер орналастырады. Бұл жағдайлар, әдепсіз сөздер мен нешетүрлі әзілдерді үйренеді және де үлкендерге дөрекілік таныта бастайды.

– Алкоголь, есірткі, темекі. Заңсыз заттарды таратушылар әр уақытта жаңа тұтынушыларды іздейді. Өздеріне тарту мақсатында жасөспірімдердің аңғалдығын пайдала отырып, есірткі немесе алкогольді пайдалану арқылы керемет сезімге бөленетінін айтады. Олар өз сеніміне кіргізіп, өмірде қиындықтар туындаған жағдайда, өздерінің тамаша «дәрілерімен» улайды. Мұндай сауда жасайтын ресурстарды Казкомнадзор үнемі бұғаттайды, бірақ олар бәрібір азаймайды.

– 18+ категориялы сайттар. Ерекше сілтемені басу арқылы немесе қалқымалы кескінді басу арқылы бұл сайтқа кездейсоқ кіруге болады. Әрине, ерте ме, кеш пе әрбір бала өмірдің ересек жағына тап болады, бірақ бұл сайт арқылы жасөспірімдердің мезгілсіз эротика мен порнографиямен танысуға әкеліп соғады.

– Лотереялар, казинолар, лотереялар. Көптеген сайттарда онлайн казино туралы жарнамалар бар. Ол баланың назарын аударатын жарқын суретпен тартады. Бұл казинолардың көпшілігі кепілдендірілген үлкен жеңіске уәде беріп, тек ақшаны тартады. Бірақ шын мәнінде, алаяқтар банк карталарының, электронды әмияндардың деректерін біліп, оларды бұзып, қаражатты алып тастайды. Сол мақсатта тегін лотерея билеттерін «тарату». Бала ата-анасының рұқсатынсыз интернетте ақшаға ойнауға, сондай-ақ күдікті сайттарға банк картасының деректемелерін енгізуге қатаң тыйым салынғанын түсінуі керек.

– Әлеуметтік желілер. Әлеуметтік желілердің қауіптілігі сол, әлеуметтік желідегі бейтаныс адамдар балалардың сеніміне кіріп, оған жақын «дос» болу арқылы балаларды қылмыстық әрекетке тарта бастайды. Тіпті балалар түгіл, ересектердің өзі қаскүнемдерге сеніп қалады. Балалар үшін өздерінің ойларымен, тілектерімен, мақсаттарыімен келіскендердің бәрі жақсы болып көрінеді. Қаскүнемдер өздерін бишара жағдайда көрсетіп, баладан қаржылық

көмек сұрауы да мүмкін. Достық пен қолдауға бағыттап, алаяқтар баланы заң бұзуға мәжбүрлей отырып, ақша әкелуге мәжібүрлейді.

– Педофилдер. Бұлар балалармен бір бағытта екендігін көрсете отырып, ақырындап достасуға тырысады. Педофил мектеп, сынып, мекен-жайы туралы біртіндеп қажетті ақпаратарды алады. Олар модельдік агенттіктің қызметкері ретінде өздерін айтып, баламен жеке кездеспей, интимдік сипаттағы фотосуретті немесе бейнені жіберуді сұрауы және фотосуреттерді алу қиын емес, өйткені әрбір жасөспірім модель болуды армандайды. Бір фотосуретті алғаннан кейін қылмыскер баланы бопсалап, фотосуреттерді сыныптастарына немесе ата-аналарына көрсетуден қорқып, педофил қажет нәрсені алады.

Тарихи тұрғыдан шабуылдарды анықтау үшін қолданылатын технологиялар шамамен екі санатқа бөлінеді: аномалды мінез-құлықтың ауытқуларын анықтау және теріс пайдалануды анықтау. Алайда, іс жүзінде мұндай жүйелерді практикалық іске асыру принциптерін ескере отырып, басқа классификация қолданылады: желі деңгейінде және хост деңгейінде шабуылды анықтау. Бұрынғы жүйелер желілік трафикті, ал басқалары операциялық жүйені немесе қолданба журналдарын талдайды. Әр сыныптың артықшылықтары мен кемшіліктері бар, бірақ бұл туралы кейінірек. Айта кету керек, кейбір шабуылдарды анықтау жүйелерін осы кластардың біреуіне ғана жатқызуға болады. Олар әдетте бірнеше санаттағы белгілерді қамтиды. Алайда, бұл жіктеу бір шабуылдарды анықтау жүйесін екіншісінен ажырататын негізгі мүмкіндіктерді көрсетеді [1].

