ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МНИСТІРЛІГІ

Сәтбаев университеті

Ақпараттық және телекоммуникациялықтехнологиялар институты

Киберқауіпсіздік, ақпаратты өңдеу және сақтау кафедрасы

Ким Таңшолпан Берікқызы

«Банк құрылымдарының клиенттерін оқытудың ақпараттық жүйесін және әлеуметтік инженерия әдістеріне қарсы әрекет ету әдістемесін әзірлеу»

ДИПЛОМДЫҚ ЖҰМЫС

5В100200 – «Ақпараттық қауіпсіздік жүйелері» мамандығы

Алматы, 2021

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Сәтбаев университеті
Ақпараттық және телекоммуникациялық технологиялар институты
Киберқауіпсіздік, ақпаратты өңдеу және сақтау кафедрасы

«Қорғауға жіберілді»
КАӨжС кафедра меңгерушісі
тех. ғыл. канд, доцент
_____Н.А.Сейлова
« 27 »___мая___2021 ж..

ДИПЛОМДЫҚ ЖҰМЫС

Тақырыбы: «Банк құрылымдарының клиенттерін оқытудың ақпараттық жүйесін және әлеуметтік инженерия әдістеріне қарсы әрекет ету әдістемесін әзірлеу»

5В100200 – «Ақпараттық қауіпсіздік жүйелері» білім беру бағдарламасы бойынша

Орындаған Ким Т.Б.

Ғылыми жетекші т.ғ.м., лектор Зиро А.А.

Алматы 2021

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Сәтбаев университеті

Ақпараттық және телекоммуникациялық технологиялар институты

Киберқауіпсіздік, ақпаратты өңдеу және сақтау кафедрасы

5В100200 – Ақпараттық қауіпсіздік жүйелері

БЕКІТЕМІН
КАӨжС кафедра меңгерушісі
тех. ғыл. канд, доцент
_____
Н.А.Сейлова
« 27 »___мая___2021 ж.

Дипломдық жұмысты орындауға
ТАПСЫРМА

Білім алушы _Ким *Таңшолпан Берікқызы*
Тақырыбы: *Банк құрылымдарының клиенттерін оқытудың ақпарттық жүйесін және әлеуметтік инженерия әдістеріне қарсы әрекет ету әдістемесін әзірлеу*
Университет Ректорының 2020 жылғы «24» 11 №2131-б бұйрығымен бекітілген.
Аяқталған жұмысты тапсыру мерзімі 2021 жылғы «30» мамыр.
Дипломдық жұмыстың бастапқы берілістері: *диплом алдындағы практикалық жұмыс қорытындысы, тақырып бойынша әдебиеттерге шолу нәтижелері, теориялық мәліметтердің жиыны*
Дипломдық жұмыста қарастырылатын мәселелер тізімі:
а) Киберқауіпсіздікке қауіп төндіретін факторлар талданды;
б) Нақты әдістер ұсынылып, нақты ұсынылған әдістердің тиімділігі көрсетілді;
в) Клиенттердің көп қолданатын қосымшаларын киберқауіпсіздіке байланысты қорғаудың нақты ережелер мен әдістері жасалынып, жұмыста топтастырылды;
г) Автоматтандырылған банк жүйесіндегі банктік ақпараттың ақпараттық қауіпсіздігінің тұжырымдамасы дайындалды.
Сызбалық материалдар тізімі: Power Point бағдарламасындағы слайдтар
Ұсынылатын негізгі әдебиет: 23 атау

Дипломдық жұмысты дайындау

КЕСТЕСІ

Бөлімдер атауы, қарастырылатын мәселелер тізімі	Ғылыми жетекші мен кеңесшілерге көрсету мерзімдері	Ескерту
Әлеуметтік инженерия	01.03.2021 ж.	Орындалды
Әлеуметтік инженерлік оқыту және ақпараттандыру	26.03.2021 ж.	Орындалды
Қазақстандағы банктер жүйесіне сипаттама және олардың қауіпсіздік деңгейлеріне талдау	22.04.2021 ж.	Орындалды
Автоматтандырылған банк жүйесіндегі банктік ақпараттың ақпараттық қауіпсіздігінің тұжырымдамалық негіздерін дамыту	17.05.2021 ж.	Орындалды

Дипломдық жұмысының бөлімдерінің кеңесшілері мен норма бақылаушыларының аяқталған жобаға қойған **қолтаңбалары**

Бөлімдер атауы	Кеңесшілер, аты, әкесінің аты, тегі (ғылыми дәрежесі,атағы)	Қол қойылған күні	Қолы
Норма бақылаушы	тех-ғыл магистрі, ассистент Кабдуллин М.А.	30.05.2021	

Ғылыми жетекші _____ Зиро А.А.

Тапсырманы орындауға алған білім алушы _____ Ким Т.Б.

Күні “24” 11. 2020ж.

АҢДАТПА

Дипломдық жұмыс 69 беттен, 11 суреттен, 2кестеден, 3 сызбанұсқадан қорытынды бөлімнен, 23 пайдаланылған әдебиеттер тізімінен тұрады.

Жұмыстың мақсаты: Қазақстанда киберқауіпсіздікті нығайту мақсатында клиенттер мен қызметкерлердің әлеуметтік инженерияда қателік пен шабуылға ұшырамас үшін нақты ережел қолдану. Киберқауіпсіздікте,әлеуметтік инженерия саласында заманауи әдістерді қолдана отырып Адамдарға қымбат ақпараттарды бөтен адамдардан қорғаудың шаралары көрсетілді.

Банк құрылымдарының клиенттерін оқытудың ақпараттық жүйесін және әлеуметтік инженерия әдістеріне қарсы тұру әдістемесін әзірленді.

Нәтижелер:

- Киберқауіпсіздікке қауіп төндіретін факторлар талданды.
- Қызметкерлер мен клиенттердің қателіктері баса назар аударылып көрсетілді.
- Нақты әдістер ұсынылып, нақты ұсынылған әдістердің тиімділігі көрсетілді.
- Клиенттердің көп қолданатын қосымшаларын киберқауіпсіздіке байланысты қорғаудың нақты ережелер мен әдістері жасалынып, жұмыста топтастырылды.
- Автоматтандырылған банк жүйесіндегі банктік ақпараттың ақпараттық қауіпсіздігінің тұжырымдамасы дайындалды.

АННОТАЦИЯ

Дипломная работа состоит из 69 страниц,11 рисунков, 2 таблиц, 3 итоговых разделов, 23 списков использованной литературы.

Цель работы: В целях укрепления кибербезопасности в Казахстане применять четкие правила, чтобы клиенты и сотрудники не подвергались ошибкам и атакам в социальной инженерии. В области кибербезопасности,социальной инженерии были продемонстрированы меры по защите дорогостоящей информации от посторонних людей с использованием современных методов.

Разработана информационная система обучения клиентов банковских структур и методика противодействия методам социальной инженерии

Результаты:

- Проанализированы факторы, угрожающие кибербезопасности.
- Большое внимание было уделено ошибкам сотрудников и клиентов.
- Были предложены конкретные методы и продемонстрирована эффективность конкретных предложенных методов.
- Разработаны и сгруппированы в работе четкие правила и методы защиты приложений, используемых клиентами, связанных с кибербезопасностью.
- Разработана Концепция информационной безопасности банковской информации в банковской системе

ANNOTATION

Thesis consists of 69 pages, 11 figures, 2 tables, 3 summary sections, 23 lists of used literature.

Purpose of work: In order to strengthen cybersecurity in Kazakhstan, apply clear rules so that customers and employees are not exposed to errors and attacks in social engineering. In the field of cybersecurity, social engineering, measures have been demonstrated to protect expensive information from strangers using modern methods.

An information system for training clients of banking structures and a methodology for countering the methods of social engineering have been developed.

Results:

- Analyzed the factors that threaten cybersecurity.
- Much attention was paid to the mistakes of employees and customers.
- Specific methods were proposed and the effectiveness of specific proposed methods was demonstrated.
- Developed and grouped in the work clear rules and methods for protecting applications used by customers related to cybersecurity.
- The Concept of information security of banking information in the banking system has been developed.

МАЗМҰНЫ

КІРІСПЕ

Бүгінгі таңда компьютерлік желінің қауіпсіздігі мәселелері ақпараттық және қаржылық жүйелердің технологиялық дамуымен тығыз байланысты. Халықаралық ақпарат алмасудың, ғаламдық коммуникациялық инфрақұрылымның және ақпараттық кеңістіктің кибер қауіпсіздігі ұлттық, мемлекеттік, жеке және желілік қауіпсіздік деңгейінде көрінеді. Әлемдік қаржы желісіндегі төлем жүйелерінің әртүрлілігі мен өзара тәуелділігі банк секторын киберқауіптерге әсіресе осал ортаға айналдырады. Кибер-шабуылдар қаржы жүйелеріне, коммуналдық қызметтерге, салаларға, корпорацияларға, автомобильдерге, үкіметке ғана емес, сонымен қатар мәліметтерді кибер кеңістігіне сеніп тапсыратын барлық салаларға қауіп төндіреді. Әлемде ұлттық заңдар мен ережелерді біріктіретін ғаламдық желіні басқару жүйесі мен заңнамалық база әлі жоқ. 2017 жылғы статистикалық мәліметтерге сәйкес, әлем халқының 49,6% -ы Интернетке қол жеткізе алады, ал аймақтық статистикаға сәйкес, ең көп қолданушылар Азия мен Еуропада. 2014 жылмен салыстырғанда телефондар. 2015 жылы ғаламдық компьютерлік желілерде 1,1 млн жұмыс орны жойылды. тәулігіне шабуыл жасайды, бұл 2014 жылмен салыстырғанда 117% артық. Пайдаланудың негізгі қатерлері Интернет-сауда, электрондық коммерция, мемлекеттік операциялар және ақша операцияларымен байланысты басқа қызметтерге байланысты. Бірнеше зерттеулердің авторлары жылына 1 триллион доллар немесе әлемдік ЖІӨ-нің 1,4% -ы шығынға ұшырағанын көрсетеді.2 Жоғарыда айтылғандардан кибер қорғаныс қоғамдық әл-ауқатпен тығыз байланысты деген қорытынды жасауға болады.

1 Әлеуметтік инженерия

Бір анықтама бойынша әлеуметтік инженерия «адамға өзінің мүддесіне сәйкес келуі немесе болмауы мүмкін әрекетті жасауға әсер ететін кез-келген әрекетті» білдіреді (Social Engineer Inc. 2016a). Бұл терминді бір сөйлеммен қамтиды, бірақ оның мәнін түсіну үшін оны әрі қарай зерттеу керек.

1.1 Әлеуметтік инженерия тарихы

Әлеуметтік инженерия ешқандай жағдайда жаңа құбылыс емес. Жылдар бойы адамдар басқалардың белгілі бір жағдайларда іс-әрекетіне әсер ету және оны пайдалану тәсілдерін тапты. Мүмкін, ең танымал тарихи мысал - Гомердің Одиссеядан шыққан трояндық ат. Ертегінің танымал болғаны соншалық, біз оның атымен зиянды бағдарламалар тобын атадық. Хикаятта гректер трояндықтармен ұзақ соғыс жүргізді және ақыры шайқастан бас тартты. Трояндықтар гректердің күн батқанға қарай жүзіп бара жатқан соңғы кемесін көреді және өз тарихын одан әрі қолдау үшін гректер бір жауынгерді артта қалдырып, артқа шегіну және бағыну символы - нақты ағаш қуыс трояндық жылқыны айналдырады. Табиғи түрде трояндықтарды аттың ішінен шыққан гректер өлтіреді. Заманауи тұрғыдан алғанда, ертегі бұрынғыдай данышпан болып көрінбеуі мүмкін. Оқиғаның шынымен болған-болмағаны мауды емес, оның элементтері мауды.

Бүгінде бұл оқиғаны естіген адам қуыс атқа таң қалмауы мүмкін, бірақ мәселе сол уақытта ешкім мұндай нәрсені елестете де алмады. Қазіргі заманда біз теледидардан немесе кинодан көрген барлық ертегілерден сюжеттік бұрылыстар мен күтпеген нәтижелер күттік, бірақ бірнеше мың жыл бұрын адамдардың бір-біріне айтқан әңгімелері бірдей құрылымға ие болмады. Бұл оқиғалар біздің әлемді қалай қабылдайтынымызды анықтайды және Гомердің Одиссея жазған кезінде әлемге деген көзқарасы басқаша болатын. Қуыс ағаш аттың идеясы мүлдем жаңа және өзгеше болды. Сол қағида да өз күшінде барлық SE. Адамдар өмірде бұрын білген нәрселеріне сүйене отырып әрекет етеді және олар іс-әрекеттер мен оқиғалардың нәтижелерін болжауға болатын деп күтеді.

1.2 Әлеуметтік инженерия психологиясы

Адамның миы әдеттер жасауда асып түседі. Ми дегеніміз - бұл машина, және оның барлық жасайтын ресурстары энергияны білдіреді. Мидың көзқарасы бойынша оңтайлы жағдай мүмкіндігінше аз энергияны

пайдаланады. Сондықтан біз күнделікті өмірде үлгілерді жасаймыз, мысалы жұмысқа келгенде кофе ішу, сағат 10-дан кейін темекі шегу немесе түскі ас кезінде жаңалықтар оқу. Үлгілер энергияны үнемдейді, әрдайым жеке тұлға не істейтіні туралы үнемі ойланудың қажеті жоқ . Компьютер әлемінде хакер X тапсырмасын орындауы керек бағдарламаны алдаудың жолын табады бағдарламаның шектеулері сақталмай тұрып, Y тапсырмасын орындау. Осындай ойлау түрі де ММ-де бар. Адамдардың белгілі бір жағдайларда қалай әрекет ететінін білгенде, сіздің нақты мақсатуға жету үшін осы мінез-құлық модельдерін теріс пайдалану оңай.

Әлеуметтік инженерия - біз орнатқан жаңа нәрсе емес. Алайда, бұл қалайша қазіргі заманға дейін мойындалмаған деген сұрақ туындайды? Неміс профессоры Вильгельм Вундт 1879 жылы Лейпциг университетінде тек психологияға арналған алғашқы зертхананы құрғанға дейін, әлеуметтік инженерияның, психологияның түбірі өзінің ғылым саласы ретінде болған емес. Вундттың зерттеулері тестке қатысушылардың сыртқы тітіркендіргіштерге реакцияларына бағытталды, мысалы, ол метронома дыбысына қатысатындарды қабылдап, олардың сезімдері туралы есеп беруін сұрайды. Бұл әлі күнге дейін мимикалық мимикаларды зерттеуден алыс жақсы бастама болды. Вундт өзінің көптеген студенттерімен танымал, олар белгілі психологтар болды, мысалы, өз жұмысын жалғастырған Эдвард Титченер.

Вундтың ақылға деген көзқарасы структурализм немесе ақыл-ойды құрайтын негізгі элементтерді зерттеу деп аталды. Вундт қарым-қатынасқа баса назар аударды сананың элементтері арасында Титченер дивидуалды элементтерге назар аударды. Структуралистік көзқараста қателіктер болғанымен, тәжірибе нәтижелерін қайта айту қиын болғандықтан, ол сәнге айналды. Нәтижелер бір мағыналы болған жоқ, бұл ғылыми-теорияның кез-келген лайықты болуына қойылатын негізгі талап.

Мұның бәрінен бас тартудың бір мауды факторы бар: адамдар тітіркендіргіштерге белгілі бір болжамды тәсілдермен әрекет етсе де, барлық адамдар бәрібір жеке адамдар. Бір адамның ашуын тудыруы мүмкін нәрсе, екіншісінде күлкі тудыруы мүмкін. Табысты әлеуметтік инженер мұны есте сақтайды және әртүрлі адамдарға бірдей айла-тәсілдерді қолданбайды.

1.3 Әлеуметтік тәсілдер

Әлеуметтік инженерия - бұл өте кең құбылыс, бірақ мен оның кең таралған техникасының көп бөлігін қамтуға тырысамын. SE белгілі бір дағдылардың жиынтығынан гөрі өнердің түрі болып табылады, сондықтан көптеген шабуылдар басталатын қадамдарға қарап, оны түсіну оңай. SE-дің

IT-ге қарағанда психологиямен көп ұқсастықтары болғанымен, оған қажет ақыл-ой әдеттегі хакерлердікіне өте ұқсас. Сондықтан шабуылдан қалай қорғану керектігін түсіну арқылы одан қорғану оңай. Интерполдың (2016 ж.) Пікірінше, әлеуметтік инженерлік алаяқтықтар әдетте төрт қадамды орындайды: ақпарат жинау, қарым-қатынасты дамыту, кез-келген анықталған осалдықты пайдалану және орындау. Бұл әлеуметтік шабуылдар шабуылдаушы мен нысана арасындағы нақты өзара әрекеттесуді білдіретін жағдайларда өте дұрыс. Бұл тарауда мен шабуылдардың әр түрлі бөліктерінде қолданылатын әлеуметтік әдістердің көпшілігін өтемін. Кейінірек біз сотталушы тараптың жәбірленушімен жеке байланысын сақтауды қажет етпейтін МҚ-ны қарастырамыз.

1.3.1 Доксинг

Ақпаратты жинау немесе мен бұдан былай сілтеме жасайтындай доксинг - кез-келген сәтті шабуылдың ең мауды бөлігі. Доксинг - бұл алдымен игеру қиын, бірақ оны ұнатып алғаннан кейін, бұрын мүлдем белгісіз адамнан Интернетте қанша ақпарат таба алатындығу таңқаларлық. Доксинг - бұл барлық шабуылдардың мауды бөлігі, себебі ол қалғаны негізделеді. Мақсаттың атын, үйдің мекен-жайын, әлеуметтік қауіпсіздік нөмірін және тіпті жұбайының атын білгеннен кейін, мақсатты еліктеп, олар туралы көбірек ақпарат алу оңайырақ. Көптеген адамдар өздерінің туған қалаларын өздерінің Instagram-да жалған анонимді аккаунтына орналастыру арқылы бейтаныс адамдарға беретін күшін жете бағаламайды. Қаланың аты мен атауының арқасында мүмкін болатын нәтижелер қазірдің өзінде айтарлықтай қысқарды. Мен өзіммен кездескен барлық жаңа адамдарды онлайн режимінде байланыстырғаныма өте қуаныштымын және бұл адамның Facebook-ті табуы әдетте 10 минуттан аспайды.

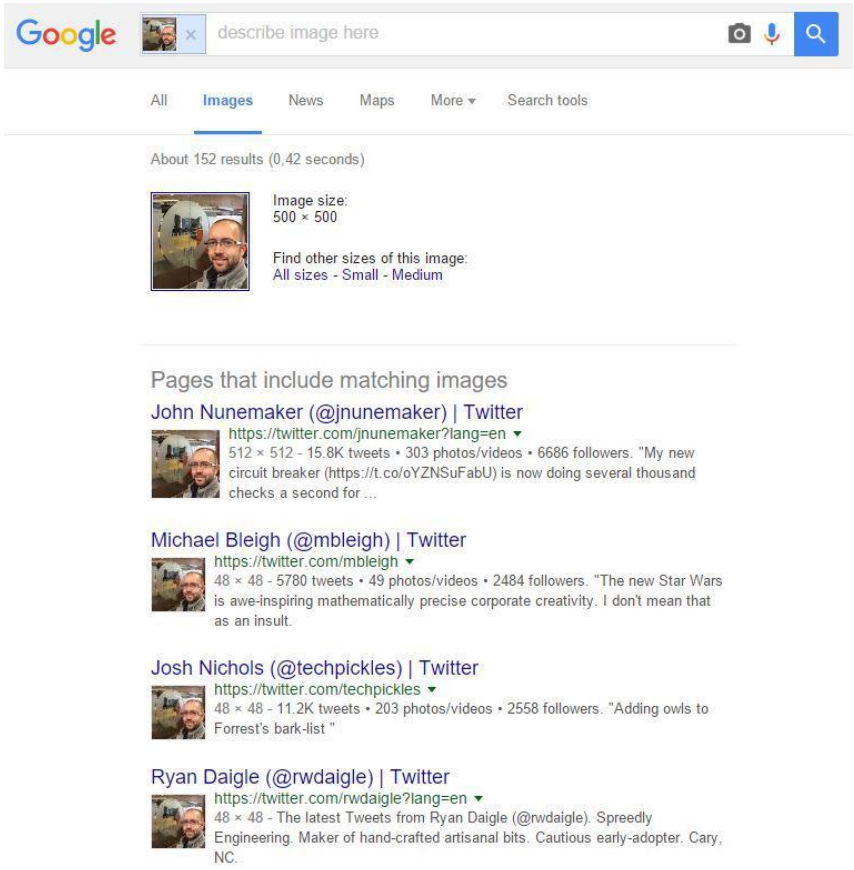
Тек олардың аты мен туған қаласы көрсетілген парақ. Бұл пациенттің парағын бірнеше рет айналдыруды қажет етеді, бұдан басқа ештеңе жоқ.

Үлкен ақпараттың таралуының ең соңғы оқиғаларының бірі желтоқсан айында Valve-тің танымал ойын және сандық дүкені Steam платформасы қолданушыларды бір-біріне дүкен беттерін қарауға қате жіберуге жол берген кезде болды. Адамдар басқа пайдаланушылардың есеп айырысу мекен-жайларын, Steam Guard телефон нөмірінің соңғы төрт санын, сатып алу тарихын, несиелік карта нөмірінің соңғы екі санын және / немесе электрондық пошта мекен-жайын көре алды. Оқиға шамамен бір-екі сағатқа ғана созылды, бірақ зиян келтірілді. Бұл ақаулық бір мезгілде қызмет көрсетуден бас тарту (DoS) шабуылына байланысты қолданылған кэштеу ережелерінде, сондай-ақ

мерекелік сатылым кезінде дүкенді қарайтын пайдаланушылардың көптігінде болды. Кез келген адамның егжей-тегжейі - бұл әлеуметтік инердің қасиетті қабығы. Ашылған егжей-тегжейлер мақсатты өте сенімді етіп көрсетуге мүмкіндік береді. Ағынның кездейсоқ сипатына байланысты оқиғаның нақты шығынын бағалау қиын. Сонымен қатар, адамның есепшотының болуы зиянкестің мақсатқа нақты зиян келтіруіне мүмкіндік береді. Өзінің видео подкастында видео ойындарды сынға алушы Джон Бэйн немесе желіде танымал Тотальбискуит те бұл мәселеге алаңдаушылық білдірді. Бейн бейне ойындар әлемінде өте қатты сыншы ретінде танымал және оның пікірлері көбіне өте түзу, көптеген адамдарды тітіркендіреді. Оның жағдайында, егер біреу үйінің мекен-жайын осындай жолмен алған болса, мысалы, оны ауыстырып тастауы мүмкін деген қорқыныш болар еді (Totalbiscuit, The Cynical Brit 2015.) Бұл жағдайда свот дегеніміз көбінесе АҚШ-та болатын зиянды заттарды білдіретін құбылыс. адам төтенше жағдай органдарына жәбірленушінің мекен-жайында ауыр қылмыс болып жатыр деген жалған уәжбен хабарласады. Шабуылшының мақсаты - бұл жерде арнайы қару-жарақ пен тактика (SWAT) тобын заңға бағындыру. Ауыстыру - бұл зиянкестің зиян келтіруі үшін мақсатты мекен-жайын пайдалануы мүмкін девиантты тәсілдердің бірі (Fagone 2015.)