Қазіргі уақытта аномалияларды анықтау технологиясы кең таралмады және ешқандай коммерциялық таратылатын жүйеде қолданылмайды. Бұл технологияның теорияда әдемі көрінетіндігіне байланысты, бірақ іс жүзінде жүзеге асыру өте қиын. Алайда, қазір оған біртіндеп оралу басталды (әсіресе Ресейде) және жақында пайдаланушылар осы технологиямен жұмыс істейтін шабуылдарды анықтаудың алғашқы коммерциялық жүйелерін көре алады деп үміттенуге болады.

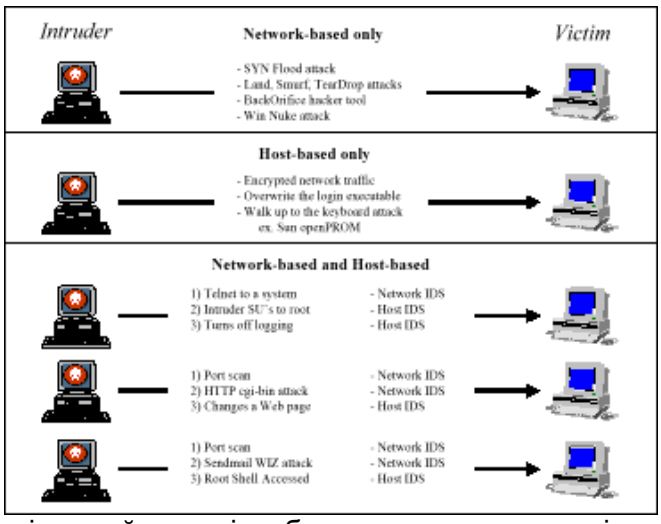
Шабуылдарды анықтаудың тағы бір тәсілі – шабуылды шаблон (pattern) немесе қолтаңба (қол қою) түрінде сипаттаудан және осы үлгіні бақыланатын кеңістікте (желілік трафик немесе тіркеу журналы) іздеуден тұратын теріс қылықтарды анықтау. Вирусқа қарсы жүйелер осы технологиямен жұмыс істейтін шабуылдарды анықтау жүйесінің жарқын мысалы болып табылады [1].

Қазіргі таңда таңда шабуылдарды анықтау ретінде Intrusion Detection System (IDS) жүйесі қолданылуда, ол компьютерлік желіде немесе жеке хостта рұқсат етілмеген және зиянды әрекеттерді анықтауға арналған бағдарламалық өнім немесе құрал болып табылады.

Осы IDS-тің негізгі міндетіне келсек, киберқылмыскерлердің инфрақұрылымға енуін анықтайды және одан әрі өңдеу үшін SIEM жүйесіне берілетін қауіпсіздік туралы ескертуді қалыптастырады. Қауіпті анықтау жүйелері классикалық брандмауэрлерден ерекшеленеді, өйткені олардың соңғысы статикалық ережелер жинағына сүйене отырып құрылғылар немесе желі сегменттері арасындағы трафикті хабарландыруларды жібермей шектейді. IDS идеясының даму барысында қауіп-қатерді анықтап қана қоймай, сонымен қатар блоктауға да қабілетті болып табылады [2].

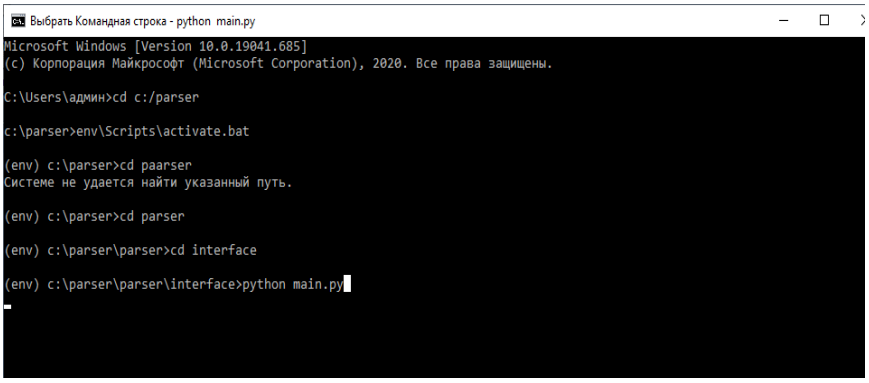
IDS және желілік және жүйелік деңгейлердің бір-бірін тиімді толықтыратын артықшылықтары бар. IDS-тің келесі буыны интеграцияланған жүйелік болып келеді және ол желілік компоненттерді қамтиды. Осы екі технологияны біріктіру арқылы желілерде болатын шабуылдарды және теріс іс-әрекеттерді болдырмауға көбірек үлес қосады, қауіпсіздік мүмкіншілігін едәуір қатаңдатады, сонымен қатар желілік ресурстарын қолдану процесіне икемділік жасайды.

Нәтижелер. Төменде келтірілген 1-ші суретте желілердегі қауіп-қатерлерден жасөспірімдерді қорғау барысындағы ұтымды жүйе құру барысында жүйелік және желілер бағыттындағы шабуылдарды анықтау мүмкіндіктерінің өзара әрекеттесу бағыттары көрсетілген. Кейбір іс-әрекеттерді тек қана желі жүйелерімен анықтайды, ал басқа жағдайларда тек қана жүйенің көмегімен анықтау мүмкіндігі бар. Кейбір адамдар сенімді анықтау мақсатында шабуылдарды анықтаудың екі түрін де қолдануды дұрыс деп санайды.



Сурет 1 – Жүйе мен желі деңгейлердегі шабуылдарды анықтау әдістерінің өзара әрекеттесуі

Бүгінгі таңда Интернет желісінің ерекшелігі – желінің ақпарат ресурстарының 99% барлық тұтынушыларға қол жетімді. Бұл ресурстарға қашықтан қол жеткізуді желінің кез-келген рұқсат етілмеген пайдаланушысы жасырын түрде қолдана алады. Жалпыға қол жетімді ресурстарға, рұқсат етілмеген ақпараттарды анықтау мақсатында Python программалау ортасында «жастардың желі ортасындағы әрекеттесу бағыттарын» анықтау мақсатында ұйымдастырылған программалық жобаға қосылу келесі 2-ші суретте келтірілген.



Сурет 2 – Әлеуметтік желілерді бақылау программасына қосылу

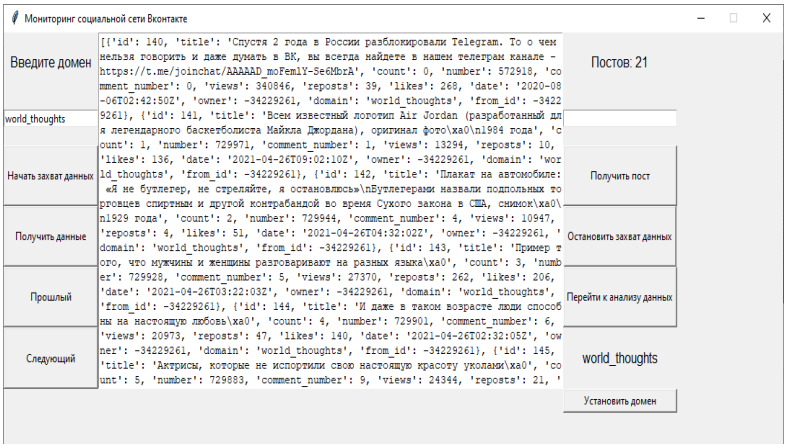
Әлеуметтік желілерді бақылау программасына қосу арқылы 3-ші суретте көрсетілгендей басқару бетіне өтеміз.

Сурет 3 – Программаның бас терезесі

Әлеуметтік желідегі қауіп-қатер тудыратын топтарды анықтап, доменін көшіріп алып «введите домен» мәзірі бойынша доменді енгіземіз де, «установить домен» батырмасын басу арқылы доменді программада сақтаймыз. Енді осы домен арқылы жұмыс жасаймыз, ол үшін «начать захват данных» батырмасын басу арқылы қауіпті мәліметтерді жинай бастаймыз.

Жиналған деректер санын «получит данных» батырмасын басу арқылы аламыз және «пост» мәтін жолынан 4-ші суретте келтіргендей нәтижені көре аламыз.

Бағдарламаның нәтижесі нақты болу үшін осы пост жолағы арқылы көптеген мәліметтердің жиналуын күту керек. Қажетті ауқымды мәліметтер жиналған соң, осы мәліметтерді талдаймыз. Талдау үшін «перейти к анализу» батырмасын басу арқылы деректерді талдау бетіне өтеміз. 5-ші суретте мәліметтерді талдау көрінісі келтірілген.