1.3.2 Хакер мүмкіндігі

Сонымен, хакерлері бар әлеуметтік инженерлер қандай техниканы қолданады? Интернетте ақпарат табудың бірнеше әдісі бар, мен мұнда ең көп қолданған кейбіреулерін келтіремін. Бірінші кезекте Google және барлық басқа іздеу жүйелері таңқаларлық емес. Егер сіздің мақсатудың толық аты-жөнін білсеңіз, сіз оны өте жақсы бастаду. Іздеудің алғашқы нәтижелері арасында көбінесе мақсатты Facebook парағын немесе басқа онлайн тұтқаларын таба аласыз. Егер сізде сурет бар болса, сізде кері кескін іздеу деп аталатын жақсы танымал емес функция бар. Оның көмегімен сіз сұрақтың кескіні орналастырылған беттерді іздеу үшін Google іздеу жүйесін пайдалана аласыз. Олар тіпті жалпыға қол жетімді болған Instagram профильдерін де тізімдейді. Егер сіз Google Chrome-ды қолдансау, сіз тінтуірдің оң жағын басып, ашылған мәзірден суретті желіден іздеу мүмкіндігін таба аласыз. Сіз суретті Google іздеу жолына сүйреп апара аласыз. Төменде Джон Нунемейкердің Twitter-дегі аккаунтынан Google Reverse Image іздеуі арқылы жүргізілген профильдік фотосуретінің мысалы келтірілген.



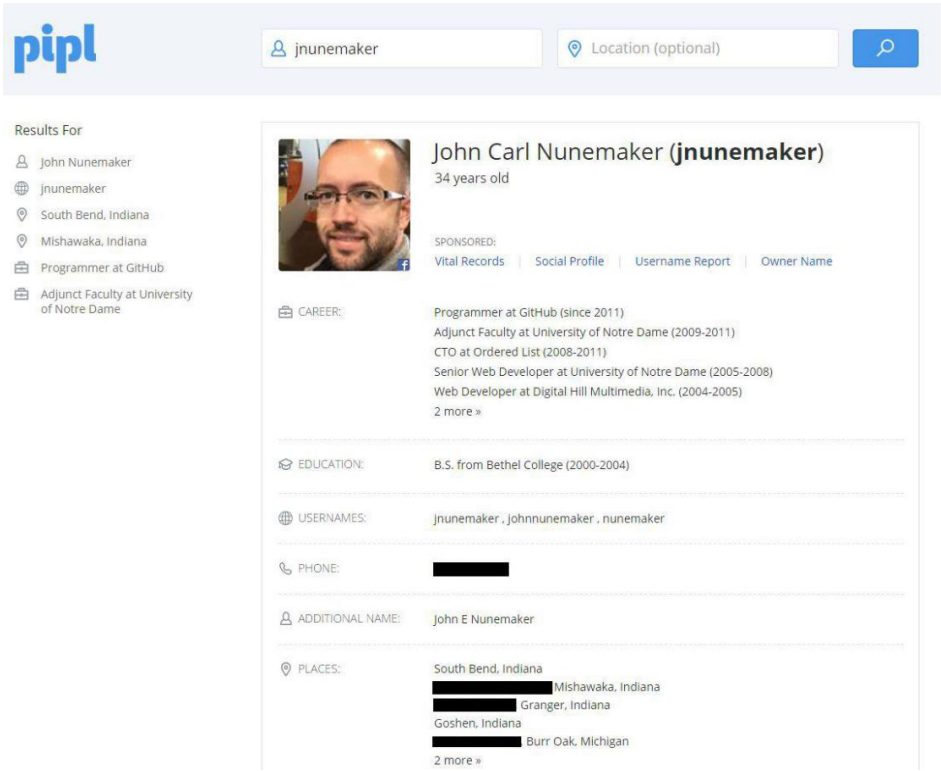
Сурет 1 - Джон Нунемейкердің Google Reverse кескін іздеуіндегі суреті

Қазіргі уақытта Bing дәл осындай функционалдылықты ұсынады және бірнеше басқа нұсқалар да қол жетімді. Негізінен кері кескін іздеуге бағытталған ежелгі тәуелсіз іздеу жүйелерінің бірі Tineye деп аталады. Сонымен қатар, тағы бір жақсы нұсқа - Google, Bing және Yandex-ті қырып, нәтижелерді бір жерде келтіретін Image Raider.

Кәдімгі іздеу жүйелерінен басқа, жақсы әлеуметтік инженер олардың өзін шектемейді. Кейбір Facebook профильдері кез-келген іздеу жүйесінде индекстелмеген етіп орнатылған, бірақ сіз оларды Facebook-тің жеке іздеу функциясында таба аласыз. Бұл Twitter және Instagram сияқты мақсатты мақсаттағы басқа әлеуметтік медиа-аккаунттарға қатысты. Әдетте ақпарат біртіндеп жинақталады, сіз оның фамилиясынан адамның нақты атын таба аласыз, ал кейбір гуглингпен олардың Twitter-дегі аккаунттары пайда болады, оларда басқа онлайн-тұтқаларының бірі көрсетілген. Көбіне бұл процесс жұмыс істейді, бірақ сіз кейде сәтті бола аласыз.

Интернеттегі адамдарды іздеуге арналған бірнеше іздеу жүйелері бар, ал қазір олардың ішіндегі ең жақсысы - pipl. Мен әлі күнге дейін Джон Нунемейкерді іздеймін, ол Github-тің қолданбалы бағдарламасының танымал инженері болып табылады және оның Github парағын оның Twitter

аккаунтында байланыстырдым. Оның парағында оның пайдаланушы аты jnunemaker ретінде көрсетілген. Пиплді жылдам іздеу ол туралы және тағы басқалардың барлығын ашады. Интернеттен өзіне тиесілі болып көрінетін pipl таба алатын барлық аккаунттар суретте көрінбейді. Nun-emaker өте танымал бағдарламашы екенін ескеру керек, сондықтан нәтижелер мөлшері алдын-ала сәйкес келеді. Pipl әдетте үлкен цифрлық ізі бар адамдармен жақсы жұмыс істейді, бірақ мен оның мекен-жайын нәтижелер қатарына қосамын деп ойламадым. Әрине, нәтижелер Интернетте жарияланған ақпарат сияқты дәл. Нәтижелерде көрсетілген мекен-жай ескі болуы мүмкін немесе мүлдем қате болуы мүмкін, сондықтан көбінесе нәтижелерді бірнеше ақпарат көздерінен тексеру ақылды. Pipl LinkedIn, Twitter, Flickr, Facebook, Pinterest және тағы басқалар сияқты бірнеше түрлі әлеуметтік медиа веб-сайттарды индекстейді және бұл мақсат үшін көбірек есептік жазба мен пайдаланушы аттарын табудың тамаша әдісі.



Сурет 2 - Джон Нунемейкердің пиптерді іздеудегі сабы

Жақсы ақпарат көзі - бұл whois іздеуі. Егер мақсатта олардың атында тіркелген веб-сайт немесе домен болса, олар туралы көбірек білуге ICANN сақтайтын доменнің whois жазбаларында мүмкіндік бар. Төмендегі цензураланған скриншот - танымал фин блогерінің веб-сайтының жазбалары. Жазбаларда аты-жөні, үй мекен-жайы, тіпті телефон нөмірі айқын көрінеді. Ірі веб-сайттар мен домендерде тіркеушінің аты-жөнінің орнына жай админ

сияқты басқа нәрсе болады, ал адрес компанияның өз мекен-жайы болып табылады. Бірнеше кішігірім веб-сайт иелері доменді тіркеу кезінде өздерінің ақпараттарын пайдаланады. Көбінесе, егер сіз доменді тіркеу кезінде жалған ақпарат берсеңіз де, сіздің байланыс төлемдерудің орнына сіздің төлемдеру қолданылуы мүмкін. Тіркеушілердің көпшілігі, әрине, олардың ақпаратын тіркелушінің орнына пайдаланатын қызметті ұсынады (Ars Technica 2015.). Ақпаратты бөлімдерге ауыстыру өте кеш болуы мүмкін, өйткені ақпарат қазірдің өзінде индекстелген және оны бірнеше жерден табуға болады. Интернет-архивтің Wayback Machine сияқты Интернеттің кэштеу қызметтері.

Сурет 3 - Whois-атақты фин блогерінің жазбалары.

Интернеттегі адамдар мен ұйымдар туралы ақпаратты табудың көптеген басқа жолдары бар, бірақ егер мен олардың барлығын осы жерде тізіп берсем, бұл жұмыс әлдеқайда ұзағырақ болар еді. Бұл әркім өзін-өзі тексере алатын және Интернетте қанша ақпарат ағып жатқанын көре алатын ең кең таралған.

1.3.3 Қарым-қатынасты дамыту

Шабуылшы нысанаға қатысты барлық мүмкіндікті біліп алғаннан кейін, олардың келесі қадамы нысанаға қатынас құруға бағытталған. Қарым-қатынас шабуылшының бастапқы мақсатына жететін болса, тіпті оң болуы шарт емес. Шабуылдаушы мақсат туралы көбірек білген сайын, мақсатты басқару және олардың сеніміне кіру оңайырақ болады.

1.3.4 Әлеуметтік дәлелдеу

Әлеуметтік дәлелдеу - бұл әсер етудің алты қағидасының ішіндегі ең қарапайымы және кең қолданылатыны. Қарапайым тілмен айтқанда, бұл жай

ғана басқа адамдардан алынған ақпаратты, пікірлерді және мінез-құлықты білдіреді. Бір көңілді мысал - Candid Camera Inc компаниясының ескі және әйгілі видео эксперименті, алдымен лифт ішіне бір актер, кейінірек бірнеше актер орналастырылған. Бұл еркелігінің құрбаны біздің лифтте жүргенде топқа енуіміз керек екендігімізді көрсетеді және лифтегі басқа адамдардың жүріс-тұрысын сол бағытқа қарап немесе басқа адамдар сияқты бас киімін шешіп алып жүреді сол кеңістікте. Адамдар әлі күнге дейін белгілі бір дәрежеде үйір менталитетіне ие және лифттегі барлық адамдар сіз сияқты қарама-қарсы тұрған кезде сіз өзуді ыңғайсыз немесе қолайсыз сезінесіз. Мұны құрдастардың қысымы деп те атайды.

Әлеуметтік дәлелдеу - бұл маркетинг әлеміндегі танымал құбылыс және ол бұрыннан қолданылып келеді. Әрине, оны пайдаланудың әр түрлі тәсілдері бар, бірақ Techcrunch-тағы мақалада әлеуметтік дәлелдеудің бес түрлі әдісі келтірілген: сарапшы-әлеуметтік дәлел, атақты адамдардың әлеуметтік дәлелі, қолданушының әлеуметтік дәлелі, көпшіліктің даналығы сіздің достарудың әлеуметтік дәлелі Соңғы екеуі жоғарыда айтылған топтық менталитетті қолданады: егер сіздің достару немесе сіздің туған жерудегі көпшілік белгілі бір жерден өз машиналарын сатып алса, сіз өз дүкендеруді дәл сол дүкеннен сатып алатын шығарсыз. жақсы. Қолданушының әлеуметтік дәлелі сәл түсініксіз және бұл маркетинг қолданушының оң тәжірибесіне сүйенеді дегенді білдіреді. Бұл ішінара желілік маркетингтің принципі болып табылады. Маркетинг саласында тәжірибесі жоқ қарапайым адам сізді жаңа өніммен таныстырғанда, сіз теледидардан жарнаманы әдемі және келбетті көруден гөрі, тауар туралы өз тәжірибеңізге сенесіз. адам сізді сол өніммен таныстырады. Мұның тағы бір жақсы заманауи мысалдары - Youtube-тегі бейнелер, онда кәдімгі контент өндірушісі белгілі бір ойын немесе өнімді насихаттайды. Алғашқы екеуі - сарапшылардың әлеуметтік дәлелі және атақ-даңқтың дәлелі - бұл беделді қабылдауға жауап берудің адамдық қасиетін өз пайдасына қолданатын қасиеттер.

1.4 Тікелей емес шабуыл

Әлеуметтік инженерия тек шабуылдаушы мен жәбірленуші арасындағы физикалық өзара әрекеттесумен шектелмейді. Оны шабуылдаушы жәбірленушімен бір бөлмеде болмай-ақ қолданудың бірнеше әдісі бар. Бұл тарауда мен SE шабуылдарында қолданылатын жанама тәсілдердің көпшілігін өтемін. Бұл шабуылдардың жұмыс жасау тәсілі - олар адамның қызығушылық сияқты кейбір негізгі қасиеттерін тағы бір рет теріс пайдалануы.

1.4.1 Фишинг және найза фишинг

Жалпы фишинг дегеніміз - шабуылдаушымен құпия ақпаратты бөлісу мақсатымен алдау әрекеті. Әдетте фишингтік шабуылдар электрондық пошта арқылы жүзеге асырылады, бірақ олар тек оны қолданумен шектелмейді. Фишингтік шабуылдардың көпшілігі бұқаралық шабуылдар ретінде жіктелуі мүмкін, бұл олардың мақсатты тобы үлкен және фишингтік әрекеттің мазмұны әр қабылдаушыға сәйкес нақты бөлшектерден тұрмайды дегенді білдіреді.Найза фишинг дегеніміз - бұл мазмұн хабарлама, кем дегенде, белгілі бір дәрежеде алушыға сәйкес келеді .

Фишингтік жаппай шабуылдар мүмкіндігінше орынсыз болып көрінгенімен, мүмкіндігінше көп аудиторияға жететіндей етіп жасалады. Соңғы мақсат - мақсатты шоттарды немесе мысалы, олардың несиелік карталарын сатып алу. Фишингтік электрондық пошта алушылардың көпшілігі eBay әкімшісі сияқты сенетін көзден шыққан сияқты. Фишер салған торлардың кеңдігі соншалық, оны байқап қалу оңай: егер eBay-да мақсатты мекен-жайы жоқ болса, олардан электронды хат алса, олар оны ашпайды (Hoffman 2013.). Мұның тағы бір жақсы мысалы бұл өте нашар грам-марға ие немесе Google Translate арқылы басқарылған фишингтік хаттар.

Найзалық фишинг - Егер шабуылшы олардың мақсатын білсе және олар туралы жақсы ақпарат жинаса, олардың электрондық поштаны ашуы үшін мақсатты түрде алуы едәуір ықтимал. Cisco жүргізген зерттеуге сәйкес, жаппай шабуылға кіретін адамның фишингтік электрондық поштаны ашудың орташа мүмкіндігі аз 3% құрайды, ал мақсатты найза фишингтік хаттар 70% жағдайда ашылған. . Найзалық фишингті нөлдік күндік ерліктермен біріктіру әдеттегідей, компанияның болжамды бас директорының электрондық поштасындағы зиянсыз көрініс сілтемесінің артында тұрады. Тахтементтерді де қолдануға болады. 2015 жылы Symantec корпорациясы ішкі интранет ішінде барлау жүргізу үшін пайдаланылған жаңа шабуылдаушыларды жұқтырған желіні жақсы түсіну үшін Лациок деп аталатын жаңа троянды анықтады. Троян корпоративті желіге қалай түсті? Бұл эксплуатация Microsoft ActiveX-те белгілі осалдығын қолданды және троян спам-поштаға тіркеме ретінде келген кәдімгі Excel файлына жинақталды. Сұрақтардағы пайдалану нөлдік күн болған жоқ, бірақ сәтті пайдаланылған жүйелер дұрыс патчталмағандықтан, ол жұмыс істеді (Symantec 2015.)

2 Әлеуметтік инженерлік оқыту және ақпараттандыру

2.1 Әлеуметтік инженерлік оқыту және ақпараттандыру бағдарламаларымен қарастыру

Әлеуметтік инженерлік қатерлерге қарсы тұруда ұйымдастырушылық ақпараттық жүйелердің тиімділігі персоналдың хабардарлығын арттыру бойынша басқарушылық күштермен қатар жетілдірілген техникалық шараларды біріктіруді қажет етеді. Мауды шаралардың бірі - қызметкерлерге шабуылдың зиянды әрекеттерін тану, жала жабу, жалтару және өшіру қабілетін дамыту үшін оларды дұрыс оқыту. Алайда, оқыту мен ақпараттандыру бағдарламаларын ұсыну жолы көптеген факторлардан туындайтын қиындықтарға толы. Факторларды жалпы түрде келесідей жіктеуге болады.

2.1.1 Іскери қоршаған орта

Іскери орта факторларына қызметкердің интерактивті жұмыс орны, сондай-ақ сыртқы аймақтар кіреді. Қызметкерлерге берілетін оқыту мен хабардар ету бағдарламаларына әсер ететін экологиялық өзгерістер басым технологиялар, ұйымдық мәдениет, қызметкерлерге білім беру, саясат және физикалық қауіпсіздікке түзетулер енгізу сияқты факторлардан тұрады [22]. Сыртқы желі арқылы қашықтықтан қол жеткізуге болатын персоналды электрондық пошта арқылы бағыттауға болады. Зақымдану қашықтықтан қол жеткізілетін ұйымдық сандық құрылғылар мен желілерде орын алуы мүмкін. Интернеттің бизнестің әр саласында интеграциялануымен қашықтықтан қол жетімділіктің әсерлері артып келеді [23]. Әлеуметтік инженерия мен Twitter, Snapchat, Facebook және т.с.с. сияқты әлеуметтік медиа веб-сайттарын пайдалану арасында өзара байланыс күшейіп келе жатқанын атап көрсетеді. Ұйымның осалдығын арттыратын аралас ақпараттық жүйеге біріктірілген. Сонымен қатар, әлеуметтік инженерлік шабуылдар динамикалық және дамып келеді, ал ақпараттық технологиялар арқылы жұмыс жасаудың және тәуелділіктің жоғарылауымен қызметкерлердің шабуылдан толық оқшауланууы өте қиын. Зерттеулер көрсеткендей, қазіргі кезде әлеуметтік инженерлік қатерлермен күресудің ең жақсы шешімі қызметкерлердің әлеуметтік инженерлік шабуылдардың жалпы әдістері туралы білімдерін дамыту болып табылады [25].

2.1.2 Әлеуметтік оқыту мен хабардар ету

Бағдарламалары арқылы әлеуметтік инженерлік шабуылдардың алдын-алу жөніндегі шектеулер әлеуметтік коммуникация процесінде пайда болады. Бір жағынан, индустриядағы бәсекелестік нарықта өзектілігін сақтау үшін клиенттермен әлеуметтік байланысты талап етеді. Екінші жағынан, бұл бейресми қарым-қатынасты тудыруы мүмкін. Мұндай бейресми қарым-қатынас пен әлеуметтік байланыс қызметкерлерді оқыту мен ақпараттандыру бағдарламалары арқылы ойлап тапқан қауіпсіздік шаралары бойынша бұзушылықты тудыруы мүмкін [26]. Әлеуметтік инженерияға қарсы оқыту және ақпараттандыру бағдарламаларындағы қиындықтарға әкелетін әлеуметтік факторларға мәдениеттердің әсері жатады. Қауымдастық сезімін қабылдайтын кейбір мәдениеттерге сәйкес, өзара әрекеттесу жұмыс өмірінің де бөлігі болып табылады. Бұл қасиетті қызметкерлер жұмыс орнына ауыстырады, бұл оларды әлеуметтік инженерия процесі арқылы бұзуға ұшыратады [27]. Біздің білуімізше, әдебиеттегі оқыту мен ақпараттандыру бағдарламаларының әсерін шектеудегі мәдени немесе әлеуметтік факторлардың әсерін көрсететін салыстырмалы зерттеу жоқ. Алайда Alseadoon [28] зерттеуін салыстыру нәтижелері Сауд Арабиясында тіркелген фишингтік электронды эксперименттердің тек 7% бар екенін көрсетеді. Жауап беру деңгейі батыс елдері бойынша тек 3–11% -ды құрайтын әр түрлі зерттеулерге қарағанда едәуір жоғары екендігі анықталды [29-31]. Тренинг пен ақпараттандыру бағдарламаларының тиімділігі мен әлеуметтік факторлар арасында тығыз байланыс жоқ болса да, әлеуметтік фактор ұйымдағы әрбір қызметкер үшін бірыңғай оқыту әдісін жобалау кезінде демографиялық әсерді есепке алуда мауды фактор бола алады.

2.1.3 Конституциялық оқыту

Конституциялық оқыту бағдарламасының дискурсына үкіметтік ықпал әдебиетте өте шектеулі. Саяси пікірталастар жүргізетін таңдау көбінесе әлеуметтік тұрғыдан жасалған шабуылдардан қауіпсіздікті арттыруға бағытталған. Сонымен қатар, жалған ақпарат тарату түріндегі мемлекеттік күн тәртібіне негізделген манипуляция - бұл әлеуметтік инженерлер қолданатын әдеттегі әдіс. Хакерлер мақұлдауды қолдайды және интеллектуалды диссонансты қолдана отырып, пікірлес топтарға бағытталған және адамдардың белгілі бір топтарына персоналды оқыту мен хабардар ету бағдарламаларынан асып түсуіне ықпал етеді [32]. Сонымен қатар, Коста мен Фигейра [33] үкіметтерге қауіпсіздік туралы көбірек заңдар шығарып, ұйымдарда оларды әлеуметтік инженерлік қауіп-қатерлерге қарсы оқыту және хабардар ету бағдарламаларын күшейтуге мәжбүр ететін шаралар қабылдауды

ұсынады. Қауіпсіздік туралы заңның бұзылмағандығын растау үшін барлық қызметкерлердің әр түрлі заңдық ережелерді сақтауын қамтамасыз ету өте мауды [34]. Шарттар тренерлерге оқу әдістерін конституциялық тұрғыдан бекіту үшін оқу материалдарын қайта өңдеуге әкелуі мүмкін. Хакерлер және / немесе әлеуметтік инженерлік шабуыл процедуралары жеке ақпаратты, соның ішінде парольдерді алу үшін бірнеше жаңа әдістерді қолданады. Қазіргі заманғы бес шабуылға фишинг, жем, квид про-кво, сылтау және пигбэкбринг кіреді [35,36]. Желіде болжау - бұл кез-келген уақытта браузерді қолданатын кез-келген адам ашық серверге қарсы іске қосатын әдістердің бірі [37]. Интернеттегі болжау әдісі көптеген үкіметтер мен ұйымдардың қауіпсіздігіне үлкен алаңдаушылық туғызды, өйткені әр түрлі жеке сәйкестендірілетін ақпарат (PII) және құпия сөздер қол жетімді болды. Сонымен қатар, онлайн-мақсатты болжау әлсіз қарапайым парольдерді ғана емес, сонымен қатар сайттарда қайта пайдаланылатын құпия сөздерді және жеке ақпараты бар құпия сөздерді қолдана алады [37]. 1-суретте үш мемлекет, Түркия, Қытай және АҚШ арасында PII-ге негізделген бұзушылықтар туралы кейбір мәліметтер келтірілген.