Сурет 4 – Жиналған «Пост» мәтіні бойынша ақпараттар

Сурет 5 – Алынған ақпаратты талдау

Сурет 6 – «Латенто-сематический анализ комментариев» батырмасы арқылы алынған көрініс

Талқылау. Бұл терезеде талдау жасаудың түрі көп. «Латенто-сематический анализ постов» батырмасымен әлеуметтік желідегі посттардың қауіпті сөздер жиынтығы арқылы, қауіпті іс-әрекет бағытын анықтауға болады. Ал «Латенто-сематический анализ коменариев»

батырмасы арқылы сол посттарға жазылған комментарийлердің қауіпті сөздер жиынтығы арқылы, қауіпті іс-әрекет бағытын анықтауға болады. Осы талдау арқылы қауіпті сөз тіркестерін табу арқылы, қауіпті жағдайда тұрған адамдарды IP адресі арқылы тауып алуға болады және қылмыстық іс болдырмау мүмкіндігі туындайды. Бұл көрініс 6-шы суретте келтірілген.

Ал толық талдау жасау үшін «полный анализ» батырмасын басамыз. Бұл нәтижелер арқылы адамдардың қандай қылмыстық іс-әрекеттерге барғалы тұрғанын алдын-ала бақылауға болады және алдын-алып тоқтатуға болады.

Қорытынды. Қорытындылай келе, ақпараттық қауіпсіздік мәселесі жыл сайын өзекті болып келе жатқанын тағы бір рет атап өтуге болады. Нарық заманында жаппай сұранысқа жауап бере отырып, қауіпсіз жағдайларды қамтамасыз ету үшін сенімді және қажетті шешімдерді ұсынады, бірақ қазірдің өзінде көптеген ұсыныстар түсуде. Ең бастысы мақсат, кез-келген тәсілмен ақпарат қауіпінің басталуын тоқтату және әуесқойлардан немесе басқа адамдардың электронды почталары арқылы құқық бұзушылығынан сақтауды қамтамасыз ету. Ол үшін әр адам баласы өзіне тиісті ақпарат қауіпсіздігімен қамтамасыз ететін сенімді ақпараттық қорғау құралын таңдауы керек, яғни біздің программа арқылы да қауіп-қатерден сақтауға болады.

Әдебиеттер тізімі

1. Чураков А.Н. Анализ социальных сетей // Социологические исследования. 2001. – № 1. – С. 109-121.
2. Лукацкий А.В. Системы обнаружения атак // Банковские технологии. 1999. – № 2.
3. Яблочкин А.С., Кошкин А.П. Современные направления исследований в области стратегий информационной безопасности // Национальная безопасность / nota bene. – 2019. – № 5. – С. 34 – 47. DOI: 10.7256/2454-0668.2019.5.31224
URL:https://nbpublish.com/library_read_article.php?id=31224
4. Миронов К.В., Шарабыров И.В. О применении метода опорных векторов в системах обнаружения атак // Мавлютовские чтения: Всероссийская молодежная научная конференция: сборник трудов в 5 т. Т. 3. – УГАТУ, 2012. – С. 28-30
5. Яблочкин А.С., Кошкин А.П. – Особенности национальной политики информационной безопасности в условиях глобализации // Вопросы безопасности. – 2019. – № 5. – С. 16-31. DOI: 10.25136/2409-7543.2019.5.31126 URL: https://e-notabene.ru/nb/article_31126.html

References

1. Churakov A.N. Analysis of social networks // Sociological research. 2001. – No. 1. – pp. 109-121. (in Russian).
2. Lukatsky A.V. Attack detection systems // Banking technologies. 1999. – No. 2. (in Russian).
3. Yablochkin A.S., Koshkin A.P. Modern directions of research in the field of strategic information security // National Security / nota bene. – 2019. – No. 5. – S. 34-47. DOI: 10.7256/2454-0668.2019.5.31224 URL: https://nbpublish.com/library_read_article.php?id=31224. (in Russian).
4. Mironov K.V., Sharabyrov I.V. On the application of the support vector machine in attack detection systems // Mavlyutov Readings: All-Russian Youth Scientific Conference: a collection of works in 5 volumes. T. 3. – UGATU, 2012. – S. 28-30. (in Russian).
5. Yablochkin A.S., Koshkin A.P. Features of the national information security policy in the context of globalization // Security Issues. – 2019. – No. 5. – P. 16-31. DOI: 10.25136/2409-7543.2019.5.31126 URL: https://e-notabene.ru/nb/article_31126.html. (in Russian).