2.1.4 Ұйымдастырушылық

Ұйымның ішкі ортасы фирмаға тән шектеулерден тұрады, егер оқыту мен хабардар ету бағдарламалары кәсіпорын ішіндегі әлеуметтік шабуылдарды басқаруда пайдалы болатын болса. Шектілік санасы әр түрлі деңгейдегі персоналдың нақты топтарына бағытталған әр түрлі жоспарланған хабардарлық бағдарламаларының болмауынан туындайды [41]. Қауіпсіздік бойынша оқыту бизнестің қажеттіліктеріне, нарықтағы қысымға, бизнесті модернизациялауға, алғышарттар мен фирмаға қол жетімді бюджетке байланысты өзгеріп отыруы керек. Ақпарат алу үшін киберқылмыскерлер қолданатын динамикалық әдістер үнемі жаңарып отырады [26,42]. Өкінішке орай, киберқылмыскерлер мақсатты фирманың алдын-алу шаралары туралы білгеннен кейін, олар қызметкерлерге таныс емес жаңа әдістерді ойлап табады және қолданады [43].

2.1.5 Қызметкерлер арасындағы экономикалық оқыту.

Ақпараттандыру бағдарламаларын интерактивті мазмұн арқылы едәуір жақсартуға болады [44]. Джемаль [44] хабарлау материалы ұсынылатын орта осындай тренингтің жалпы әсер етуінде мауды рөл атқаратынын көрсетеді. Алайда, дамып келе жатқан әр шабуылға үнемді оқытуды ұсыну ұйымдар үшін қиындық тудырады. Сонымен қатар, дамып келе жатқан әлеуметтік

инженерлік қатерлерге қатысты болу үшін ұйым өз қызметкерлерінің дайындығын белсенді түрде тексеруі керек. Бұл процесс қызметкерлерді олардың дайындығына қарай бағалауды және олардың тұрақтылығы мен қауіпсіздіктің төтенше жағдайлар жоспарларын орындау қабілетін бағалауды қамтиды [45]. Сынақтарды ақпараттық технологиялар немесе қауіпсіздік бөлімі өздері өткізген жағдайда да, қаражат ұйымның басқа бөлімшелерінен оқыту және ақпараттандыру бағдарламаларына бағытталуын талап етеді. Қысқаша айтқанда, егер кадрларды даярлау үшін қажетті экономикалық ресурстарды кезең-кезеңімен бөліп отыру мүмкін болмаса, бизнестің үздіксіздігі үлкен тәуекелге ұшырайды [46,47].

2.1.6 Жеке тұлғаның қасиеттері

Бұл жеке тұлғаның тән сипаттамалары, ол әлеуметтік инженерлік шабуылдарға қарсы оқыту мен хабардар ету бағдарламаларының тиімділігіне қауіп төндіруі мүмкін. Әлеуметтік инженерлер мақсатты қызметкердің жеке басына негізделген шабуыл әдістерін таңдап алады [48]. Хакерлер құрбандардың мінез-құлқындағы осалдығын нақты тану үшін әртүрлі психологиялық әдістерді қолданады. Луо және басқалардың зерттеуі. [49] хакерлердің адамдардың жемге әсер етуін қамтамасыз ету үшін моральдық міндетті кінәлау техникасын қолдануы мүмкін екенін көрсетеді. Сонымен қатар, персоналдың жеке басындағы айырмашылықтар, тіпті қызметкердің әлеуметтік инженерлік ерліктерге деген реакциясына әсер етеді [50]. Анықтама [51] нейротизмді атап көрсетеді, бұл қорқыныш сезімдерін, мысалы, мазасыздық, ашуланшақтық, әлсіздік немесе депрессияны бастан кешіру, фишингтік хаттарға жауап беру мүмкіндігімен өте байланысты. Сонымен қатар, экстраверттер және толқуды іздейтін қызметкерлер де талапшыл және ақпаратты оңай бере алады. Ақырында, адамның жеке басының қасиеті ретіндегі ашықтық қызметкерлердің хакерлерге өз ұйымдарына өтуі үшін жеке ақпаратты және сандық іздерді қалдырып, жаңа нәрселерді жасауға дайын екендігін білдіреді [26,28,52]. Адамдардың сенгіш табиғаты әлеуметтік инженерлік қауіп-қатерлерге қарсы хабардар болу бағдарламалары үшін үлкен сынақ болуы мүмкін. Жеке адамдар мен ұйымдардың физикалық және мәліметтер қауіпсіздігіне ұйымдағы адамдар аса байыпты қарауы қажет [48-50]. Жеке тұлғалардың өз ұйымдарының АТ-инфрақұрылымына деген сенімі көп болғандықтан, қызметкерлер қауіпсіздікті қауіп деп санамайды. Ұйымдар, әдетте, адамдардың табиғатында болатын сенім кемшіліктерін жабу үшін оқу материалдарын қамтуы керек [51]. Ақпараттық қауіпсіздікті тиімді және жан-жақты оқыту мен хабардар ету

бағдарламалары арқылы қызметкерлердің сеніміне байланысты проблемалардың алдын алуға болады. Алайда, кейбір жағдайларда ұйымдар өз қызметкерлерін әлеуметтік инженерлік шабуылдардан болатын минималды зиянды өтеуге үйрету үшін шектеулі ресурстармен қамтамасыз етеді [50]. Қауіпсіздік бойынша қосымша дайындықты қажет етпейтін тұжырымдама әлеуметтік инженерлік қатерлерге қарсы тиімді қауіпсіздікті талап ететін негізгі факторға айналды. Нәтижесінде, мамандар арасында көбірек ақпараттандыру науқанының көмегімен азайтуға болатын сенім аралықты жабу туралы білімдер жетіспейді. Бұл алшақтық әлеуметтік инженерлерге оларды оңай бағыттауға тамаша мүмкіндік туғызуы мүмкін. Әлеуметтік инженерияға қарсы оқыту және ақпараттандыру бағдарламалары үшін қиындық тудыратын тағы бір фактор - бұл жалпы кадрларға деген қызығушылықтың аздығы. Жеке адамдарда өзін және ұйымдарын қорғау үшін жүйелі түрде оқудан өту үшін жеке мотивация жетіспейді [52].

Қауіпсіздік туралы хабардар болу тұжырымдамасы көбінесе жеке және кәсіби рөлдеріне қатысты ақпарат пен мәліметтер үшін шабуылға ұшыраған адамдардың жиі кездесетініне қарамастан құлақ естімейді. Бұл қызығушылықтың болмауы Хаднаги сияқты әдебиеттерде де көрініс тапты [53], бұл қауіпсіздік туралы хабардар етуге қатысты қолданушылардың білімі мағынасыз, өйткені жеке адамдар жеткілікті қызығушылық танытпайды. Хаднаги бұл қызығушылықтың жоқтығын соңғы пайдаланушылар қауіпсіздікті өздері ойламайды деп санауға болатындығын да атап өтті. Керісінше, қызметкерлер қауіпсіздік ұйымы кез-келген қауіп-қатерге жауап беруі керек деп ойлайды. Нәтижесінде әлеуметтік инженерлік қауіп-қатерлерге қатысты адамдардың қызығушылығының болмауы персоналдың тиімді дайындығы мен хабардар болуын талап ететін өте мауды факторға айналады [54]. Әлеуметтік инженерлік шабуылдардың зиянды ниеті түрлерін түсінудің әр түрлі жеке мүмкіндіктері хабардар болу бағдарламаларында тағы бір үлкен қиындық тудырады [55]. Бұрын әлеуметтік инженерия техникасының тәсілдері қазіргіден гөрі тікелей болды. Бұрын олар нашар жамылған болатын, бұл адамдарға мұндай шабуылдардың мәнін түсінуге мүмкіндік берді. Алайда, әлеуметтік инженерия әдістерінің күрделілігі мен күрделілігінің жоғарылауы құрбандарға оларды тануды қиындатады [56]. Қысқаша айтсақ, манипуляция тактикасының дамуы, егер адамдар ақпараттандыру бағдарламаларына қатысса да, әлеуметтік инженерлік шабуылдардың жаңа әдістерін білмей қалуы мүмкін. Әлеуметтік инженерлер көбінесе үлкен ұйымдар үшін онша стратегиялық емес рөлі төмен қызметкерлерді мақсатты түрде таңдайды. Әлеуметтік инженерлер бүкіл фирмаға шабуыл жасауды жоспарламас бұрын мүмкіндігінше құпия

мәліметтерді жинау үшін төменгі деңгейдегі қызметкерлерден жұмыс туралы мәліметтер жинай бастайды [51]. Мұндай шабуылдардың маудылығы туралы хабардар болмау, сонымен қатар қызметкерлер өздерін ірі корпорацияларда өте мауды деп санамауы мүмкін, қызметкерлерді өте осал етеді [57]. Бұл өзіндік маудылықтың болмауы ақпараттандыру бағдарламалары үшін қиындық тудырады. Бұл өзіндік маудылықтың жоқтығын қамту туралы хабардар ету бағдарламаларына қосуға болады. Қызметкерлер өз ұйымдарының азаматтығын сезінуі және ұйымның қауіпсіздігіне инвестиция құйылғандығын сезінуі керек. Соңғы жеке қиындық - адамдар кейде кәсіби рөлдерінде үлкен жұмыс қысымына ұшырайды және соның салдарынан жұмыс пен өмірдің тепе-теңдігі шектеулі болады. Бірнеше ұйымдар барлық қызметкерлерге әлеуметтік инженерлік қатерлер туралы білімдерін арттыру үшін қажетті қауіпсіздік курсынан өтуге мәжбүр ету үшін күшті қауіпсіздік саясатын белгіледі. Оқыту және хабардар ету бағдарламалары жүргізілген кезде қызметкерлер жұмыс уақытында қажетті дайындықтан өтуге тырысады. Алайда, жұмыс қысымы бұл мәселеде әлсіздікті тудыруы мүмкін, өйткені кейбір персонал жұмыс пен өмірдің тепе-теңдігі тұжырымдамасына қарсы күрделі мерзімдерге тап болады [58].

Бұл жұмыс қысымы тренинг барысында тыңдаушылардың назарының аздығына әкеледі және оларды хабардар ету бағдарламаларының сессияларына немқұрайлы қарау сезімін қалдырады [48]. Бұл бейқам көзқарас тренинг сабақтары үшін қызметкерлердің әр түрлі әлеуметтік инженерлік шабуылдардың үнемі дамып келе жатқан әдістеріне деген хабардарлығын арттыру үшін олардың білім қорын тиімді дамытуға қиындық туғызады. Ақпараттық жүйелер мен құпия деректерге қол жеткізудің ең кең таралған тәсілдерінің бірі - мәжбүрлеп енгізу немесе электрондық ұрлау арқылы емес, жеке адамдар мен адамның ақыл-ойымен айла-шарғы жасау. Әлеуметтік инженерия - бұл құпия және құпия ақпаратқа рұқсатсыз қол жеткізу тәсілі, өйткені ол жеке тұлғалардың психологиялық манипуляцияларына сүйенеді. Нәтижесінде, сол адамдар мұндай ақпаратты ашады немесе тыйым салынған жерлерге олардың дұрыс емес іс-әрекеттерді жасырғанын білмей қол жеткізеді. Олар әлеуметтік инженерияның құрбаны болып, заңсыздықпен айналысады, өйткені олардың адами қасиеттері пайдаланылады [48].

2.2 Заманауи әлеуметтік инженерлік оқыту және ақпараттандыру бағдарламаларымен байланысты мәселелерге шолу

Әлеуметтік инженерлік шабуылдардың қаупі артып келе жатқандықтан оқыту және ақпараттандыру бағдарламалары дамып келеді. Қауіпсіздік

тренингтері және ақпараттық қауіпсіздік туралы хабарлау бағдарламалары модельдеу әдістерін, мауды ойындарды, виртуалды зертханаларды және тақырыптық бейнероликтер мен модульдерді қамтиды [59]. Алайда, осы заманауи оқыту әдістемесі қызметкерлердің дайындығын арттырудың өзіндік шектеулері бар. Бірқатар зерттеулер [8,9,60] байыпты карточкалық ойындарды әлеуметтік инженерлік шабуылдарға қарсы саналы деңгейдің жоғарылауының мауды құралы ретінде енгізуді ұсынады. Карточкалық ойындар әдісі, алайда, тыңдаушылар командалары арасында үйлестіру қиынға соғады. Оқыту кезеңінде ойынның осы түрлері үшін ынтымақтастық тәсіл қолданылады. Бұл нақты шабуылдар кезінде жұмыскердің шешім қабылдау дағдыларын жақсартуға көмектеседі. Алайда командалар арасында оқу материалын қабылдау мен қабылдау кезіндегі тұлғалардың айырмашылықтары қиындық тудыруы мүмкін [9,61]. Интерактивті ойындар мен виртуалды зертханаларды қамтитын соңғы оқыту әдістері үйлестіру проблемасына тап болды. Ойын шабуылдарды анықтау мен азайтудың әр түрлі қадамдарын қамтитындықтан, бәрін дұрыс тәртіпте қосу қиынға соғады. Қызметкердің хакерге ұшырауын бақылау және ұйымның ақпараттық жүйесінде болуы мүмкін зиянның таралуын бақылау қиын. Координацияның шектелуі туындайды, өйткені қауіпсіздік шараларына кімнің қатысу керектігін анықтау қиын. Әр түрлі командалардың өздерінің мамандандырылған жұмыстарын орындаудың дұрыс тәртібі бар-жоғын анықтау да қиын [6]. Тақырыптық бейнематериалдар мен хабардарлық модульдері сияқты хабардарлықты дамытудың соңғы әдістері шығармашылық тәсілдер болып табылады. Хабардар болу модульдері барлық қауіпсіздік шараларын қамтуға арналған болса да, бір ғана шешім болмауы мүмкін. Себебі әлеуметтік инженерлік шабуылдағы сенімсіздіктер оқу және ақпараттандыру бағдарламаларын жобалаушылардың болжамдық қабілеттерінен тыс болады [61]. Сонымен қатар, әлеуметтік инженерлер қызметкерлерге жемшөппен әрекет етудің ерекше қажеттілігін құруға мамандандырылған, бұл хабардар ету бағдарламалары қамтымай қалуы мүмкін психологияны жоғалту және кері қайтару қорқынышын қолданады [62-64].

Қазіргі заманғы оқыту әдістері, соның ішінде өмірлік модельдеу сценарийлері, әлеуметтік инженерия және әлеуметтік инженерлердің шабуыл жасау әрекеті туралы хабардар болуға бағытталған [58]. Оқудың заманауи әдістері қызметкерлерге хабарламаның әлеуметтік инженерлік шабуыл немесе жоқ екендігі туралы стратегиялық ойлауға көмектесу үшін осы модельдеуді қолданады. Алайда, бұл модельдеу барлық қызметкерлерге ұқсас түрде дайындалады және әр қызметкердің жеке түсінуіне жауап бермейді [65]. Модельдеу сеанстарын аяқтау процесі адамның хабарламаны қалай

қабылдауы мүмкін екенін қарастырмайды. Әр сценарийге әр түрлі қызметкерлердің реакциясы әртүрлі болуы мүмкін, өйткені әр адамның инстинкттері, сенімділік деңгейі және алдану немесе алдау мүмкіндігіне қатысты хабардарлығы әртүрлі. Бұл әр түрлі мінез-құлық аспектілері шабуылдан қалай аулақ болу керектігін тиімді талқылауға қиындық туғызады, өйткені әрбір жеке тұлғаны қабылдау рөл атқарады. Сонымен қатар, тренинг сабақтарының көп бөлігі жалпыланған болғандықтан, олар көпжақты әлеуметтік инженерлік шабуылдарды түсінбеуіне әкеліп соқтыруы мүмкін және сайып келгенде, осындай хабардар ету бағдарламаларын жүзеге асырудың жалпы мақсатына сәйкес келмейді [66]. Оқытудың заманауи әдістерінің тағы бір қиыншылығы - бұл олардың көп уақытты алуы. Модельдеу, бейнежазбалар және интерактивті ойындар қызметкерлерден кәдімгі кәсіби міндеттерін бөліп, қажетті оқу сабақтарын аяқтай алады. Оқытуға арналған қосымша уақыт олардың жұмысындағы өнімділігін шектейді, бұл жұмыс уақытына жететін қызметкерлерге әсер етуі мүмкін [49]. Егер семинарлар жұмыс уақытынан тыс өткізілсе, бұл кедергі тудыруы мүмкін, өйткені қызметкерлер жұмыс пен өмір балансының бұзылуына байланысты қатыса алады немесе келмеуі мүмкін. Әлеуметтік инженерлік шабуылдарға арналған қазіргі заманғы оқыту әдістерін көбіне IT мамандары жасайды. Бұл IT-емес ұйымдардағы қызметкерлердің көпшілігінің техникалық білімінің болмауына байланысты қиындық тудыруы мүмкін [67]. Қарапайым дизайнның болуы тыңдаушыларға жаттығудың қазіргі заманғы әдісімен қалай жұмыс істеуге болатындығын түсінуге емес, оның мазмұнына назар аударуға көмектеседі. Соңғы пайдаланушылар осы заманауи оқыту құралдарының интерфейсінің соңғы дизайнының қарапайымдылығын бағалайды. Қысқаша айтқанда, оқытудың заманауи әдістері дизайнының қарапайымдылығы персоналдың жалпы ақпараттылығына қол жеткізуде және сайып келгенде ұйымның ақпараттық жүйелерін қорғауда мауды.

2.3 Дәстүрлі әлеуметтік инженерлік оқыту және ақпараттандыру бағдарламаларымен байланысты мәселелерге шолу

Дәстүрлі оқыту мен хабардар ету бағдарламаларын негізінен фирмалар қызметкерлерді әлеуметтік инженерлік шабуылдардан жаңартып отыру үшін қолданады. Мұндай ақпараттық бағдарламаларға жергілікті жерлерде оқыту және ақпараттандыру лагерлері, скринсаверлер, постерлер, қолмен еске салғыштар және онлайн-курстар кіреді [5,68]. Ғафир және басқалар [69] фирмалардың оқу бюджеттерінің жетіспеушілігі оқу-танымдық лагерьлерге және жергілікті жерде оқытудың басқа әдістеріне қиындық туғызуы мүмкін

екенін көрсетеді. Қиындықтың бұл түрі, негізінен, компаниялардың оқыту бюджеттерін минимизациялауға ынталандыратын экономикалардың төмендеуіне байланысты. Бұл сонымен қатар әлеуметтік инженерияға негізделген хакерлерге фирманың ескірген жүйелерін бүлдіру үшін жаңа әдістер ойлап табуға мүмкіндік ашады. Сондай-ақ, әлеуметтік инженерлік шабуылдар персоналды электронды түрде бағдарлаумен шектелмейтіндігін ескеру қажет. Егер физикалық қол жетімділік қатерлері, соның ішінде қоқыс жәшігі, егер ұйымдар өз қызметкерлеріне білім беруді тоқтатса, үлкен зиян келтіруі мүмкін. Барлық қызметкерлерге - жоғары деңгейлі менеджерлерден бастап, тазалаушыларға дейін оқыту мен хабардар ету әдістерін енгізу қиынға соғады, өйткені әр түрлі қажеттіліктерге сай оқу материалы жеке адамдардың оқу қабілетіне сүйенеді [6,34]. Дәстүрлі оқыту әдістері, әдетте, олардың жетістігін шектейтін скучно және жалықтырғыш деп бағаланды. Ақпараттық қауіпсіздік тренингтері әлеуметтік инженерлік қауіп-қатерлерге қарсы кейде қызметкерлерді хакерлердің манипуляциялау тәсілдерін еске түсіруге мәжбүр ететін негізгі мақсатқа бағытталмайды. Керісінше, олар өте жалпыланған және түпкілікті нәтижеде теріс нәтиже әкелуі мүмкін елеулі жағдай туғызатын толық формальды жағдайларда жасалады. Оқу ортасының бұл түрі қызметкерлерге осы сессиялар кезінде алатын қауіпсіздік туралы мауды ақпаратты ұмытып кетуді жеңілдетеді [20]. Оқу сабақтары қызметкерлерге дайындалған оқу материалдарымен өзара әрекеттесуіне көмектесетін бірнеше қызықты іс-шаралар өткізуі керек. Әлеуметтік инженерияның дәстүрлі оқыту әдістері көбінесе қызметкерлерге практикалық әсер етпейді [68]. Әдістердің бұл түрлері қызметкерлерді қазіргі өмір сценарийлеріне ұшыратпайды, өйткені қазіргі оқыту әдістері қол жетімді. Қызметкерлер дәстүрлі әдістермен шабуылдың не туралы болатынын білуге кіріседі, бірақ нақты шабуылға тап болған кезде олар оны оңай тани алмауы мүмкін. Сонымен қатар дәстүрлі оқыту әдістері, соның ішінде постерлерді басып шығару, экрандық қорғағыштар мен жұмыс үстеліне әлеуметтік инженерлік шабуылдар туралы ескерту және құпия ақпараттың таралуының мауды салдарын орналастыру өте қарапайым және жалпы ақпаратты қамтиды. Осы дәстүрлі әдістердің өзі қызметкерлер арасында жеткілікті қауіпсіз мәдениетті қалыптастыра алмайды [44]. Дәстүрлі оқыту әдістері кездесетін тағы бір қиындық - олардың сенімділікті толық сыни бағалауды шеше алмауы. Әлеуметтік инженерлік шабуылдаушылар қолданатын негізгі қару - құрбандарына құпия ақпаратпен бөлісу немесе олардың мақсатына жетуге көмектесу үшін оларға сенім арту [48]. Әлеуметтік инженерлік шабуылшылар алдымен қызметкердің жеке басымен танысуы мүмкін, содан кейін шабуыл жасауды кейінгі кезеңде жүзеге асыруы мүмкін. Бұл табиғи сенім мәселесі қызметкерді әлеуметтік инженерлік

акт болып жатқандығы туралы ерте кезеңде ескертуі мүмкін. Дәстүрлі жаттығу әдістері жеке адамдардың мінез-құлық аспектісін де ескермейді, әр адамда әр түрлі болады. Бір қызметкер шабуылды басқа қызметкер сияқты қабылдай алмауы мүмкін, нәтижесінде мінез-құлық әр түрлі болуы мүмкін [65].

Дәстүрлі жаттығу сессиясы қызметкерлерді белгілі бір уақытта кейбір классикалық шабуылдарды тануға бағыттауы мүмкін, бірақ мұндай жағдайлармен қалай күресуге болатындығын толық көрсете алмауы мүмкін. Бұл мәселенің өзі нақты жағдайлармен бетпе-бет келген адамдарға қиындықтар тудырады. Әлеуметтік инженерия табиғаты бойынша инновациялық болып табылады және күн сайын диверсиялық ұйымдарға жаңа әдістер ойлап табылуда. Бағдарламаларды жобалаудағы технологиялық жетістіктер қолданыстағы дәстүрлі оқыту әдістерін, соның ішінде қолмен еске салғыштарды, постерлер мен скринсаверлерді ауыстыруы мүмкін, себебі олар ескірген. Сонымен қатар, шабуыл режиміндегі белгісіздік әлеуметтік инженерлік қатерлерді ұстаудың дәстүрлі тәсілдеріне қиындық тудырады. Капуто және т.б. [70] дәстүрлі оқыту әдістері енгізілгенімен, қызметкерлер фишингтік хаттарға әлі де теріс әсер ететіндігін атап көрсетті. Оқытуға қанша сағат жұмсалғанына қарамастан, қызметкерлер электрондық поштадағы барлық сілтемелерді тексеруге қызығушылық танытады. Сондықтан модельдеу нұсқасын қамтитын дамыған оқыту әдісі қызметкердің білім базасын дамыту барысында жақсы жұмыс істейтін болады. Дәстүрлі хабардарлық бағдарламаларындағы тағы бір қиындық жаттығу сабақтарына назар аудармау немесе оқу модулін толық оқымау болып табылады. Сонымен қатар, жоғары когнитивті жұмыс жүктемесі жұмыс қысымы мен стресстен персоналды әлеуметтік инженерлік шабуылдарға қарсы оң реакциядан алшақтатуы мүмкін [25,71]. Субъективті ақыл-ой жүктемесі қызметкерлердің нақты және жалған хабарламаларды ажырата алмауына әкелетін жад тапшылығын тудырады. Сонымен қатар, Халеви [72] адамның шешімдері тұтастай алғанда қисынды емес және олардың елеулі қауіп-қатерлерге қарсы пікірлері мен пікірлеріне әсер етуге бейім эмоционалды бейімділікке ие болуы мүмкін дейді. Бұл жағдайлар қызметкерлерді қауіп-қатер туралы білмеуді, олардың ұйымдарының қауіпсіздік жүйелерін асыра бағалауды, тіпті шабуылдаушылардың қабілеттерін төмендетуді қамтуы мүмкін [25].

2.4 Қиындықтардың ұйымдардың қауіпсіздігіне әсері

Бүгінгі күні көптеген ұйымдар негізінен ақпараттық технологияларды қолдануға сүйенеді, бұл оларды өз тұтынушыларының құпиялылығын

қорғауды міндеттейді [73]. Қиындықтар барлық уақытта кәсіпорындардың тұтастығына, сондай-ақ ақпараттық мәліметтердің қол жетімділігіне қауіп төндіреді. Ақпаратты дұрыс пайдаланбау ұйымның іскерлік сабақтастығына тікелей теріс әсер етуі мүмкін [74,75]. Егер бұл шектеулер оқыту мен ақпараттандырудың соңғы бағдарламаларын іске асыру үшін шешім қабылдаушылармен ескерілмесе, ұйымдар өздерінің ақпараттық активтеріне үлкен зиян келтіруі мүмкін. Бұл зияндардың кейбіреулері мәліметтердің ағып кетуін, тұтынушылардың сенімін жоғалтуды, зияткерлік қасиеттерін жоғалтуды және ақпараттық жүйелер қызметінен бас тартуды қамтиды [24,76,77]. Ақпараттық қауіпсіздік бойынша оқыту мен хабардар ету бағдарламаларын өткізудің негізгі мақсаты құпия деректердің жалпы қауіпсіздігін арттыру үшін қауіпсіздік техникасы, құралдары мен саясатын толықтыру болып табылады. Қызметкерлерге қауіпсіздік туралы ақпараттандырудың қажетті бағдарламаларын ұсыну әлеуметтік инженерия және басқа киберқауіпсіздік қатерлерімен күресудің жалпы қауіпсіздігін арттырады [58]. Осы зерттеудегі қарастырылған мәселелер ұйымдарға олардың қауіпсіздігіне осындай жағымсыз әсерлерден аулақ болуға көмектеседі. Бұл қиындықтардың салдары қысқа мерзімді немесе ұзақ мерзімді болуы мүмкін. Егер қиындықтар шешілмесе, қысқа мерзімді әсерге жаттықтырушылар мен тыңдаушылардың уақыты мен күшін ысырап ету кіруі мүмкін, нәтижесінде осы бағдарламалардың жалпы мақсаты орындалмаса, осы оқу сабақтары үшін бөлінген бюджетті жоғалтады. Ұзақ мерзімді әсерге ұйымның әлеуметтік инженерлік шабуылдарға қарсы осалдығының жоғарылауы кіруі мүмкін [66]. Ұйым тиімді оқыту және ақпараттандыру бағдарламаларын өткізу кезінде туындаған қиындықтарға байланысты ең үлкен әсердің бірі - бұл мәліметтердің, персоналдың және оның әлеуметтік және технологиялық инфрақұрылымының қауіпсіздігіне қауіп төндіреді [44]. Әсер етуі мүмкін құпия деректердің көптеген түрлеріне бизнес жоспарлар мен процедуралар, қаржылық мәліметтер, қызметкерлердің жеке мәліметтері, жалақы туралы мәліметтер және басқалары кіреді. Тіпті құпия деректер қорғалған техникалық серверлерде сақталса да, әлеуметтік инженерлер ескерілмеген жағдайда, сол қиындықтардың әсерін пайдалана алады. Тиімді оқыту және ақпараттандыру бағдарламаларының болмауы қызметкерлер арасында қауіпсіз мәдениетті қалыптастыруға әсер етеді. Жалпы, АТ емес қызметкерлер әлеуметтік инженерлік шабуылдарға күдіктенбейді, әсіресе әлеуметтік инженерлер оларға жұмысына қол жетімділікті өзгертуде немесе парольдерін қалпына келтіруде белгілі бір көмек көрсеткен кезде. Әлеуметтік инженердің қызметкерлерге жақындауының тағы бір тәсілі - сыйақы беру немесе үлкен мүмкіндікке үміт беру [78].

Мұндай трюкты түсінудің жеткіліксіздігі ойдағыдай бұзушылыққа әкелуі мүмкін. Содан кейін әсер, егер бұзушылық сәтті болса, кәсіпорынға үлкен шығындарды әкелуі мүмкін. Оқыту мен хабардар ету бағдарламаларының қиындықтары сонымен қатар ұйымның әлеуметтік инженерлік шантажға осал болуын тудырады. Ақпараттық қауіпсіздік туралы білімдері шектеулі қызметкерлердің болуы, әлеуметтік инженерлік шабуылдар арасындағы алшақтықты кеңейтуі мүмкін [79]. Егер қызметкерлерде әлеуметтік инженерия саласындағы алаяқтықтың соңғы әдістері туралы жаңартылған ақпарат болмаса, олар шабуылдаушыларға ұйымдастырушылық ақпараттық жүйелерге қол жеткізуге ашық жол ұсынуы мүмкін. Егер әлеуметтік инженерлер бейхабар қызметкерлер арқылы қол жеткізе алса, компаниялар жақында жасалған төлемдік бағдарламалар шабуылынан зардап шегуі мүмкін. Шабуылшылар ұйымдастырушылық жұмыс станциясын немесе ақпараттық жүйені қатырғаннан кейін, келіссөздер процесі сәтсіздікке ұшырап, мауды деректердің жойылуына әкелуі мүмкін [60]. Қысқаша айтқанда, әлеуметтік инженерлік шабуылдарға қарсы оқыту мен ақпараттандыру бағдарламаларының қиындықтарын ескермеу құрбан болуға әкелуі мүмкін. Қауіпсіздікті жақсылап үйрету әлеуметтік инженерлік шабуылдардан қорғанудың бірінші жолы болып саналады [44]. Сонымен қатар, адамдарды алдау және жаңылыстырудың әлеуметтік инженерия техникасына қарсы қауіпсіздік техникасы бойынша қажетті дайындықты алмаудың салдары кәсіпорындардың беделіне нұқсан келтіруі мүмкін. Ұйымның беделі басқа кәсіпорындармен және клиенттермен тиімді қарым-қатынас үшін өте мауды. Беделді жоғалту ұйымның жұмысына, сондай-ақ қызметкерлерді ұстап қалуға елеулі зиянды әсер етеді [66]. Егер ұйымның беделіне нұқсан келсе, сол фирманың жалпы сеніміне де әсер етуі мүмкін [80]. Қысқаша айтқанда, хабардар болмау салдарынан қызметкерлердің қауіпті әрекеттері пайдаланушылардың өздеріне де, олардың ұйымдарының жалпы беделіне де үлкен зардаптар мен зиян келтіруі мүмкін [81].

2.5 Әлеуметтік инженерлік білім беру мен ақпараттандыру мәселелерін шешудің стратегиялары

Кәсіпорындардың әлеуметтік инженерияға қарсы оқыту және хабардар ету бағдарламаларын ұсыну кезіндегі басты және жетекші проблемаларының бірі - оқыту бюджетінің болмауы. Қиындық әлемдік экономикалық ереуілдер нәтижесінде одан әрі арта түседі. Қазіргі бәсекеге қабілетті экономикада көптеген кәсіпорындар өз шығындарын барынша азайтуға тырысады, әсіресе олардың пайдалану құнына кірмейтін шығындар туралы. Өкінішке орай,

көптеген ұйымдар оқыту бюджеттеріне басымдық бермейді, өйткені олар қажет [44,69]. Барлық қызметкерлердің бірдей ақпараттылық деңгейіне ие еместігін ескере отырып, оқыту шығындарын көптеген стратегиялармен азайтуға болады. Оқу шығындарына байланысты қаржылық шектеулерді жоюдың бір стратегиясы - қызметкерлерді олардың қазіргі осалдығын түсіну үшін тестілеуді бастау. Мамандандырылған оқыту офицерлерінің бағалау тесті немесе фишингтік электрондық пошта арқылы тестілеу қазіргі кездегі хабардарлық деңгейін анықтауға көмектеседі. Қызметкердің ерекше осалдығы анықталғаннан кейін, ұйымдар ұйым үшін қауіптілігі жоғары деңгейге ие адамдарға бағытталған мақсатты сессия құруға бағытталуы мүмкін. Бұл сессиялар осал пайдаланушылар үшін арнайы жасалуы керек. Сондай-ақ, әлеуметтік инженерлік талпыныстарға жиі ұшырамайтын қызметкерлерге хабардар ету бағдарламасы ұсынылады, ал оның ұзақтығы қысқа болады. Бұл әдіс оқыту мен ақпараттандыру бағдарламаларының құнын барлық қызметкерлер үшін бірдей сессияларды өткізумен салыстырғанда азайтуға көмектеседі. Барлық қызметкерлерге ұқсас оқыту және ақпараттандыру бағдарламаларын ұсыну қосымша шектеулер тудырады. Кәсіпорындардың көпшілігі әлі күнге дейін экран сақтағыштары мен плакаттарын қолдану арқылы қызметкерлерді хабардар етудің дәстүрлі әдістерін қолданады [5]. Алайда мұндай кең тараған әдістер әртүрлі ұйымдық иерархияларда тиімділікті төмендетуі мүмкін. Жалпы айтқанда, басшылар жалпы рөлдерді орындайтын жалпы қызметкерлерге қарағанда әр түрлі типтегі деректерді бұзу тәсілдеріне ұшырайды. Мысалы, қоқыс шығаруға жауапты адам сияқты жалпы қызметкерлерге әлеуметтік инженерлер қолданатын ақпараттарды жинау кезінде қоқыс тастайтындай сүңгу қаупін болдырмаудың алдын-алу әдістері туралы оқыту қажет [6,34]. Пенетрациялық тестілеу бұл қиындықты жеңудің өте пайдалы стратегиясы бола алады. Бұл корпорациялардың құпия деректерді ұрлауға тырысатын нақты шабуыл әрекеттерін модельдеуге бейімделетін әдістерінің бірі [82].

Сол сияқты, алдын-алудың бірдей құралдары мен әдістерін ұйымның менеджерлері мен басқарма мүшелеріне қолдануға болмайды, өйткені олар фишингтік қоңыраулармен жиі ұшырасады. Жұмыс берушілер иерархияның әр деңгейінде анықталған әлсіз жақтар үшін рөлдік араласуды жобалауға назар аудара алады. Ену тестілеуінің нәтижелерін нығайту үшін оқыту мен хабардар ету бағдарламалары тиімді және заманауи болуы керек. Тиімділік қызметкерлерден талап етілетін профилактикалық іс-әрекеттерді бөліп көрсетуден және оларға тақырыптың не үшін мауды екенін түсінуді кеңейту арқылы профилактикалық қатынасты қалыптастырудан туындайды [83]. Әлеуметтік инженерия адамның мүмкіндіктерімен байланысты болғандықтан,

қызметкерлердің мінез-құлқындағы шектеулер оқыту мен ақпараттандыру бағдарламаларының тиімділігіне қиындық туғызады. Барлық қызметкерлер арасында мінез-құлықтың нақты шектеулеріне бейімділік, мәдени ықпал және когнитивті жағымпаздық жатады [27,58,84]. Алдыңғы зерттеулерде [62-64] ұйымдарда әлеуметтік инженерлік шабуылдардың мүмкіндігін арттыратын негізгі себептердің арасындағы мінез-құлық шектеулері көрсетілген. Ең алдымен, оқыту және ақпараттандыру бағдарламалары кезінде қызметкерлер арасында байқалатын талаптарға сәйкес келмейтін мінез-құлық қауіпсіз мәдениетті қалыптастыру үшін еңсеру керек мәселелердің бірі болып саналады. Ақпараттық қауіпсіздік ағып кеткен жағдайда, фирмалар үшін оқшаулау шығындары бірінші кезекте оқыту қарастырылғаннан гөрі көп болуы мүмкін. Осындай мінез-құлық шектеулері мен біржақты көзқарастарға қарсы тұру үшін ұйымдар қауіпсіздік туралы нақты нұсқаулықтар құрып, барлық қызметкерлерге олар туралы білім беруі керек. Оқыту және ақпараттандыру бағдарламаларында осындай қиындықтарға қарсы тұрудың негізгі стратегияларының бірі - қызметкерлер қауіпсіздік тәуекелдерін азайту үшін олардың мүмкіндіктерін асыра бағаламауды үйренуі керек. Керісінше, қызметкерлерге қауіпсіздік туралы білімдерін жалпы қауіпсіздікте оң нәтижелі нәтиже алу үшін пайдалануға болатындығы туралы хабарлау бағдарламалары арқылы үйрету керек. Қызметкерлерге арналған ақпараттандыру науқандары жеке көзқарасты жоққа шығарып, мұндай шабуылдар «менде болмайды» деген ойларды жоюы керек [70,85-87]. Топ мүшелері арасындағы үйлестіру оқыту мен хабардар ету бағдарламаларында қиындықтар туғызады. Әлеуметтік инженерлік шабуылдар қарқынды және дамып келе жатқандықтан, ұйымдар оқытудың заманауи әдістерін қолдана отырып, хакерлік қатерлерді болдырмауға тырысады. Бұл әдістерге мауды ойындар, виртуалды зертханалар, тақырыптық хабардарлық бейнелер мен модульдер кіреді [59]. Соған қарамастан, соңғы әдістер туралы білетін ақпараттық қауіпсіздікке мамандандырылған оқыту бойынша үйлестірушілердің болуы қауіпсіздік туралы хабардар болмауынан туындаған осалдықтарды азайтудың алдын-алу шарасы ретінде мауды болып табылады. Тренингтің үйлестірушілері мен нұсқаушылары барлық қызметкерлерге қауіп-қатерді бақылаудың қандай аспектісімен айналысатындығы туралы нақты хабарлау үшін қауіп-қатерді болдырмау схемаларын құрудың маудылығын атап өтуі керек [9]. Әлеуметтік тұрғыдан жасалған қауіп-қатерлерді ұстау стратегияларына бірлескен кездейсоқ реакциялар процедураларына негізделген дайындық жаттығуларын өткізу кіреді. Әр түрлі ұйымдық топтар арасындағы өзара тәуелділіктің егжей-тегжейлі сипаттамасын картаға түсіру өте мауды. Олар фирмаға негізделген оқыту мен ақпараттандыру

бағдарламаларын жеңілдету үшін барлық қажетті әрекеттерді дәйектілікпен қамтуы керек. Қысқаша айтқанда, тренингтер мен хабардар ету бағдарламалары қызметкерлердің әлеуетін дамытуды жақсартады, олар ұйымдық осал тұстарға қатысты кеңірек көріністі күтеді [31,33,34]. Ақырында, динамикалық әлеуметтік-инженерлік шабуылдармен жұмыс істеуді үйлестіруді жақсарту үшін координаторлар мен нұсқаушылар жаңартылған болуы керек және ішкі тренингті қалай дамыту керектігін жақсы білу үшін соңғы конференцияларға үнемі қатысуы керек. Оқытудың жаңа әдістері арқылы әлеуметтік инженерияға қарсы тұру өзара тәуелділіктің қиындықтарына тап болады. Кейбір тренинг жаттығулары әр қатысушыға әлеуметтік инженерлік шабуылдардан туындайтын қауіпсіздік тәуекелдерін бақылау үшін бір команда ретінде үйлестіре отырып орындауға тиісті рөлдерді көрсетеді. Алайда, бұл бірлескен міндеттер жекелеген қызметкерлер үшін өзара тәуелділіктер туғызуы мүмкін, олар жеке жұмыс кезінде олардың жұмысын шектейді. Мұндай жағдайларда, қызметкерлер бір-біріне тәуелді жұмыс істеуге үйретілген кезде, олар өздерінің ұйымдарын ашық қалдырып, әлеуметтік қауіпті тежеу үшін келесі жауапкершілікті білмейді. Өзара тәуелділік әлеуметтік инженерлер үшін ойықтар мен ашық есіктер жасайды [7,45,88].

Сонымен қатар, алдыңғы зерттеулер [9,89] әлеуметтік инженерлердің осындай әрекеттерді синхрондау және ресурстарды бөлісу арқылы өзара тәуелділікті пайдаланатынын көрсетеді. Әлеуметтік инженерлер бүкіл ұйымға әсер ете алатын ауқымды шабуыл жасайтын арнайы желіні жасайды. Мұның артында айла-шарғы - жалғыз басты қызметкерлерді фишинг арқылы ақпараттық жүйеге енгізу. Өзара тәуелділікке қарсы тұру стратегиялары қолданушыларға байланысты қатынасты жақсарту және қызметкерлерді әлеуметтік тұрғыдан жасалған шабуылдарды қамтудың келесі қадамына автоматты түрде болжам жасауға итермелеу үшін арнайы дайындалған оқыту және хабардар ету бағдарламаларын қамтуы мүмкін. Стратегиялық шараға сонымен қатар, өмірдегі имитацияланған рөлдерді қолданатын және барлық қызметкерлер мен менеджерлерді қатердің алдын алу үшін қатысатын Үстел үстіндегі жаттығулар кіруі мүмкін. Үстел үстіндегі жаттығулар желіде де, қағаз жүзінде де жүзеге асырылады және қатысушы агенттерді анықтауға және шешім қабылдау сапасының дұрыс ағымына арналған. Жаттығу қызметкерлерге өздерінің ұйымдарының апаттарға қарсы әрекет жоспарымен ыңғайлы болуды көздейді. Фирманың қауіпсіздік жоспарындағы рөлді тану модельдеу қауіпсіздік кемшіліктерін анықтауға көмектеседі. Бұл олқылықтар ұйымдар шешкен кезде фирмалардағы қауіпсіздікке мүдделі тараптар арасындағы байланысты жақсартуға көмектеседі және қауіпсіздік

жоспарларын орындаудың жаңа тәсілдерін білуге көмектеседі. Фирмалардың алдында тұрған тағы бір қиындық - әлеуметтік инженерлік хакерлік шабуылдардың инновациялық тәсілдеріне дайындық. Тренинг пен хабардар ету бағдарламасының ең соңғы құралдарының өзінде қызметкерлер құрбан болудан қорқу сияқты осалдықтарға ие болуы мүмкін. Хакерлер кері психологияны таңдап алған мақсаттарына жем болатындығын қамтамасыз ету үшін қолдана алады [62-64]. Тренингтің стратегиясында қызметкерлерге хакерлердің мүмкіндіктерін төмендетуден аулақ болу туралы нұсқаулар болуы керек. Әлеуметтік тұрғыдан жасалған шабуылдар әлеуметтік-эмоционалды перспективалар мен сенім өлшемдері сияқты осалдықтарға сүйенеді. Хакерлермен қарым-қатынас ұйымдарға қауіп төндіреді. Қызметкерлер арасындағы жеткіліксіз дайындыққа қарсы стратегияларға нақты сценарийлер мен жағдайлық зерттеулерді қамтитын оқыту және ақпараттандыру бағдарламалары кіреді. Бұл сценарийлер хакерлер құртып алуы мүмкін әлсіздіктер туралы білім қорын арттыра алады. Қысқаша айтқанда, оқыту мен ақпараттандыру бағдарламаларын іске асыру барлық жастағы пайдаланушылар позитивті және өзін-өзі дамытатын іс-шаралар жүргізу үшін технологияны еркін қолдана алатын қауіпсіз киберлік ортаға ие болу жолындағы шешуші қадам болып табылады. Технологияның дамуы адамдарға хакерлер мен киберқылмыскерлердің әлеуетті нысанасына айналуына байланысты әлеуметтік инженерлік қатерлермен күресудің ең тиімді әдісі болып саналады [4,6,10– 12,44,90–92].