Г.Е. Жидекулова*, А.Д. Абдувалова, С.Б. Бекболатов
Таразский региональный университет имени М.Х. Дулати
г. Тараз. Ул. Сулейменова, 7
*e-mail: gul2006@mail.ru

ВОЗМОЖНОСТИ ЗАЩИТЫ ПУТЕМ МОНИТОРИНГА УГРОЗ СОЦИАЛЬНЫХ СЕТЕЙ

В настоящее время каждый второй житель планеты зарегистрирован В контакте, Whatsapp, Instagram, Skype, Periscope и других социальных сетях. Хуже всего, социальные сети также могут поставить под угрозу человеческую жизнь. Во многих случаях через эти

социальные сети может распространяться незаконный оборот наркотиков и психотропных веществ, поэтому особое внимание следует уделить изучению проблем доверия к информации в виртуальном пространстве.

Поскольку анализ социальных сетей – это направление, которым занимаются во всем мире, неудивительно, что существует множество программ, а также создание системы с использованием языка программирования Python, которая анализирует тексты в различных предметных областях, которые наша общество нуждается и старается следить за всем виртуальным миром. Мы можем достичь этой цели, внедрив необходимые алгоритмы в специальную программу.

В целях выявления и предотвращения противоправных действий было рассмотрено организовать мониторинг социальных сетей и предотвращение преступлений, организованных через Интернет, путем создания программного обеспечения для мониторинга социальных сетей.

В статье рассматриваются виды киберугроз и методы защиты от них, а также в среде Python создана программа для мониторинга социальных сетей и показаны ее результаты. На основании полученных результатов он рассмотрел возможность предотвращения путем выявления видов угроз.

Ключевые слова: *компьютерная система, программа, угроза, социальная сеть, Интернет, атаки, сетевые IDS, хост, обнаружение атак, Python.*

G.E. Zhidekulova*, A.D. Abduvalova, S.B. Bekbolatov
Taraz Regional University named after M.H. Dulati
Taraz. 7 Suleimenov St.
*e-mail: gul2006@mail.ru

OPPORTUNITY PROTECTION PUTEM MONITORING THREAT SOCIAL NETWORKS

Currently, every second inhabitant of the planet is registered in Vkontakte, Whatsapp, Instagram, Skype, Periscope and other social networks. Worst of all, social media can also endanger human life. In many cases, illicit trafficking in drugs and psychotropic substances can spread through these social networks, so special attention should be paid to studying the problems of trust in information in the virtual space.

Since social network analysis is a field that is practiced all over the world, it is not surprising that there are many programs, as well as the creation of a system using the Python programming language, which analyzes texts in various subject areas that our society needs and tries to monitor the entire virtual world. We can achieve this goal by introducing the necessary algorithms into a special program.

In order to detect and prevent illegal actions, it was considered to organize the monitoring of social networks and the prevention of crimes organized via the Internet by creating software for monitoring social networks.

The article discusses the types of cyber threats and methods of protection against them, as well as a program for monitoring social networks in the Python environment and shows its results. Based on the results obtained, he considered the possibility of prevention by identifying types of threats.

Key words: *computer system, program, threat, social network, Internet, attacks, network IDS, host, detection of attacks, Python.*

Авторлар туралы мәліметтер

Гулкиз Егеновна Жидекулова* – техника ғылымдарының кандидаты, «Ақпараттық жүйелер» кафедрасының доценті; М.Х. Дулати атындағы Тараз өңірлік университеті, Қазақстан; gul2006@mail.ru; ORCID: 0000-0002-6962-2188;

Айнұр Джумабаевна Абдувалова – техника ғылымдарының кандидаты, «Ақпараттық жүйелер» кафедрасының доценті; М.Х. Дулати атындағы Тараз өңірлік университеті, abduvalova_ad@mail.ru; ORCID: 0000-0002-4683-7821;

Самат Берикулы Бекболатов – техника ғылымдарының магистрі, «Ақпараттық жүйелер» кафедрасының аға оқытушысы; М.Х. Дулати атындағы Тараз өңірлік университеті, Қазақстан; sake929224@gmail.com; ORCID: 0000-0002-6127-5249.