Бұл зерттеу әлеуметтік инженерияға қарсы оқыту және ақпараттандыру бағдарламаларын жүзеге асырудан туындаған қиындықтарды жеңуге ықпал ететін факторларды қарастырады. Бүгінгі таңда қаржы және жабдықтау тізбектері сияқты бизнес функциялары үлкен ақпараттық жүйелерге бірігеді. Ақпараттық жүйелердің интеграциясы ұйымның осалдығын арттырады. Осындай өзара байланысты ақпараттық жүйелерді қолдана отырып, қызметкерлердің әлеуметтік медиаға қол жетімділігі зиянды әлеуметтік инженерлердің шабуыл қаупінің артуына әкелуі мүмкін. Сонымен қатар, егер әлеуметтік инженерлер қолданатын ең жаңа техникалар туралы ақпараттық қауіпсіздік туралы хабардар болу деңгейі жақсы сақталмаса, ұйымдар олардың шабуыл қаупін арттырады. Әлеуметтік инженерлік шабуылдар өзгермелі технологиялармен де, қауіпсіздік шараларымен де дамуға арналғандықтан, мұндай қауіп-қатерлерге қарсы білім қорын дамыту және дамыту үшін санатталған оқыту қажет. Ақпараттық қауіпсіздік бойынша оқыту мен хабардар ету бағдарламаларының негізгі мақсаты - қызметкерлерге кез-келген әлеуметтік инженерлік зиянды әрекеттерді анықтау, ажырату және есеп беру дағдыларын дамытуға мүмкіндік беру. Оқыту мен хабардар ету

бағдарламаларын ұсыну кезінде кәсіпорындармен кездесетін негізгі проблемалардың бірі - оқыту бюджеттерінің болмауы, әсіресе әлемдік экономикалық ереуілдер кезінде. Бұл жұмыста оқыту құнын төмендетуге арналған кейбір жұмыс стратегиялары келтірілген. Қызметкердің жағымсыз мінез-құлқы немесе ақпараттық қауіпсіздік пен ұйымдық қауіпсіздік мәдениетін түсінбеуі құпия осалдық болып саналады. Бұл зерттеу бұдан әрі ұйымдарда қауіпсіздік шешімдерін қабылдаушылар тұрғысынан қиындықтарды шешудің стратегияларын ұсынады. Осы жұмыста кейбір кездесулер бірлескен кездейсоқ жауаптарға негізделген дайындық жаттығуларын өткізуді ұсынатын бірнеше ұсынымдар келтірілген. Ақпараттық қауіпсіздік пен білім беру бағдарламаларын арттыру ұйымдарға әлеуметтік инженерия әдістеріне қарсы жақсы нәтижелерге қол жеткізуге көмектеседі.

3 ҚАЗАҚСТАНДАҒЫ БАНКТЕР ЖҮЙЕСІНЕ СИПАТТАМА ЖӘНЕ ОЛАРДЫҢ ҚАУІПСІЗДІК ДЕҢГЕЙЛЕРІНЕ ТАЛДАУ

3.1 Қазақстандағы банктер қаупсіздігіне шолу

Пандемиядан туындаған қаржы саласын цифрландыруды жеделдету Киберқауіпсіздіктің жоғары қатерлеріне байланысты болады, бұл ретте Қазақстан тәуекел аймағында тұр.

Comparitech компаниясы Киберқауіпсіздік бойынша әлемнің 76 елінің жаңа рейтингін жасады, онда қауіп деңгейі, қаржылық зиянды БҚ шабуылдарының саны, кибершабуылдарға дайындық және киберқауіпсіздік туралы заңнама сияқты факторлар ескерілді. Осы рейтингке сәйкес Қазақстан 2020 жылы 26-орында тұр. Салыстыру үшін, әлемдегі ең аз киберқауіпсіз ел-Алжир-бұл рейтингте бірінші орында. Басқа осал елдер — Тәжікстан (2 орын), Түрікменстан (3), Сирия (4) және Иран (5). Бірақ ең қауіпсіз елдер Дания (76 орын), Швеция (75) және Германия (74) болды. Бізге Comparitech есептегендей, рейтингке енген бірде-бір ел барлық бағыттар бойынша "өз класында ең жақсы" болған жоқ. Барлық талданған елдер бағалаудың белгілі бір параметрлері бойынша айтарлықтай жақсартуларды қажет етеді.

Біздің еліміз рейтингте алғаш рет пайда болды, сондықтан бір жыл ішінде киберқауіпсіздік көрсеткіштерінің өзгеруі мүмкін емес. Алайда, рейтингтегі мұндай жоғары орын АҚ тұрғысынан елеулі қиындықтар туралы айтады. Рейтингтен ҚР-ның жеке көрсеткіштері: зиянды БҚ-ны жұқтырған ұялы телефондардың 4,8% - ы; пайдаланушылардың 0,9% - ы қаржылық зиянды шабуылдарға бейім; зиянды БҚ-ны жұқтырған компьютерлердің 9,22% - ы; криптомайнерлердің шабуылдарының 3,66% - ы. Бұл пайдаланушы құрылғыларында (мобильді және стационарлық) сақталған деректер өте осал екенін көрсетеді. Карантиндік шектеулерге байланысты ҚР-да тіркелген онлайн-төлемдердің өсуін ескере отырып, қазақстандықтардың қаржылық ақпаратының қауіпсіздігіне қатысты елеулі қауіптер бар.

Азия, ТМД және Балтық елдеріндегі" Касперский Зертханасының " басқарушы директоры Евгений Питолиннің айтуынша, Қазақстанның банк секторы үшін ең өзекті киберқауіптерді мыналар деп санауға болады: DDoS-шабуылдар мен өңірлік кеңселер мен филиалдарға жасалған кибершабуылдар. Ал банк клиенттері үшін төнетін қатерлердің ішіндегі ең өзектісі-Интернет-банкингке, оның ішінде банк клиенттерінің жеке деректерін алуға бағытталған фишингтік схемалар көмегімен шабуылдар, сондай-ақ зиянды БҚ.

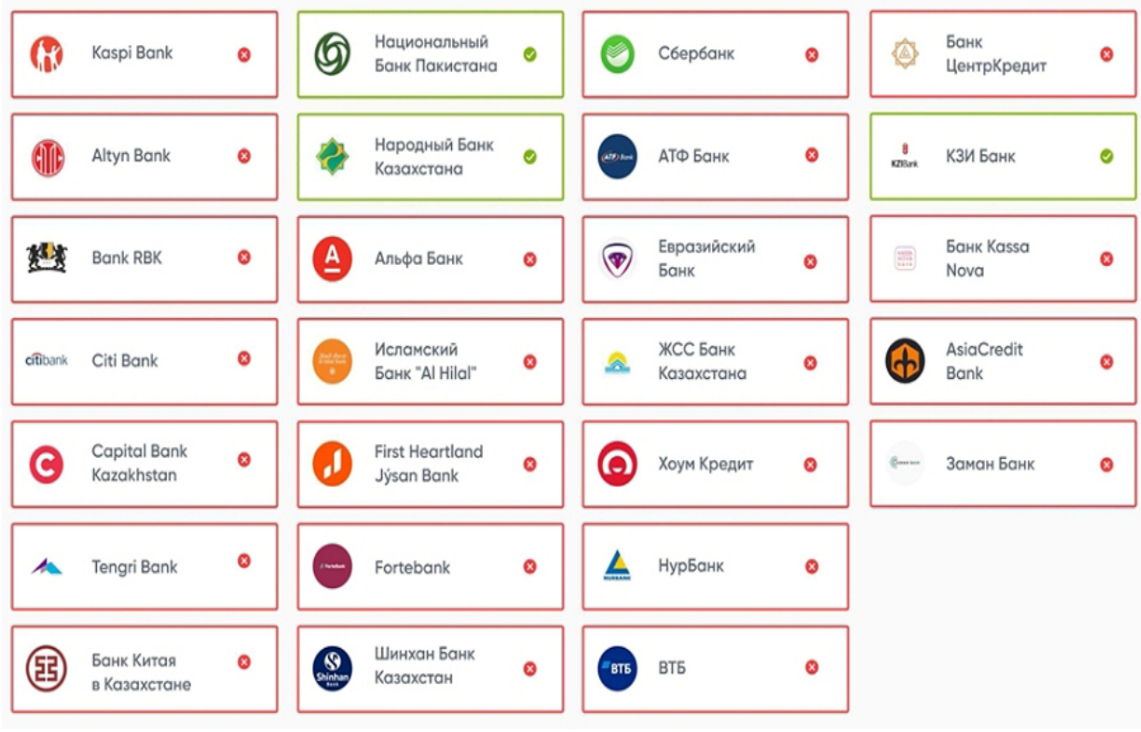
КШТТО-да Қазақстан банктерінің ресми сайттары қаншалықты қауіпсіз екендігі туралы айтылды. Зерттеу WebTotem бақылау және қорғау шешімінің көмегімен жүргізілді. Есеп авторлары түсіндіргендей, пайдаланылған бағалау әдістемесі ең үздік әлемдік тәжірибені, бағдарламалық жасақтама мен кәсіби қауымдастықтардың танымал әзірлеушілерінің ұсыныстарын, сондай-ақ жиі қолданылатын стандарттарды ескереді. Бұл ретте зерттеу саласына интернет-банкинг сервистері кірмеді, Екінші деңгейдегі 26 банктің веб-ресурстарының

қорғалу жай-күйі ғана бағаланды. Зерттеу веб-серверлер мен байланысты компоненттер үшін ұсынылған параметрлерді орындау тәсілдерін қолдануды талдауды қамтыды.

"Зерттеудің басты мақсаты-көпшілікке қол жетімді банк ресурстарының қауіпсіздік деңгейін бағалау. Бұл Банктің ресми сайты туралы. Зерттеу барысында біз шабуылдаушыларға қандай ықтимал векторлар қол жетімді болуы мүмкін екенін анықтауға тырыстық", — деп түсіндірді КШТТО. Банктердің веб-сайттары бірнеше тәуекел факторлары бойынша бағаланды.

3.2 CMS ескі нұсқаларының жәй-күйі

Егер CMS немесе оның компоненттері жаңартылмаса, онда ескі нұсқалардың осалдықтарын пайдалануға мүмкіндік беретін пайдалану мүмкіндігі жоғары. CMS-тің ескірген нұсқасын әзірлеуші қолдамайды, сонымен қатар қауіпсіздікке қауіп төндіреді. Осы фактор бойынша банктердің 26 доменінің үшеуі ғана "өтті": "Қазақстандағы" Пәкістан Ұлттық Банкі" ЕБ "АҚ," Қазақстан Халық жинақ банкі "АҚ, "Қазақстан-зират интернешнл Банкі"Еншілес банкі" АҚ.



4-сурет - Қазақстандағы ірі банктер тізімі

3.3 Жүктеу жылдамдығы

Жүктеу жылдамдығын бағалау сайттың жүктелуін модельдеу арқылы алынған FCP және FID деректеріне негізделген. Ең жақсы өнімділік тәжірибесін тестілеу сайттың жүктемелерге тұрақтылығын талдау үшін жасалады. Сонымен қатар, төмен өнімділік шабуылдаушыларға веб-ресурсты шамадан тыс жүктеуге мүмкіндік береді, бұл оны пайдаланушылар үшін қол жетімді емес етеді. Банк домендерінің 46% — ында жүктеу жылдамдығы жоғары, тағы 46% — да орташа және 8% - да төмен екендігі белгілі болды.

Жоғары жылдамдық 80-100 %.

Орта жылдамдық 50-79 %.

Төмен жылдамдық 0-49 %

5-сурет - Банктердегі жүктеу жылдамдығы

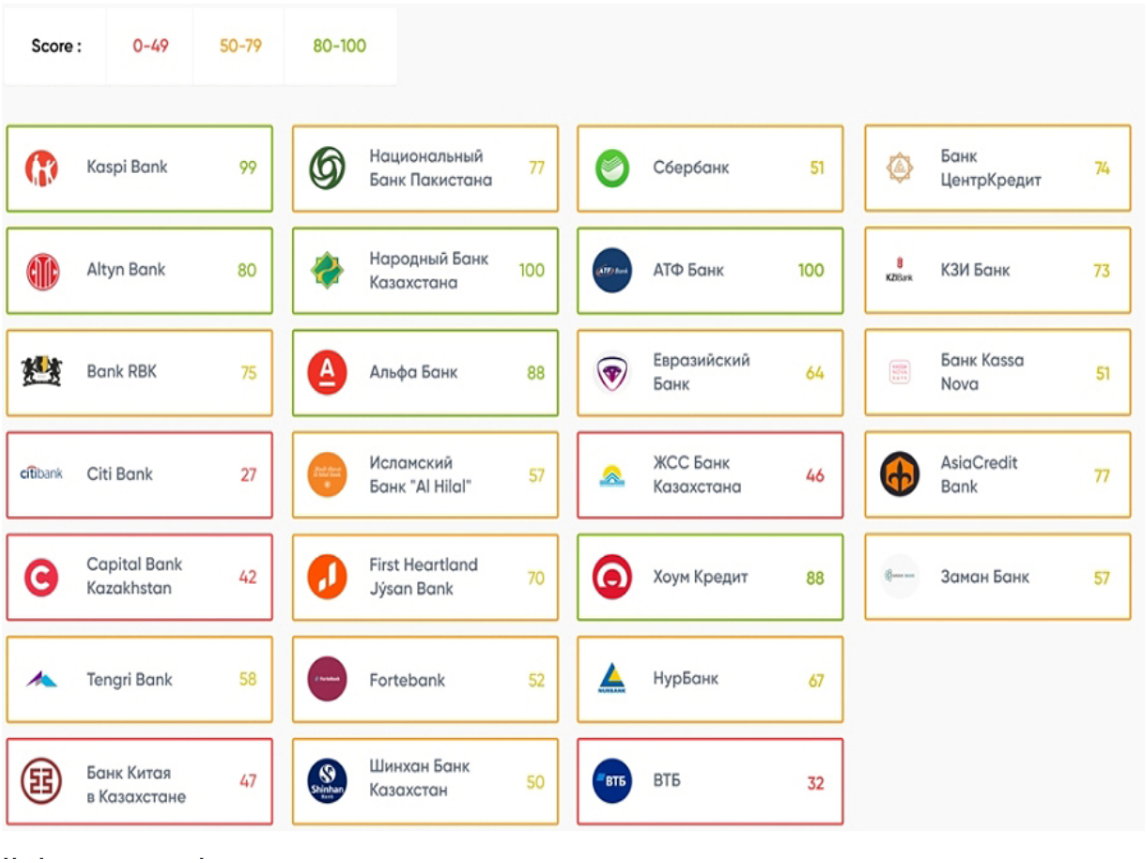
3.4 Банктердегі IP доменінің беделі

Жақсы бедел веб-ресурстың қауіпсіз екенін білдіреді, ал антивирустың "қара тізім" мәртебесі келушілерге қауіпсіздікке төнетін қауіптер туралы ескертеді. Егер веб-ресурс бедел негіздерінің бірінің қара тізіміне енгізілсе, оны браузерлер кіруден бұғаттай алады және тіпті іздеу нәтижелерінен жоғалып кетуі мүмкін. Бұл өз кезегінде трафиктің жоғалуына, клиенттердің сеніміне және демек ақшаға әкеледі.

Жалпы, Forcepoint ThreatSeeker-тің бір ғана домені "ықтимал зиянды" ретінде анықталып, осы жүйенің қара тізіміне — "Банк Kassa Nova"АҚ енді.

3.5 Контентті қорғау саясаты, CSP

Content Security Policy-XSS-шабуылдарды пайдалану кезінде туындайтын тәуекелдерді азайтудың негізгі тәсілдерінің бірі. CSP көмегімен сайт әкімшісі парақтарда рұқсат етілген атрибуттарды анықтай алады (қаріптер, стильдер, суреттер, JS сценарийлері, SWF және т.б.). Қауіпсіздік тақырыптарының болмауы келушілерге бағытталған шабуылдарға әкелуі мүмкін. Мұндай шабуылдардың ішінде-зиянды кодты енгізу, XSS және веб-ресурсты зиянды кодқа өзгерту. Домендердің 23% — ы жоғары, 58% — ы орташа және 19% - ы төмен екендігі белгілі болды.



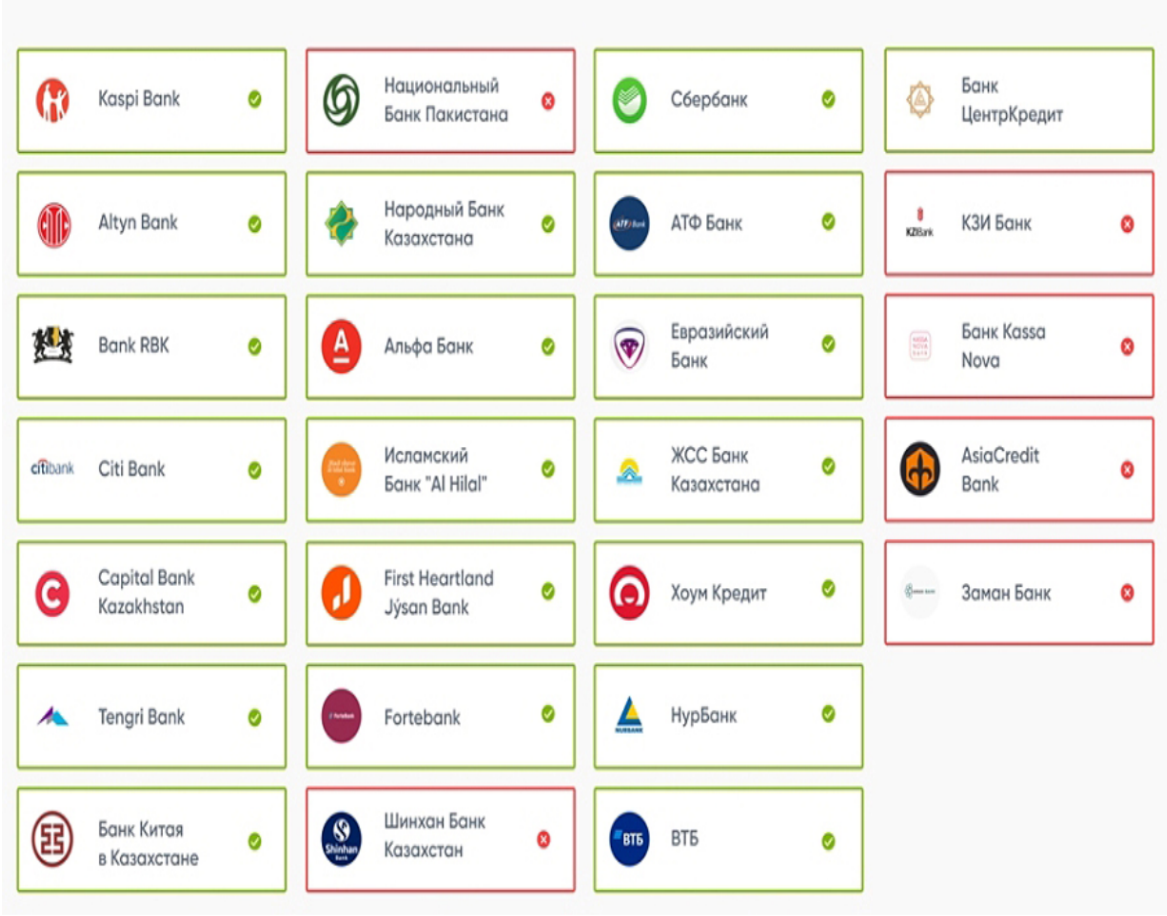
6-сурет - Контентті қорғау саясаты

3.6 Трафикті шифрлау

Ең маңызды параметрлердің бірі-SSL/TLS параметрлерін тексеру, өйткені бүгінгі таңда бұл криптографиялық протоколдар интернетте қауіпсіз деректермен алмасуды қамтамасыз етудің ең танымал әдісі болып табылады. Егер бұл параметрлер дұрыс орындалмаса, деректерді ұстап алу мүмкіндігі бар. Бұл "ортадағы адам" класындағы шабуылдардың бір түрі. Мұндай шабуылдар сайт пен пайдаланушы арасында жіберілетін деректерді ұстап

алатын және өзгерте алатын делдалдың болуын білдіреді. Мұндай шабуылдардың құрбандары, әдетте, шабуылдаушылардың олардың арасындағы ақпарат алмасу процесіне араласуын білмейді. Зардап шеккендер веб-сайтқа тікелей кіретініне сенімді болған кезде, трафик Барлық жіберілген деректерді алатын шабуылдаушының аралық түйінінен өтеді (бұл логиндер, парольдер, ПИН-кодтар және т.б. болуы мүмкін).

Осы тексеру нәтижелері бойынша бірнеше банктерде SSL/TLS: "Қазақстандағы "Пәкістан Ұлттық Банкі" ЕБ" АҚ, "Шинхан Банк Қазақстан" АҚ, "Қазақстан-зират интернешнл Банкі "Еншілес банкі" АҚ, "Банк Kassa Nova" АҚ, "AsiaCredit Bank (Азия Кредит Банк)" АҚ, "Заман-Банк "Ислам банкі"АҚ проблемалары анықталды.



7-сурет - SSL/TLS мәселесі кездескен банктер

3.7 Ақпараттың ағымы.

Ақпараттың кез-келген ағымы компания үшін белгілі бір жағымсыз салдарға әкеледі. Тексеру нәтижелері бойынша 13 банкте ақпараттың жария болу жағдайлары анықталды, барлығы осындай 386 жағдай тіркелді.

8-сурет - Ақпараттар ағымы бойыншы тіркелеген банктер

3.9 Желілік қауіпсіздік

Веб-Сервердің өзі тікелей пайдаланбайтын порттарға талдау жасалды (80 және 443 порттар). Ашық порттардың болуы осалдық болмаса да, қауіпсіздіктің ең жақсы тәжірибесі тұрғысынан веб-серверде веб-қызметтермен жұмыс істеуді білдіретіндерден басқа ашық порттар болмауы керек.

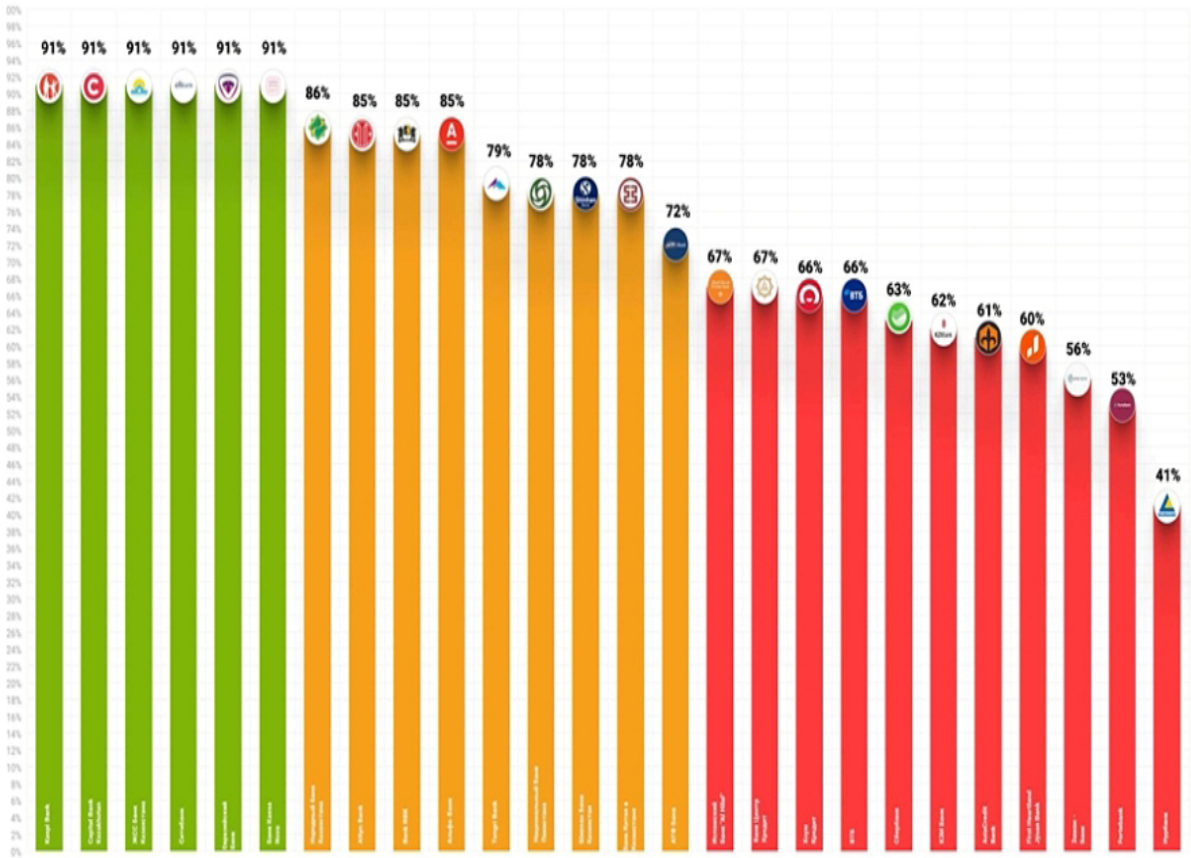
Alert Logic зерттеуі туралы мәліметтер бар, оның барысында 2018 жылдың қарашасынан 2019 жылдың сәуіріне дейін жасалған 5000-нан астам шабуыл талданды. Шабуыл жасау үшін ең көп қолданылатын порттар 22, 80 және 443 екендігі белгілі болды. WannaCry — мен сенсациялық оқиғаны еске түсірген жөн-445 ашық TCP порты бар компьютерлер бұзылды. Бұл шабуылдардың сәтті болуына себеп болған периметрді бақылаудың болмауы. КШТТО зерттеулерінің мәліметтері бойынша, ҚР сегіз банкінде ашық порттар анықталған.

9-сурет - Порттары ашық банктер тізімі

3.10 Веб-ресурстардың пошта серверінің қауіпсіздігі

Электрондық пошта трафигінің 90% - дан астамында спам, фишинг, зиянды бағдарламалар және басқа да қауіптер бар. Электрондық пошта-Ransomware және зиянды бағдарламалар үшін инфекцияның негізгі векторы. Осылайша, "Касперский Зертханасының" деректері бойынша спамның үлесі Қазақстанның барлық пошта трафигінің жартысына жуығын (48%) құрады. Сонымен қатар, 2019 жылы Касперский Зертханасының шешімдері қолданушылардың фишингтік сайттарға кіруге үш миллионға жуық әрекетін бұғаттады. Ал Check Point Software Technologies Украина, Грузия және ТМД елдеріндегі өкілдігінің басшысы Александр Савушкин қаржы секторына жиі шабуыл жасайтын схемалардың бірі — BEC (Business Email Compromise) туралы айтып берді, ол сөзбе-сөз "іскерлік Электрондық поштаның бұзылуы"деп аударылады. Зиянкестердің негізгі мақсаттары әдетте акциялар, венчурлық капитал және бухгалтерлік есеп болып табылады.

Банктердің веб-ресурстарын пошта серверінің қауіпсіздігі тұрғысынан бағалау кезінде веб-ресурстың пошта сервері осындай қауіптердің алдын алу үшін дұрыс конфигурацияланғанын тексеру жүргізілді. Email security бірнеше тексерулер жүргізілді, олардың нәтижелері бойынша банктердің әрқайсысы үшін индекс анықталды. "Жасыл" аймақта алты банк болды: "Kaspi Bank" АҚ, "Capital Bank Kazakhstan" АҚ, "Қазақстанның тұрғын үй құрылыс жинақ банкі" АҚ, "Ситибанк Қазақстан" АҚ, "Еуразиялық банк "АҚ,"Банк Kassa Nova" АҚ.



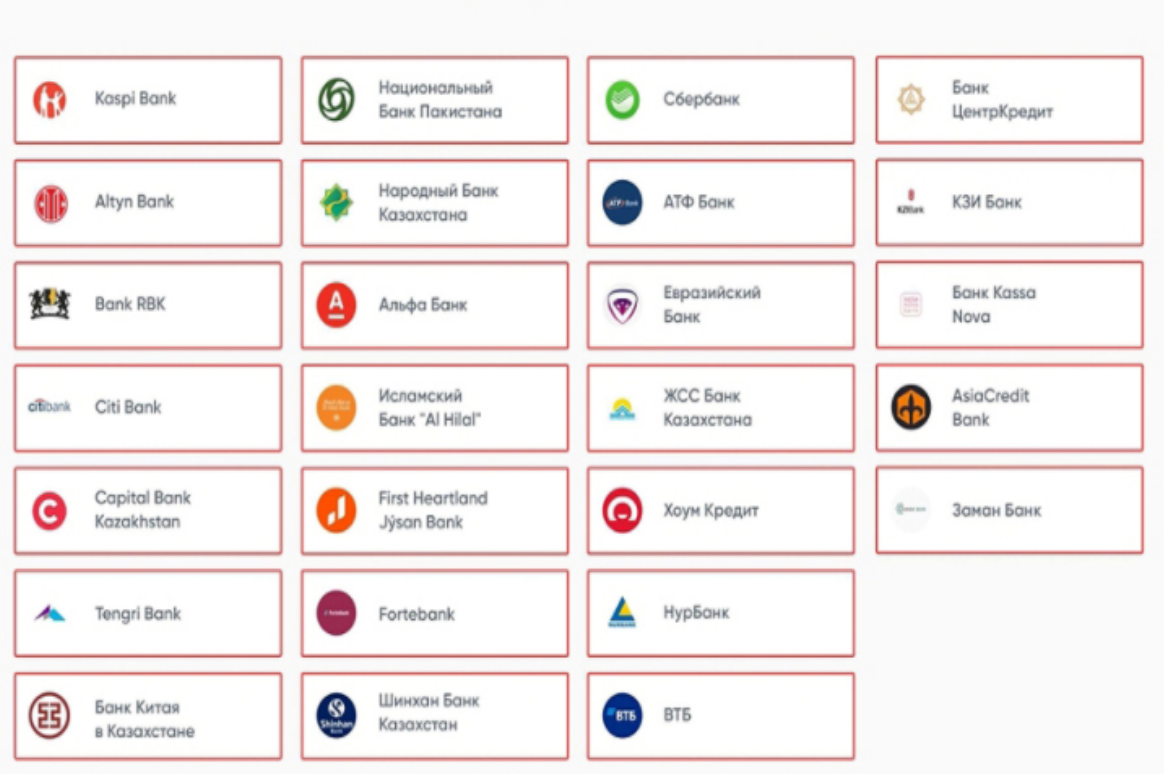
10-сурет - Веб-ресурстардың пошта серверінің қауіпсіздігі бойынша график

Жалпы ағымдағы жағдайы

Осы параметр аясында сыртқы белгілер бойынша ресурсты бұзу үшін тексеру жүргізілді. Оларға сайтта зиянды сценарийлердің немесе желілік кеншілердің болуы, сайттың жылдамдығын тексеру, пайдаланушылардың вирустарға шағымдары кіреді. Осы параметр бойынша банктердің барлық зерттелген сайттары "таза" болып шықты.

GDPR сәйкестігі

Дербес деректер рұқсатсыз немесе заңсыз өңдеуден, кездейсоқ жоғалудан, зақымданудан немесе жойылудан қорғауды қоса алғанда, олардың тиісті қауіпсіздігін қамтамасыз ететіндей өңделуі тиіс. GDPR талаптарына сәйкес веб-сайттар пайдаланушыларға олардың жеке деректері мен cookie файлдары қалай өңделетіні, сондай-ақ пайдаланушы деректерін беру қалай жүзеге асырылатыны туралы ақпарат беруге міндетті. GDPR сәйкестігін тексеру нәтижесінде барлық банктерде проблемалар анықталды.



11-сурет - GDPR мәселесі кездескен банктер тізімі

4 Автоматтандырылған банк жүйесіндегі банктік ақпараттың ақпараттық қауіпсіздігінің тұжырымдамалық негіздерін дамыту

4.1 Автоматтандырылған банктік жүйелердегі банктік ақпараттық қауіпсіздік қатерлерінің синергетикалық моделін құру тұжырымдамасын әзірлеу

Қазіргі жағдайда компьютерлік жүйелер мен телекоммуникациялардың жаппай қол жетімділігі, банктер мен клиенттер арасындағы электронды құжат айналымының ұлғаюы табиғи және БИ байланысты электронды сауданың қауіпсіздігі мәселелеріне көшу тек ауырлататын жасанды факторлар. Нәтижесінде BI қауіпсіздігін бұзудан болатын шығындар банктер мен олардың клиенттері үшін қымбаттайды [1, 2, 46]. Мысалы, ABS Украина қауіпсіздігіне қауіп төндіретіндердің көпшілігі, басқа мемлекеттердегідей, BI ашық байланыс арналарын беру кезінде Интернеттен келеді [3, 2, 32, 42, 44, 45]. Украинаның IT-қауіпсіздігін стратегиялық басқарудағы олқылықтар бірқатар проблемаларда мемлекеттік банк секторына ABS-ті жіберді, олардың бастысы - жүйенің қауіпсіздігінің жоқтығы, ABS-тің қауіпсіздігін қамтамасыз ету үшін үйлестіру механизмдерінің болмауы, әсіресе екі халықаралық және көпжақты форматтарда және т.б. . [4, 41, 42]. Украинаның негізгі халықаралық стандарттары мен стандарттарын талдау жеке тұлғаны тексергенін көрсетті банктік операциялардың ажырамас бөлігі болып саналмайтын қауіпсіздік моделі - тұтастық, құпиялылық және қол жетімділік (DCI моделі) негізінде банк саласында қолданылатын ақпараттық қауіпсіздік технологияларын бағалау әдістемесінің компоненттері - аутентификация қызметі - мемлекеттік банктегі ақпарат қандай ақпарат аутентификация көзін (авторизацияланған пайдаланушы және / немесе процесс) ұсынады. Банк секторының стандарттарындағы тәуекелдерді талдаудың синергетикалық тәсілінің, ақпараттық технологиялардың қауіпсіздігін бағалаудың бірыңғай әдістемелерінің болмауы оның жетілдірілмеген механизмдеріне байланысты тиісті саясатты, ABS қауіпсіздігін қамтамасыз етудің жаңа тәсілдері мен шараларын уақтылы құруға мүмкіндік бермейді. IS, CB, SI, мәселенің ажырамас бөлігі - қауіпсіздікке байланысты BI тәуекелін талдау. Шын мәнінде, тәуекел - бұл қолданыстағы емдеу құралдарының банктік ақпаратқа шабуылға қаншалықты төтеп бере алатындығының ажырамас бағасы. Қазіргі кезде әзірленген тетіктер мен ақпараттық қауіпсіздіктің жиынтығына қарамастан, қазіргі уақытта АБС АТ қауіпсіздігінің тиімділігін тиісті көрсеткіштерге сүйене отырып бағалау басымдықтардың бірі болып табылады. Мысалы, талдауда көрсетілгендей , ең көп таралған көрсеткіштер

қатарында олардың қауіпсіздігі келесі таксономия болып табылады: Вон-Хенниг-Сирадж, NIST STS822, OCIPEP, OCTAVE , CISWG, Эркан Кахраман.

Осы көрсеткіштердің қауіпсіздігі бойынша зерттеулер нәтижесінде олардың банктік секторға тиімді енгізілуі Украинаны тежейді: анықталған белгісіздік - ұлттық заңнаманың жетілмегендігінен және осы саладағы озық халықаралық тәжірибелермен келіспеуінен; алынған рейтингтердің төмен объективтілігі - халықаралық тәжірибенің болмауынан, негізінен банк қызметкерлерінің АБС-да қауіпсіздігін қамтамасыз етеді; әдістемелік проблемалар - проблемалық мәселелерге байланысты сандық және сапалық бағалаулар бір-бірімен үйлеседі [5, 50]. Мәселелердің соңғы бөлігінде жүйенің шешуші сипаты бар, сондықтан терең ғылыми-техникалық өңдеуді және қосымша тергеуді қажет етеді. Талдау көрсеткендей, ақпараттық қауіпсіздік мәселелерін шешуге мауды теориялық және практикалық үлес қосқан [6] негізгі құжаттар: «Қызғылт кітап» деп аталатын компьютерлік жүйелердің қауіпсіздігін бағалау критерийлері [7]; Еуропалық ақпараттық қауіпсіздікті бағалау критерийлері [8]; Канадалық қауіпсіздікті бағалау критерийлері сенімді компьютерлік жүйелер [9]; АҚШ-тың Федералдық критерийлері [10]; ISO / IEC 15408 халықаралық стандарты - «АТ қауіпсіздігін бағалау критерийлері» [11, 12, 13]; CEM-97/017 стандартының жұмыс жобасы - «АТ қауіпсіздігін бағалаудың жалпы әдістемесі» [34] ISO ISO / IEC TR 13335. Ақпараттық технологиялар. 27002: 2010 Ақпараттық технологиялар. Қорғау әдістері. Ақпараттық қауіпсіздікті басқарудың практикалық кодексі (ISO / IEC 27002: 2005, MOD) [23]. ХБ үшін қойылған міндеттерді шешу үшін процестерді модельдеудің және қауіпсіздік жүйелерінің тиімділігін бағалаудың формальды әдістерімен қатар жүйелер мен процестердің ыдырау және құрылымдау әдістерін, бейресми бағалау әдістері мен әдістерін қолдану қажет екендігін растайтын құжаттарды талдау шешім қабылдау тиімділігі. Бұл дегеніміз, құрылғы ақпараттық қауіпсіздік жүйелерінің өмірлік циклінің барлық кезеңдерінде жүйелік талдауды қолдануы керек [46, 50]. ABS-де ақпараттық технологиялардың қауіпсіздігін бағалау әдістемесін жасауда ISO / IEC 15408 «АТ қауіпсіздігін бағалаудың жалпы өлшемдері», «Жалпы критерийлер» стандарттары ерекше орын алады. Стандарт ақпараттық өнімдер мен технологиялардың қауіпсіздік қасиеттерін бағалаудың негізі ретінде пайдаланылатын жалпы критерийлерді көрсетеді [11, 12, 13]. Өнімдер мен АТ жүйелерінің қауіпсіздік сипаттамаларына, сондай-ақ осы функцияларды орындауға қойылатын жалпы талаптар жиынтығын енгізу арқылы әр түрлі сарапшылар алған бағалау нәтижелерінің салыстырмалылығын қамтамасыз етуге арналған жалғыз критерийлер. Талдаулар жүргізетін стандартты қолдану сәйкес өнімділік талаптарын және АТ қауіпсіздігін таңдай отырып, нақты

қолданбалы мәселені шеше алады [6, 46]. Сонымен қатар, бір өлшеммен қауіпсіздіктің ықтимал қатерлері, яғни тұтастық, қол жетімділік, құпиялылық кейіннен қауіпсіздікке жаңа қатерлер моделінің синергетикалық компоненттерін қоюды ұсынады ISO 27001 [19] және ISO 27002 [20] оларды банктік және заңдық талаптардың ерекше қажеттіліктеріне байланысты оларды деректерді қорғау талаптарына қосу [23]. ұлттық заңнама .

Талқыланатын құжаттардың негізгі мәні - олардың банктің ақпараттық қауіпсіздігін басқару принциптеріне жатқызуы, олардың ішіндегі ең маудылары - тәуекелді бағалау .Практика көрсеткендей, қазіргі кезде біз қауіпсіздік тәуекелдерін бағалау әдістерінің екі негізгі тобын нақты ажырата аламыз . Әдістердің бірінші тобы ақпараттық қауіпсіздікке қойылатын талаптардың жиынтығын бағалау арқылы тәуекел деңгейін орнатуға мүмкіндік береді. Банк секторындағы осындай талаптардың қайнар көзі ретінде Украина 1-суретте көрсетілген сызба бойынша тапсырыс бере отырып, халықаралық және ұлттық нұсқаулықтарға қызмет ете алады. Тәуекелді бағалаудың екінші тобы ABS-де шабуыл ықтималдығы мен зақымдану деңгейін анықтауға негізделген. Бұл жағдайда тәуекел мәні әр қауіп үшін есептеледі және тұтастай алғанда осы қауіптен болатын ықтимал шығындар шамасының қауіптілігінің туындысы болып табылады. Шығынның мәні жеке BI-мен өлшенеді, ал қауіптің туындау ықтималдығы аудиторлық процедураны жүргізетін топпен есептеледі. Бірінші және екінші топ әдістерінің айрықша ерекшелігі - тәуекелді анықтау үшін әр түрлі шкалаларды қолдану. Бірінші жағдайда тәуекел және оның барлық параметрлері санмен көрсетілген, і. е. сандық мәндер. Екінші жағдайда сапалы шкаланы қолдану. Украинаның Ұлттық Банкінің стандарттарына сәйкес ABS Ukraine стратегиялық ақпараттық технологияларды басқарудың тұжырымдамасына сәйкес 1-сурет АЖ басқару жүйесінің (ББАЖ) қолданылу аясы, жалпы, банк. ABS BI Ukraine қауіпсіздігімен байланысты барлық күрделі мәселелерді шешу - мысалы, ABS-де IS, CB, SI бір-бірімен үйлесімді түрде толықтырылып, қажет болған жағдайда бір-бірін толықтыратын және бір-бірінен ажыратылмайтын түрде шешілуі керек. ABS-те BI қауіпсіздігін қамтамасыз ету үшін әр жағдайда мүмкіндіктерді оңай интеграциялау практикалық және ғылыми көзқарастарға сәйкес келмейді. Басқа альтернативті тәсілдердің жетіспеушілігі туындаған проблеманы шешудің өзектілігін тудырады - жаңа тәсілдерді әзірлеу арқылы қауіпсіз BI ABS. АБ-дағы IS, CB, SI BI гибридтік қатерлерін ескере отырып, BI-нің типтік қауіптерін синергетикалық модель бойынша BI қауіп-қатерлерін синтездеуге шақырады . Ұсынылып отырған тәсілдің айрықша ерекшелігі гибридтік қауіптер тұрғысынан ABS-те қауіпсіздік компоненттері, IS, CB, SI BI саласындағы синергияға қол жеткізуде жаңа әдіснамалық негіздерді жасау

үшін қажетті және жеткілікті жағдайлар жасау болып табылады. тек Украинаға емес, басқа дамыған елдерге.

ISO 13335 - Халықаралық ақпараттық технологиялар қауіпсіздігі стандарттары
Бұл серияға келесі 4 стандарт кіреді:
ISO13335-1: 2004 Ақпараттық технологиялар. АТ қауіпсіздігін басқару бойынша нұсқаулық. Ақпараттық-коммуникациялық технологиялар қауіпсіздігін басқарудың тұжырымдамалары мен модельдері
ISO13335-3: 1998 Ақпараттық технологиялар. АТ қауіпсіздігін басқару бойынша нұсқаулық. АТ қауіпсіздігін басқару әдістері
ISO13335-4: 2000 Ақпараттық технологиялар. АТ қауіпсіздігін басқару бойынша нұсқаулық. Қауіпсіздік шараларын таңдау
ISO13335-5: 2001 Ақпараттық технологиялар. АТ қауіпсіздігін басқару бойынша нұсқаулық. Желілік қауіпсіздікті басқару бойынша нұсқаулық

ISO 15408 - Ақпараттық технологиялар қауіпсіздігін бағалаудың жалпы өлшемдері Қорғау профилі - тұтынушылардың нақты қажеттіліктерін қанағаттандыратын АТ өнімдерінің белгілі бір санаты үшін қауіпсіздік талаптарының іске асыруға тәуелсіз жиынтығы (ГОСТ Р ISO / IEC 15408). Қорғау профилі - бұл қорғаныс мақсаттарының, функционалдық талаптардың, жеткіліктілік талаптарының және олардың негіздемелерінің жиынтығы болып табылатын арнайы нормативтік құжат.
ISO 15408 халықаралық стандарты туралы жалпы ақпарат

ISO 27000 стандарттары ақпараттық қауіпсіздікті басқару жүйелеріне қатысты келесі құжаттарды қамтиды:
ISO / IEC 27001 Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар - ақпараттық қауіпсіздікті басқару жүйелері. Талаптар.
ISO / IEC 27000 Ақпараттық қауіпсіздікті басқару жүйелері. Шолу және сөздік - Ақпараттық қауіпсіздікті басқару жүйелері. Шолу және терминология.
ISO / IEC 27003 ақпараттық қауіпсіздікті басқару жүйелері. Нұсқаулық - ақпараттық қауіпсіздікті басқару жүйелері. Көшбасшылық.
ISO / IEC 27004 Ақпараттық қауіпсіздікті басқару. Өлшеу - ақпараттық қауіпсіздікті басқару жүйесінің тиімділігін өлшеу.
ISO / IEC 27006 Ақпараттық қауіпсіздікті басқару жүйелерінің аудиті мен сертификаттауын жүзеге асыратын органдарға қойылатын талаптар - Ақпараттық қауіпсіздікті басқару жүйелерінің аудиті мен сертификаттауын жүзеге асыратын органдарға қойылатын талаптар.
ISO / IEC 27007 Ақпараттық қауіпсіздікті басқару жүйесінің аудиті жөніндегі нұсқаулық (FCD) - ББАЖ-ға аудит жүргізу жөніндегі нұсқаулық.

Банктік нормативті ережелері.

Қауіпсіздік саясаты Ережелер Бұйрықтар Рәсім

- ARS стратегиялық ақпараттық қауіпсіздікті басқару тұжырымдамасы.
- Бағдарламалық және аппараттық қосымшалар өндірушілерінің

1. Сызбанұсқа - ABS IT қауіпсіздік талаптарының негізгі систематикасы

Осылайша, ABS қауіпсіздігін бағалау әдістемесі мәселелері бойынша алдыңғы қатарлы халықаралық практиканың талаптарын түзету арқылы негізгі қауіпсіздік тәуекелдері мен BI арасындағы өзара байланыс орнатылған, бүгін және жақын болашақта Украинада ABS өтеді.