Сведения об авторах

Гулкиз Егеновна Жидекулова* – кандидат технических наук, доцент кафедры «Информационные системы» Таразского регионального университета имени М.Х. Дулати, Казахстан; gul2006@mail.ru; ORCID: 0000-0002-6962-2188;

Айнұр Джумабаевна Абдувалова – кандидат технических наук, доцент кафедры «Информационные системы» Таразского регионального университета имени М.Х. Дулати, Казахстан; abduvalova_ad@mail.ru; ORCID: 0000-0002-4683-7821;

Самат Берикулы Бекболатов – магистр, старший преподаватель кафедры «Информационные системы» Таразского регионального университета имени М.Х. Дулати, Казахстан;sake929224@gmail.com; ORCID: 0000-0002-6127-5249.

Information about authors

Gulkiz Zhidekulova – candidate of technical sciences, associate professor Department of Information Systems, Taraz Regional University named after M.Kh. Dulaty, Taraz, Kazakhstan; gul2006@mail.ru; ORCID: 0000-0002-6962-2188;

Ainur Abduvalova – candidate of technical sciences, associate professor Department of Information Systems, Taraz Regional University named after M.Kh. Dulaty, Taraz, Kazakhstan; abduvalova_ad@mail.ru; ORCID: 0000-0002-4683-7821;

Samat Bekbolatov – Master of Technical Sciences Department of Information Systems, Taraz Regional University named after M.Kh. Dulaty, Taraz, Kazakhstan; sake929224@gmail.com; ORCID: 0000-0002-6127-5249.

Материал 25.03.2023 ж. баспаға түсті.

DOI: 10.53360/2788-7995-2023-1(9)-5

ҒТАХР: 65.63.33

Г. Мажит, Н.С. Машанова, Л.Г. Кудренова*

С. Сейфуллин атындағы Қазақ агротехникалық зерттеу университеті

010000 Қазақстан Республикасы, Астана қаласы, Жеңіс даңғылы 62

*e-mail: kudrenova99@bk.ru

СҮТҚЫШҚЫЛДЫ СҮТ ӨНІМДЕРІНЕ ТҰТЫНУШЫЛАРДЫҢ ҚАЛАУЫН БАҒАЛАУ

Аңдатпа: *Бұл мақала ақпарат алу әдістерінің бірі ретінде сауалнама жүргізу арқылы ашыған сүт өнімдеріне, атап айтқанда йогуртқа халықтың қажеттіліктерін, қалауын анықтау мәселелеріне арналған. Зерттеулер шеңберінде сұранысқа қатысты сұрақтарды кеңінен қамтитын 20 құрылымдық сұрақтан тұратын сауалнама әзірленіп, https://docs.google.com/forms платформасына орналастырылды және сауалнамаға жауап берушілерге сілтеме жіберілді (сұраққа жауап беру міндетті болып табылады), йогурт түрлері, көлемі және өндірушілері бойынша тұтынушылардың қалауын анықтау, сондай-ақ сатып алу жиілігі және тұтынушылардың шығарылатын йогурттардың ассортиментіне қатынасы белгіленді. Сауалнамаға ҚР барлық өңірлерінен 100 адам қатысты. Сұрақтардың реттілігі логикаға сәйкес келеді, сұрақтардың тәртібі респонденттің белсенді сауалнамасына ықпал етеді. Зерттеу сауалнамасы аясында зерттеудің сипаттамалық әдісі қолданылды, респонденттердің сауалнамаларының деректері өңделді, жүйеленді және диаграмма, кестелер түрінде ұсынылды. Сауалнаманың нәтижесі, йогуртқа сұраныс бар және негізінен толтырғыштары бар йогурттарға артықшылық беріледі. Йогуртты таңдаудың негізгі критерийлері құрамы болды, бұл адамдардың ағзаға ең пайдалы тағамдарды тұтынуға қызығушылығын көрсетеді, жалпы адамдар функционалды қасиеттері бар йогурттарды жақсы көреді, осыған байланысты йогурт өндіру нарығы біртіндеп кеңейіп, тұтынушылардың жалпы тағамға деген қызығушылығын арттырады.*

Түйін сөздер: *сауалнама, йогурт, ашытылған сүт өнімдері, функционалды тағамдар, қоспалар*