ABS-те BI BI үшін концептуалды негізді құру үшін типтік ендірудің стратегиялық жиынтығының үш деңгейлі функционалды моделіне негізделген [4] үштікке негізделген ABS-те қауіп-қатерлер моделін құру тұжырымдамасы ұсынылды. - ABS-де қауіпсіздікті басқарудың деңгейлік стратегиясы

Бірінші деңгей банктің жалпы корпоративті стратегиясын және оның функционалды стратегиясын сипаттайды (2.3 а суретті қарау). Корпоративтік стратегия даму перспективаларын анықтайды және банктің негізгі миссиясына қызмет етеді. Бұл деңгейде синергетикалық тәсілге сәйкес АБС ақпараттық технологиясының жалпы тұжырымдамасы және КБ қамтамасыз етудің алға қойылған мақсаттары мен міндеттері. Бұл деңгей АБС-тағы АЖ BI күйімен анықталады:

$$S^{ABS} = \{S_1^{ABS}, S_2^{ABS}, ..., S_m^{ABS}\},$$

$S_i^{ABS} \in \{S^{ABS}\}$, $(i = 1, m)$ — АВ BI-ді ABS-ке қосу. Функционалды стратегиялар - бұл көлденең коммуникацияның бірі және мақсаттар деңгейінде үйлестірілген, әрі қарайғы деңгей стратегиялық жоспарда егжей-тегжейлі.

Екінші деңгей АБ-дағы IS BI корпоративтік стратегиясы қалыптасқан:

$$\{RR^{ABS}\} = \{R_{BBI}\} \{OV_{BBI}\} \{IU_{BBI}\}, \quad (2.1)$$

$\{RR^{ABS}\}$— Нормативтік талаптардың жиынтығы BI сұранысына қойылатын талаптарды қамтиды — $\{R_{BBI}\}$ халықаралық және ұлттық стандарттарда анықталған, қауіпсіздік талаптарының дәрежесін бағалайды $\{OV_{BBI}$ BI қауіпсіздігінің соңғы деңгейін орнату $\{IU_{BBI}\}$.

Сондай-ақ заңды және жеке клиенттердің жеке деректерін қорғауға қатысты негізгі бизнес-процестердің мақсаттары мен міндеттері анықталды. Корпоративті қауіпсіздік стратегиясы қауіпсіздіктің әртүрлі аспектілерін қалай басқаруға және қалай үйлестіруге болатындығын сипаттайды. Ол функционалдық стратегияларды, экономикалық қаржылық, физикалық және ақпараттық қауіпсіздікті дамытады.

Үшінші деңгей корпоративті ақпараттық қауіпсіздік стратегиясы қалыптасқан екінші деңгейлі стратегиялық жиынтықтың функционалды стратегиялары жасалады.

Қорғаудың негізгі бағыттары персонал қауіпсіздігін, физикалық қауіпсіздікті, желіні және BI-ді қамтамасыз ету. Бұл деңгей BI-дің ABS-індегі

ақпаратты қорғаудың қолданылатын техникалық құралдары мен IS, CB, SI қатерлері арасындағы сәйкестікпен анықталады:

$$OPZ^{ABS} = \sum_{i=1}^{k} OPZ_i, \qquad (2.2)$$

мұндағы OPZi - АБС қауіпсіздік деңгейінің жалпы индикаторы, TMIP реттеушілерінің талаптарына сәйкестік деңгейін бағалау.

АЖ стратегиясы банк менеджментінің мауды функциясы болып табылады және қауіпсіздікті қалыптастыру керек және оны жоғары басшылыққа алу керек.

Бұл тұжырымдама банктің стратегиялық басқарудың барлық деңгейіндегі тәуекел мәніне ABS-те BI BI мақсаттарына жетудің тиімді жолдарын таңдауға синергетикалық көзқарасқа негізделген. Тәсіл қауіпсіздікке қатысты стратегиялық шешімдердің мүмкін болатын баламаларын жан-жақты іріктеуге және үш кезеңді қамтитын АБС АЖ-да жалпыланған индикаторын бағалау әдісін жасауға мүмкіндік береді:

1) АИ, CB, SI ақпараттарының қауіптіліктің әсер ету ықтималдығын анықтау.
2) ABS инфрақұрылымының инфрақұрылымының элементтері, IS, CB, SI және TMIP қатерлері арасындағы жетілдірілген инфрақұрылымдық ABS синергетикалық моделінің қауіптері, шабуылдаушының жетілдірілген моделі негізінде тәуелділікті анықтау.
3) ABS моделіндегі BI BI-нің жалпыланған индикаторының анықтамасы, ABS-тағы BI қауіпсіздігін жақсартылған бағалау негізінде, мысалы, 2.4-суретте көрсетілген Украина OPS.
4) Ақпараттық қауіпсіздік, киберқауіпсіздік және ақпараттық қауіпсіздік құрамдастарын біріктіру арқылы тұжырымдамалық модель негізінде жасалған банктің стратегиялық басқару моделіне негізделген банктік автоматтандырылған жүйелердегі банктік ақпараттық қауіпсіздікті қамтамасыз етуде жаңа бағыт ашылады әр деңгейдегі тәуекел мәні.

4.2 Құрылыс компоненттерінің қағидаларын рәсімдеу салалық банктік ақпараттық қауіпсіздікке, ақпараттық қауіпсіздікке, киберқауіпсіздікке, ақпараттық қауіпсіздікке қауіп төндіреді.

1-қадам. Ұсынылған классификатор негізінде іске асырылатын BI ақпараттық қауіпсіздігі АЖ, СБ, СИ қауіптерінің әсер ету ықтималдығын анықтау.

Жіктеуіштің құрылысында белгілі болғаннан айырмашылығы, төрт платформаның әрқайсысын қамтьиды, тиісінше:

Бірінші платформа - OPS ABS-тегі BI қауіпсіздігінің қауіптерін жіктеу: ақпараттық қауіпсіздік (IS) (01), ақпараттың қауіпсіздігі (SI) (02), киберқауіпсіздік (CS) (03).

Біз келесі анықтамаларды енгіземіз:

Анықтама 1. Қауіпсіздіктегі банктік ақпарат (S BI) - пайдаланушылардың, аппараттық құралдардың және формациялық технологияның ABS-де өңделген кезде BI құпиялылығын, тұтастығын, шынайылығын және қол жетімділігін қамтамасыз ету қабілетімен сипатталатын банктік ақпаратты қорғау жағдайы;

Анықтама 2. Ақпараттық қауіпсіздікті қамтамасыз ететін банктік ақпарат (БИ АЖ) - мемлекеттік қауіпсіздік ақпараты, оның қалыптасуын, қолданылуын және дамуын азаматтар мен ОПС мүдделері үшін қамтамасыз ететін OPS ортасы.

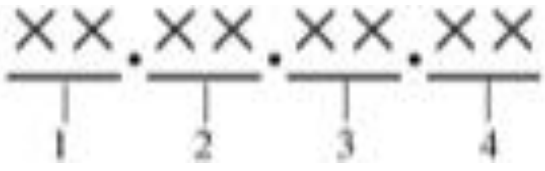
Анықтама 3. Кибер-банктік ақпарат (CB BI) - киберкеңістікті ABS, ресурстар мен OPS пайдаланушыларын қорғау үшін қолданылатын құралдар, саясат, қауіпсіздік принциптері, қауіпсіздік кепілдіктері, тәуекелдерді басқару тәсілдері, әрекеттері, оқыту, сақтандыру және технологиялар жиынтығы.

Екінші платформа - табиғат аймақтарындағы қатерлерді жіктеу: нормативтік (01), ұйымдастырушылық (02), инженерлік (03);

Үшінші платформа - ақпараттың негізгі белгілеріне сәйкес қатерлерді жіктеу: құпиялылық (01), тұтастық (02), қол жетімділік (03), шынайылық (04);

Төртінші платформа - қатерлердің деңгей иерархиясы бойынша классификациясы ABS: PHL - физикалық деңгей (01), NL - желілік деңгей (02), OSL - деңгейлік операциялық жүйелер (OS) (03), DBL - дерекқорды басқарудың деңгейлік жүйелері (04) , BL деңгейіндегі банктік технологиялардың қосымшалары мен қызметтері (05).

Классификатордың бөліктері нүктемен бөлінген. 2-суретте айқын көрсетілген.



Сурет 2 - Жалпыланған Классификатордың компоненттері

1 - BI синергетикалық компонентінің қауіпсіздігі; 2 - табиғат зоналары; 3 - ақпараттың ерекшеліктері; 4 деңгейлі ABS иерархия инфрақұрылымы.

ABS OPS қауіп-қатерлерінің байланыс блок-схемасы келтірілген 2-сурет. ABS кезіндегі IS, CB, SI BI қатерлер жиынтығы электронды қайта дереккөздерді қолдануға итермеледі (http://bdu.fstec.ru/vul).

4.3 Автоматтандырылған банктік жүйелердегі банктік ақпараттық қауіпсіздіктің жалпыланған индексін бағалау мәселесін рәсімдеу

4.3.1 Автоматтандырылған банк жүйесінің инфрақұрылымын жетілдіру

Қауіпсіздікті жетілдіретін кешенді қауіпсіздік жүйесін құрудың мауды міндеттерінің бірі - ақпарат алудың барлық ықтимал қатерлерін ең сапалы және мүмкін болатын ресурстардың ресурстарымен бейтараптандыруды қамтамасыз ететін жалдау құралдарының көптігін таңдау. Ақпараттық қауіпсіздіктің ең тиімді мәселелері жобалау сатысында ықтимал қауіптер мен оларды қорғаудың тетіктерін бағалау кезінде профилактикалық қорғау стратегиясы бойынша шешіледі. Операцияның нәтижелері туралы статистикасы бар әзірлеушімен жүйелерді жобалау барысында жүйе айтарлықтай белгісіздік жағдайында болатын СО құралы туралы шешім қабылдауы керек [1, 48, 56, 59, 61].

Қауіпсіздік модельдері ABS кіретін қауіпсіз компьютерлік жүйелерді жасауда және зерттеуде мауды рөл атқарады. Модельдер жүйелік интеграторлар тәсілін ұсынады, оған мауды проблемаларды шешуге кіреді: АБС архитектурасының негізгі принциптерін таңдау және зерттеу, ақпараттық қауіпсіздік құралдары мен әдістерін жетілдіру механизмдерін анықтау, дамыған жүйелердің байланыстарын (қауіпсіздігін) дәлелдеу қорғалған компьютерлік жүйелермен қамтамасыз етілген ұйымдастырушылық-құжаттық бағдарламалық жасақтаманың мауды компоненті ретінде қауіпсіздік саясатының ресми спецификациясын әзірлейтін қауіпсіздік саясатына (талаптарға, шарттарға, өлшемдерге) сәйкестігінің ресми дәлелі.

Банктердегі ақпараттық қауіпсіздікті жобалау немесе жаңарту кезіндегі модельдерді құру табиғи түрде минималды шығындармен және жоғары тиімділікпен талдау мен жобалауды шешетін сияқты. Осылайша, ақпараттық қауіпсіздікті талдау кезеңінің моделі әр функцияны (операцияны) зерттеу үшін пайдаланылды, мысалы, кез-келген кез-келген жұмысшыға қандай ақпарат және қандай ресурстар қол жетімді болуы керек [1, 48, 56, 59, 61].

Жүйелік тәсілдемеге сәйкес BI-ге тәуелділіктің BI-нің әдіснамалық негіздерін қалыптастырудың басты нәтижесі - бұл BI-нің психологиялық қауіпсіз технологияларын жүзеге асыратын, қорғалған ABS идеалдандырылған немесе анықтамалық моделі (RM). Сонымен қатар, RM BI

қауіпсіздік ережелері мен стандарттарын әзірлеу арқылы архитектуралық тәсілдерді стандарттау және үйлестіру шешімдерін жүзеге асырудың әлеуетін қамтамасыз етеді.

Қауіпсіздік компоненттеріне қарамастан, BI-ге қауіп төндіретін синергетикалық көзқарасқа негізделген қауіпсіздік моделін құру: IS, CB, SI тәуекелдерді басқару принциптерін қолдану орынды, бұл оның негізгі процедураларын дер кезінде анықтауға және жіктеуге мүмкіндік береді. қауіп-қатерлер және олардың ықтимал көріністерінің жағымсыз салдарларының ықтималдығы бойынша АБС-да тиісті қауіпсіздік жүйесін ұйымдастырады.

Қауіпсіздік ақпараты банктік қызметті қоса, кешенде өндірістік жүйенің барлық құрылымдық элементтеріндегі және циклді өңдеудің барлық кезеңдеріндегі қол жетімді құралдардың барлық кешенін ғана қамтамасыз етуге болады. Ақпараттық қауіпсіздіктің жетілмегендігінен, әсіресе индикаторлар мен критерийлер саласындағы жүйенің белгіленген тиімділігін объективті растаудың қиындығы мен мүмкін еместігіне негізделген банктік ақпарат жүйесін құру үшін жүйелік талдау әдістемесін ескермеу [69, 72, 74]. жоғарыда аталған мәселелерді шешуге кедергілер.

IS, CB, SI даму теориялары қазіргі кезде жоғары технологияларға негізделген ақпараттық қоғамның қазіргі даму кезеңіне тән жаңа жағдайлармен байланысты. Біріншіден, бұл тек деректерді қорғау ғана емес, сонымен қатар қауымдастықты, адамдар мен коммуникациялық жүйелерді, ең алдымен, мауды қосымшаларды (КА) киберкеңістіктегі информацияның зиянды әсерінен қорғау, қауіпсіздіктің пайда болу проблемасы ақпараттық қауіпсіздік пен ақпаратты қорғаудың органикалық жиынтығы.

Екіншіден, ақпаратты өңдеудің автоматтандырылған технологиясын жүйелі түрде қолдана бастағаннан бастап, ақпараттың қажетті сапасын қамтамасыз ету міндетінің өзектілігі және проблема күрделене түседі. Осылайша, есептеу технологиясының эволюциясы автоматтандырылған жүйелерді басқарудың туындайтын қасиеттері мен сапа кепілдігі туралы ақпаратсыз мүмкін болатын қауіпсіздік міндеттеріне әкеледі.

Үшіншіден, ақпараттық қауіпсіздікті, ақпаратты қорғаудың мақсаттары мен ақпараттарды сапалы шешу проблемалардың тиімділігін анықтайды. Жоғарыда анықталған тұжырымдамаларды біріктіретін ақпаратты басқарудың жалпыланған тұжырымдамасы бар. Өз кезегінде, объектілерді ақпараттық қамтамасыз ету тұжырымдамасын қалыптастыру, жүргізу және пайдалану үшін қажет жұмыс есебінің ақпаратын басқару.

Төртіншіден, ақпараттық қауіпсіздік теориясының дамуының жаңа кезеңіне елеулі назар ақпараттық қауіпсіздіктің, ақпараттың проблемаларына органикалық байланыста туындаған кез-келген қиындықтардың шешілуін

қамтамасыз ететін ғылыми-әдістемелік негіздер мен құралдарды жетілдіруге аударылуы керек. технология, ақпараттық қоғам. Сонымен, жоғарыда келтірілгендер АЖ теориясы мен практикасының өзекті мәселелерін ашады [2, 36, 37, 39, 45, 48]:

– барлық компоненттерді бағалаудағы синергетикалық тәсілдің өзара байланыстағы дестабилизациялық факторлардың (қауіп туралы ақпараттың) айтарлықтай белгісіздік пен болжамсыздық көріністері процестерін адекватты сипаттай алатын теориялық негіздер құру және ғылыми-метододологиялық негіздер қалыптастыру. қауіпсіздік, IS, CB, SI тұжырымдамасы;

– түзілу қаупін зерттеу және классификациялау негізінде ABS-те BI-ге сәйкестік туралы ғылыми негізделген нормативтік құжаттар әзірлеу және қорғаудың стандарттық талаптарын әзірлеу;

– ақпараттық қауіпсіздік жүйелерін құруға және басқару құрылымдары мен схемаларын қорғауға арналған тәсілдерді стандарттау.

Осы проблемалардың шешілу ауқымы Украинаның ұлттық қауіпсіздік стратегиясын және доктринаны жүзеге асыруда және банктің қалыптасу қауіпсіздігінде мауды. Ақпараттық қауіпсіздіктің оңтайлы кешенін құрудың мауды міндеттерінің бірі - ең жақсы сападағы және мүмкін ресурстардың ең төменгі ресурстарындағы барлық ықтимал қатерлерді бейтараптандыруды қамтамасыз ететін жалдаудың осындай құралдарының көптігін таңдау. Осы мақсатта ABS қауіпсіздік параметрлерін синтездеуге, еңбек шығындарын азайтуға және CO (ішкі жүйелер) жүйесін жобалау кезінде және ABS-де TSZI пайдалану циклі кезінде қорғауды жоспарлау кезінде ережелерге сәйкестік дәрежесін арттыруға мүмкіндік береді.

Қауіпсіздіктің ұсынылған ap-proach модельдеу моделінің басты айырмашылығы, біріншіден, қауіп-қатер моделін құруға синергетикалық әдісті қолдану, бұл өзара байланысты қауіп-қатерді бағалауды алудың тиімді нәтижесін береді. екіншіден, бизнес-процестерді сәтті жүзеге асыруды қамтамасыз ету үшін талаптарға негізделген ABS таңдалған элементтерінде BI қауіпсіздігі бар:

– ақпараттың құпиялылығын қамтамасыз ету;

– ақпаратқа, қызметтерге және желілік-аппараттық ішкі жүйелерге қол жетімділікті қамтамасыз ету;

– ақпараттың тұтастығын қамтамасыз ету; — бизнестің үздіксіздігін қамтамасыз ету.

Іс жүзінде қауіпсіздік ішкі жүйесінің жобасын зерттеу үшін ең кең қолданылатын екі тәсіл қолданылады [1, 45, 57].

Біріншісі, ақпараттық қауіпсіздік саласындағы стандарттардың бірінің IP қорғау талаптарының сәйкестігін тексеруге негізделген. Бұл ISO - 15408

стандартына немесе кез-келген басқа талаптарға сәйкес жасалған қорғау профильдерінің талаптарына сәйкес қорғаныс түрі болуы мүмкін. Қауіпсіздіктегі мақсат критерийі - өнімділік талаптарының берілген жиынтығы. Тиімділік критерийі - функционалдық талаптарды орындаудың минималды жалпы құны: Σсі → мин, мұндағы сі - і-ші құралдың құны. Бұл тәсілдің негізгі кемшілігі - қажетті қорғаныс деңгейі қатаң түрде белгіленбеген жағдайда (мысалы, заң талаптары арқылы) ABS-тің «ең тиімді» қорғаныс деңгейін анықтау қиынға соғады.

Қауіпсіздік жүйесін құрудың екінші тәсілі «ақылға қонымды жеткіліктілік» қағидаты негізінде тәуекелдерді басқарумен және бағалаумен байланысты. Алайда, талдау көрсеткендей, қорғау құны мен нәтижесінде туындайтын әсерлер арасындағы қауіпсіздік тепе-теңдігінің бұзылуынан болатын шығындарды азайтуға бағытталған тепе-теңдік субъективті болып табылады және ABS элементтеріне төнетін қауіп-қатерді бағалауға тәуелді.

Талдау BI синергетикалық тәсілге негізделген қауіпсіздік моделін құру шеңберінде ақпараттық қауіпсіздік анықтамасын, негізгі механизмдер мен процедураларды енгізу:

Анықтама 4. Банктік ақпарат (БА) - банктік қызметтен туындайтын ақпарат, сондай-ақ банктің өзін, оның қаржылық жағдайын, заңнаманың тиімділігі мен сенімділік талаптарын сипаттайтын ақпарат.

Анықтама 5. Құпиялылық - ақпаратты рұқсатсыз пайдаланушылар және / немесе процестер ала алмайтын BI шарты.

Анықтама 6. Құпиялылық жүйесі (жүйенің құпиялығы) - пассивті шабуылдардан трансферт кезінде BI-ді қорғауға арналған меншік жүйесі;

Анықтама 7. Тұтастық (тұтастық) - ақпаратты рұқсатсыз пайдаланушы және / немесе процесс өзгерте алмайтын BI шарты.

Анықтама 8. Жүйенің тұтастығы (жүйенің тұтастығы) - BI және BI сақтауды қорғауға арналған sys-tem қасиеті, тек авторизацияланған пайдаланушыны және / немесе процесті өзгерту мүмкіндігі.

Анықтама 9. Қол жетімділігі (қол жетімділігі) - ақпаратқа қол жеткізуге және авторизацияланған пайдаланушының және / немесе процестің тұрақты пайдаланылуына кедергі болмайтын BI шарты.

Анықтама 10. Жүйенің қол жетімділігі (жүйенің қол жетімділігі) - жүйенің қасиеті, бұл тиісті авторизацияланған пайдаланушы және / немесе үрдіс ресурстарды РВ ережелеріне сәйкес ұзақ күте тұрмай қолдана алады. (аз) уақыт, пайдаланушыға қажет пайдаланушыны орналастыру үшін қажет болғанда және қажет болған уақыт.

Анықтама 11. Түпнұсқалық (түпнұсқалық) - ақпараттың аутентификация көзін (авторизацияланған пайдаланушы және / немесе процесс) қамтамасыз ететін BI шарты.

Анықтама 12. Жүйенің түпнұсқалығы (жүйенің түпнұсқалығы) - сенімді жүйе, бұл авторизацияланған пайдаланушы және / немесе тиісті аутриенттіліктегі процесс дереккөздердің шынайылығын растай алады.

Анықтама 13. Іскерлік үздіксіздік (Іскерлік сабақтастық) - ішкі және сыртқы қолдану жүктемелері мен қызметтерінің үздіксіз жұмысын қамтамасыз ететін меншікті жүйе, жоспарланған үзілістер мен жоспарланбаған үзілістер кезінде үзіліссіз жұмыс істейді және мауды іскери деректердің сақтық көшірмесі мен сақталуын қамтамасыз етеді. күтпеген оқиға немесе апат болған жағдайда оларды ақылға қонымды уақыт аралығында қалпына келтіру мүмкіндігі.

Анықтама 14. АЖ қатерлері - банктің құрамы, жағдайы және қызметі туралы ақпарат (персонал, материалдық және қаржылық құндылықтар, ақпараттық ресурстар банкі).

Анықтама 15. BI-ге қауіп-қатер - рұқсат етілмеген, соның ішінде банктік деректерге кездейсоқ қол жеткізуді тудыратын жағдайлар мен факторлардың жиынтығы, олар BI-ді жою, өзгерту, бұғаттау, көшіру, тарату және басқа емдеудің нәтижелері болуы мүмкін. ABS.

Ақпаратқа оның қол жетімділігін, тұтастығын, түпнұсқалығын және құпиялығын бұза отырып қорқыту.

Анықтама 16. АБС-тегі банктік ақпараттық қауіпсіздіктің синергетикалық индикаторы - банктік информациялық қауіпсіздіктің антагонистік қарсы әрекет жүйесі тұрғысынан кездейсоқ және мақсатты қауіпсіздік қатерлері тұрғысынан ақпараттық қауіпсіздіктің синергетикалық интеграцияланған қолдану мүмкіндіктерінің тиімділігін бағалау.

Қауіп бәсекелестер, қылмыскерлер, хакерлер және инсайдерлер әрекет етеді. Қауіп-қатер көздері келесі мақсаттарды көздеу кезінде: оларды өзгерту кезіндегі банктік ақпаратпен танысу және тікелей материалдық шығындарды қолдану үшін пайдалы мақсаттарды жою.

Құпия ақпаратты заңсыз иемдену оның жабылуына, BI-дің техникалық құралдар арқылы ағып кетуіне және BI-ге рұқсатсыз қол жетімділікке байланысты мүмкін.

Дереккөздер құрамы құпия ақпарат, банктік процестер, құжаттар, BI медиа-технологиялары, банктік операцияларды қамтамасыз ету болып табылады.

Ақпараттық қауіпсіздіктің негізгі бағыттары - ақпараттық қауіпсіздікке интеграцияланған тәсілдің көрсеткіштері ретінде ақпаратты құқықтық, ұйымдастырушылық және техникалық қорғау.

Ақпаратты емдеу құралдары - бұл физикалық, аппараттық, микробағдарламалық жасақтама және криптографиялық әдістер. Қорғау құралы ретінде ұйымдастырушылық және техникалық шаралар, заңсыз әрекеттердің алдын алу, BI-ге рұқсат етілмеген қол жетімділіктің алдын алу, жолын кесу және онымен күресу әдістері мен қадамдары қолданылады.

4.3.2 Ақпараттық қауіпсіздікке, киберқауіпсіздікке және ақпараттық қауіпсіздікке төнетін қатерлерді бағалаудағы синергетикалық көзқарас негізінде құқық бұзушылық моделін жетілдіру

Модельдің негізгі қауіп-қатерлерінің бірі - толық сипаттама арасындағы мағыналық қатынастарды қамтамасыз ететін қылмыскер моделі. қоқан-лоққылар мен мүмкіндіктер, ол қауіп-қатерлердің қайнар көзі болып табылатын заңсыз әрекеттерді болжау, ол шабуылдарды жобалау және жүргізу үшін пайдалана алады, сондай-ақ осы мүмкіндіктерге шектеулер. Зиянкестердің тәсілдерін қолданатын, жалпы классификациялық критерийлері бар, бірақ әрдайым әр түрлі ақпарат көздерімен байланысты емес модельді құру үшін.

Үлгілерді құру кезінде қылмыскер ішкі және сыртқы қылмыскерлерді бөліп, ескереді [47, 58]: - стандартты құралдарға (бағдарламалық жасақтама, аппараттық-бағдарламалық және аппараттық құралдар жиынтығы) қол жеткізетін құқық бұзушылардың болуы; - қылмыскерлердің мақсатына қатысты білімдер; - бұзушыларды даярлау деңгейі; - шабуыл үшін қылмыскерлердің әртүрлі құралдарын қолдану; - заң бұзушылардың мақсаты; - құқық бұзушылардың әртүрлі санатындағы ықтимал келісім. Осы аспектілерден басқа, ABS қылмыскерінде модельдердің құрылысын объектілердің шабуылына, арналардың сипаттамасына, шабуылдарға, шабуылдардың субъектілердің шығарылуын ықтимал қылмыскерлер санымен, сондай-ақ өмірлік цикл мен ABS деңгейлерімен сәйкестендіру үшін қарастыру керек, бұл қылмыскерге әсер етуі мүмкін. АБС-дағы ақпараттық қауіпсіздік мәселелеріне жауап беруге кепілдік берілген [47, 48] мұндай құқық бұзушылардың әсер ету деңгейлерін ескеруі керек: техникалық арналардың деңгейі, рұқсат етілмеген, зиянды әсерлер, ендірілген құрылғылар, ақпараттық қауіпсіздік жүйесі. Рұқсат етілмеген қол жетімділікті қолдана отырып орнатылған құралдар әр түрлі болуы мүмкін: бағдарламалық жасақтама, аппараттық қамтамасыз ету және компьютерлік технологияларға қызмет

көрсету (Sot) немесе ABS. Сондықтан BI-ге, сондай-ақ ABS объектілері мен сызықтарына (LS) рұқсатсыз қол жеткізу деңгейін санатқа бөлу қажет. Ұсынылған модель негізінде қылмыскерлердің біліктілік сипаттамалары бес санатты анықтайды (2.10-сурет): 1-санат. ABS қолданушылары және қосымшалары - OPS қызметкерлері, олардың қызметтік міндеттері шеңберінде құпия ақпаратқа қол жеткізу мүмкіндігі бар. Ақпаратты ұрлау немесе апатты растау үшін мәліметтер базасын басқару жүйелерінің деңгейіне (04) және банктік технологиялардың қосымшалары мен қызметтерінің деңгейіне (05) әсер етуі мүмкін. Бұл үшін ABS компоненттерін өзгертпестен ұстап қалудың техникалық құралдары және стандартты қорғаныс құралдары мен кемшіліктері қолданылады.

ABS пайдаланушылар санаты келесідей топтарға бөлуге кеңес беріледі:

сенім - 1.1 сенімді пайдаланушылар (мысалы, ұйымның жоғарғы басшылығы BS); 1.2.— пайдаланушы (OPS жұмысшыларының көпшілігі); 1.3 - «тәуекелге ұшыраған» пайдаланушы (мысалы, босату туралы өтініш берген немесе бұрын ИС оқиғаларына қатысқан, пробациядағы OPS қызметкерлері). 2-санат. Операциялық персонал - тұлғалар, оның ішінде жұмыс істемейтін BS ұйымы, OPS, ABS ақпараттық қосымшаларын және BS қолданбалы ақпараттық инфрақұрылымын басқаруға және (немесе) басқаруға байланысты міндеттерді орындау кезінде құпия сипаттағы ақпаратқа қол жеткізу мүмкіндігіне ие. Барлық деңгейлерге әсер етуі мүмкін - физикалық деңгей (01), желілік деңгей (02), операциялық жүйелердің деңгейі (ОЖ) (03), мәліметтер базасын басқару жүйелерінің деңгейі (04), банктік технологиялар қосымшалары мен қызметтерінің деңгейі (05) , ақпаратты ұрлау және ABS өшіру үшін. Бұл барлық шабуылдарды қолдануды білдіреді. Үшінші және бесінші категорияларды бұзушыларға қарсы ықтимал сюжет. Бақылауды (тексеруді) қоспағанда, құралдардың желілік конфигурациясына қол жеткізу құқығына ие болмау. 3-санат. Техникалық және көмекші персонал - құпия ақпаратқа қол жеткізу құқығы жоқ, бірақ осындай ақпаратты өңдейтін үй-жайға тікелей физикалық қол жеткізуді жүзеге асыратын, оның ішінде жұмыс істемейтін OPS қызметкерлері. Барлық деңгейлік физикалық деңгейге (01), желілік деңгейге (02), операциялық жүйелердің деңгейіне (ОС) (03), мәліметтер базасын басқару жүйелеріне (04), банктік технологиялар қосымшалары мен қызметтер деңгейіне (05) әсер етуі мүмкін, ақпаратты ұрлауға және АБС-ны өшіруге тапсырыс беру. Бұл барлық шабуылдарды қолдануды білдіреді. Екінші және бесінші санатты бұзушыларға қарсы ықтимал сюжет. 4 санат. BS ұйымының қызметкерлері болып табылмайтын адамдар келісімшарттық қатынастар негізінде құпия ақпаратқа қол жеткізе алады (аудиторлар, серіктестер және мердігерлер сияқты) заң талаптары

(мысалы, мемлекеттік органдар) және (немесе) үкім. ABS өшіру үшін барлық деңгейлерге әсер етуі мүмкін. Бұл барлық шабуылдарды қолдануды білдіреді. Екінші және бесінші санатты бұзушыларға қарсы ықтимал сюжет. Ақпараттық қауіпсіздікке және журналға және АБС негізгі элементтеріне қол жеткізе алмау. 5-санат. Сыртқы құқық бұзушылар, олар OPS бақыланатын аймағынан тыс ықпал ететін адамдар. Ақпаратты ұрлау, сенімділік және ABS-ді өшіру үшін барлық деңгейлерге әсер етуі мүмкін. Бұл үшін белсенді ықпал ету әдістері мен құралдары қолданылады (арнайы құралдар мен технологиялық бағдарламаларды қолдана отырып, мәліметтер арналарына, бетбелгілерге қосылатын қосымша техникалық құралдарды өзгерту және қосу).

Сонымен, ұсынылған тұжырымдаманың екінші бөлімінде банктің стратегиялық басқарудың барлық деңгей моделдеріндегі тәуекел мәніне ABS-те BI BI мақсаттарына жетудің тиімді жолдарын таңдауға негізделген. Нәтижесінде келесі ғылыми және практикалық нәтижелер: 1. АБ-дағы қауіптердің синергетикалық моделін құру тұжырымдамасы, оның негізі банктік ақпараттық технологияларды стратегиялық басқарудың үш деңгейлі қауіпсіздік моделі болып табылады. Тұжырымдама банктің стратегиялық басқарудың барлық деңгейіндегі модельдерінде тәуекел мәніне ABS-те IS BI мақсаттарына жетудің тиімді жолдарын таңдауға синергетикалық тәсілге негізделген ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі банк қызметінің барлық негізгі бағыттарын қамтиды. OPS функцияларының орындалуына тиімді бақылауды қамтамасыз етеді. 2. Қауіпсіздік компоненттері, қызмет түрлері және автоматтандырылған банк жүйелерінің инфрақұрылым иерархиясы деңгейлері бойынша қатерлерді жіктеуге мүмкіндік берген белгілі синергетикалық модельге негізделген қауіптерден автоматтандырылған банктік жүйелердегі банктік ақпараттық қауіпсіздік қатерлерінің жетілдірілген классификациясын жүзеге асыратын бағдарламалық құрал . Практикалық іске асыру онлайн режимінде BI қауіптерін сараптамалық бағалауға, синергия мен будандықты талдауға, бұл қауіптердің банктік ақпараттың ақпараттық қауіпсіздігіне айтарлықтай шығынсыз және адам ресурстарынсыз ресурстарға әсер ету ықтималдығын бағалауға мүмкіндік береді (ресурстарға электрондық қол жетімділік: http: / /skl.hneu.edu.ua). 3. ABS синергетикалық моделіне негізделген ақпараттық қауіпсіздікті ақпараттық қауіпсіздікті бағалаудың практикалық әдісі, құқық бұзушыларды бағалаудың қорғалған моделі BI-нің қауіпсіздік моделі, ABS және ABS модельдеріндегі инфрақұрылым модельдері үшін BI BI жүйесін құруға қаражат құнын оңтайландыру ABS. Практикалық маудылығы - активтер BI, инфрақұрылым элементтері, ABS, ABS TMIP және қауіп-қатерлердің ықтимал белгілері арасындағы қатынастарды уақытында бағалау

мүмкіндігі, бұл АЖ банктің нұсқауларын түзетуге, ТМІР-ке инвестицияларды жоспарлауға уақыт береді. , қауіп-қатердің алдын-алу бойынша алдын-алу шараларын жасау.

4.4 Онлайн төлем ережелері

Интернет-браузер арқылы сатып алу және интернетте төлеу-бұл тәжірибелі тұтынушылардың көпшілігі үшін тез әрі оңай. Дебеттік немесе несиелік карта нөмірін интернетте хабарлау шынымен қауіпсіз бе? Егер сіз ештеңеге қол қоймаған болсау, сатушы қалай болады? Бұл мақалада тауарларды немесе қызметтерді сатып алу кезінде онлайн-төлемдерге қатысты құқықтық және практикалық мәселелер, соның ішінде интернеттегі әртүрлі төлем әдістері және электрондық сауда операцияларын реттейтін заңдар қарастырылған.

FindLaw жеке басын ұрлау және Интернеттегі қауіпсіздік бөлімдерін қарау, онда сіз тиісті мақалалар мен ресурстарды таба аласыз. Интернетте қауіпсіз сатып алуды үйрену? Интернеттегі сатып алуға қатысты қауіпсіздік мәселелері туралы көбірек білу үшін Интернеттегі сатып алу мәселелері.

Төлем туралы ақпаратты енгізбес бұрын бірінші кезекте қосылымудың қауіпсіз екенін анықтау керек. Қауіпсіз қосылыстарды үшінші тарап тексереді, шифрлау деңгейін қосады және әдетте тыңдаудан қорғайды. Мұны бірнеше түрлі белгішелер көрсетуі мүмкін:

* Шолғыштың шарлау өрісіндегі URL (веб-мекен-жай) алдындағы "https" әріптері;

* URL мекенжайындағы құлыптың суреті (веб-мекен-жайға дейін немесе одан кейін) немесе шолғыш терезесінің төменгі бұрышында.

Егер сізде қауіпсіз байланыс болмаса, серверге жіберілген ақпарат шифрланбауы мүмкін (немесе тек ішінара) және оны үшінші тарап оңай ұстап алады.

Несие немесе дебеттік карта арқылы онлайн төлем

Дебеттік карта чек кітапшасы ретінде пайдаланылады және әдетте сіздің банктік шотудағы қолма-қол ақшамен шектеледі. Екінші жағынан, несие картасы - бұл карта ұстаушымен келісім шарттарымен шектелген жаңартылатын несие түрі. Бірақ онлайн сатып алу үшін (және офлайн) дебеттік және несиелік карталарды тұтынушылар бірдей пайдаланады, тек серверде әр түрлі өңделеді. Сонымен қатар, несие карталарын шығаратын ірі компаниялар өңдейтін несие және дебеттік карталар бойынша транзакциялар жиі жаңартылып отыратын аутентификация және қауіпсіздік шараларымен қорғалған.

Несиелік карта бойынша сатып алу несие картасының Эмитентінен (несие ұсынатын банк) алынады, ол сізге шот-фактураны және кез-келген қолданылатын пайыздық төлемдер мен комиссияларды жібереді, дебеттік карта бойынша сатып алу тікелей ағымдағы шоттан алынады. Интернетте төлеген кезде бұл мауды салдарға әкеледі.

Несие беру туралы Заңға сәйкес тек несиелік карта бойынша алаяқтық төлемдер үшін жауап бересіз. Сонымен қатар, Сіздің картаудың жоғалғаны немесе ұрланғаны туралы хабарлағаннан кейін сіз қандай да бір қарыздар үшін жауап бермейсіз. Егер сіздің картау ұрланған болса, сіздің банктік шотудан қолма-қол ақша алынбайды.

Дебеттік карталар несиелік карталар ұсынатын алаяқтық пен ұрлықтан қорғауды қамтамасыз етпейді, ал рұқсатсыз пайдалану сіздің банктік шотудан мәселе шешілгенге дейін (егер мүлде болса) алып тастауға әкеледі. Қысқаша айтқанда, онлайн-транзакциялар үшін дебеттік карталарды пайдалану үлкен тәуекелге ие және ұсынылмайды.Электрондық ақша аударымдары туралы заң дебеттік карталарды пайдалануды реттейді, бірақ несиелік карталар үшін бірдей қорғаныс деңгейін қамтамасыз етпейді.

Онлайн төлемдердің басқа нұсқалары

Несиелік карталар-бұл интернеттегі ең көп таралған төлем әдісі, бірақ жалғыз емес. Кейбір банктер мен үшінші тарап провайдерлері есептік жазбауға рұқсатсыз кіруді шектеу үшін шифрлау және қатаң аутентификация процедураларын қолдана отырып, төлемдерді онлайн режимінде төлеу мүмкіндігін ұсынады.

Сонымен қатар, көптеген онлайн сатып алуды PayPal, eBay бөлімшесі арқылы жасауға болады, ол несие карталарын ұсынатын компанияларға ұқсас төлем опциясын ұсынады. Сонымен қатар, кейбір транзакциялар (негізінен бизнес арасында) электронды ақша аударымын немесе EFT, бір шоттан екінші шотқа онлайн ақша аударымын ұсынады. Басқа опцияларға сандық әмияндар деп аталатындар кіреді; алдын-ала төленген сауда қызметтері; және онлайн сатып алуды бір айлық шотқа біріктіретін үшінші тарап жеткізушілері.

Технология, қауіпсіздік мәселелері және тұтынушылардың мінез-құлқы өте тез өзгеретіндіктен, онлайн-төлем опциялары әдетте дамып, жиі өзгеріп отырады.

Интернеттегі қолтаңбалар

Интернет арқылы сатып алу-сату шартына "қол қоюға" болады. Заңды тұрғыдан алғанда, иә, бірақ бұл несие картасының түбіртегіне қол қою сияқты емес. Әдетте, бүкіл ел бойынша Соттар орындалуға жататын электрондық қолтаңбалар мыналарды қамтуы мүмкін деп келісті:

* Пошта арқылы келісімдер;

* Банк автоматтарында ПИН-кодты енгізу;

* Сандық қалам планшеті арқылы дебеттік немесе несиелік карта туралы түбіртекке қол қою;

* Кез-келген басқа "электрондық дыбыс, символ немесе келісім-шартқа немесе басқа жазбаға бекітілген немесе логикалық байланысқан және жазбаға қол қою ниетімен адам жасаған немесе қабылдаған процесс" (Ғаламдық және Ұлттық саудадағы Электрондық қол қою туралы Заңнан, GPO).

Демек, федералды және / немесе мемлекеттік заңдарға сәйкес келетін электрондық қолтаңба қағаз келісімшартында немесе түбіртекте "дымқыл сиямен" қол қою сияқты заңды салмаққа ие.

Интернеттегі төлем ыңғайлы және тиімді болуы мүмкін, бірақ оның қауіптері мен алдыңғы қатарлы әдістермен осы тәуекелдерді азайту тәсілдерін түсінетіндігуге көз жеткізу. Егер сізде қосымша сұрақтар туындаса, тұтынушылар құқығын қорғау жөніндегі адвокатқа хабарласу.

Смартфондарды қолданумен байланысты қауіптер туралы айта келе, Кингер: "қазіргі жағдайда ұялы арнадағы алаяқтық қаупі басқа арналарға қарағанда әлдеқайда жоғары. Көптеген пайдаланушылар телефондарына олардың деректеріне сөзсіз қол жеткізуге мүмкіндік беретін қосымшаларды орнатады. телефонда орнатылған басқа қолданбалар. Содан кейін бұл "зиянды" қосымшалар мобильді банк қосымшасы сияқты сіздің әрекеттеруді қадағалап, қосымшаның иесіне беру үшін құпия деректерді шығара алады ".

4.5 Интернет-банкингті қауіпсіз пайдалану туралы кеңестер.

1. Әрқашан шынайы антивирустық бағдарламалық жасақтаманы қолдану. Компьютерді фишингтен, зиянды бағдарламалардан және басқа да қауіпсіздік қатерлерінен қорғау үшін әрқашан шынайы антивирустық бағдарламалық жасақтаманы пайдалану. Антивирус құпия ақпаратты ұрлай алатын шпиондық бағдарламаны анықтауға және жоюға көмектеседі.

2. Жалпыға қол жетімді Wi - Fi немесе VPN бағдарламалық жасақтамасын пайдаланудан аулақ болу. Ашық Wi-Fi желісінің ең үлкен қауіпі-хакер соңғы пайдаланушы мен кіру нүктесі арасында болуы мүмкін және барлық деректерді оңай қадағалап отырады. Хакерлер қорғалмаған қосылымды құрылғыға зиянды бағдарламаны енгізу мүмкіндігі ретінде қарастырады. Осылайша, Интернет-банкинг немесе мобильді банкинг үшін жалпыға қол жетімді Wi-Fi кіру нүктелерін пайдаланудан және электрондық коммерция сайттарында төлемдер жасаудан аулақ болу керек. Алайда, егер сіз жалпыға қол жетімді Wi-Fi-ны үнемі қолданатын болсау, компьютерге VPN бағдарламалық жасақтамасын орнатуды қарастыру. Ол компьютер мен интернет арасында Қауіпсіз туннель жасайды және хакерлерге трафикті ұстап тұруға мүмкіндік бермейді.

3. Смартфонның операциялық жүйесінің соңғы жаңартуларын тексеру. Смартфон қолданушылары операциялық жүйенің соңғы қауіпсіздік түзетулерімен және жаңартуларымен жаңартылғанына көз жеткізуі керек. Сондай-ақ, олар көбінесе "түрмені бұзу" немесе "тамырлау"деп аталатын қауіпсіздік басқару элементтерін телефоннан алып тастамауы керек. Олар әрқашан орнату кезінде қолданбалар сұраған қол жетімділікті тек қолданба қажет ететін нәрселермен шектеуге тырысуы керек.

4. Құпия сөзді үнемі өзгерту және оның сенімді екеніне көз жеткізу. Бұл қарапайым болып көрінуі мүмкін, бірақ сіздің есептік жазбаудың қауіпсіздігін қамтамасыз ету және құпиялылықты сақтауға көмектесу өте мауды. Әрине, өз деректеруді ешкімге айтпау. Сіздің банк ешқашан құпия ақпаратты телефон немесе электрондық пошта арқылы сұрамайды. Егер сіз өзудің банктік құпия сөздеруді дәптерге немесе сүт дүкеніне жазған болсау, оның құпия екеніне көз жеткізу. Әрі қарай, сенімді және ұзақ парольдерді таңдағануға көз жеткізу. Интернет-банк арқылы қаржылық операциялардың қосымша қауіпсіздігі үшін кіру және транзакциялар үшін әртүрлі құпия сөздерді жасау және қолдану.

5. Мобильді хабарландыруларға жазылу. Егер сіз оны әлі жасамаған болсау, қазір жасау. Бұл хабарламалар сізге кез-келген күдікті транзакция туралы тез ескертеді. Транзакция көрсетілген лимиттен асып кетсе немесе оның шегінде болса да, сіз шоттағы қалдық туралы ескерту аласыз. Тек транзакциялар ғана емес, банк сіздің желілік банктік шотуға кірудің сәтсіз әрекеттері туралы ескертеді.

6. Электрондық пошта бағдарламалары арқылы желілік банктік шотқа кіруден аулақ болу. Жарнамалық хат немесе басқа үшінші тарап веб-сайты арқылы қайта бағыттаудан гөрі Банктің URL мекенжайын өзу енгізу әрқашан қауіпсіз. Жоғарыда айтылғандай, банк ешқашан сіздің есептік жазбауға кіру үшін тіркелгі деректерін енгізуді сұрамайды. Сондықтан, егер сізді Банктің веб-сайтына қайта бағыттауды ұсынатын жалған электрондық пошта болса және оны басқаннан кейін жеке деректеруді сайтқа енгізсеңіз, тіркелгі деректерін ұрлау қаупі бар. Сондықтан, егер Сіз банктен кіру мәліметтерін сұрайтын электрондық хат алсау, оған күдікпен қарау.

7. Интернет-банкингке кіру үшін жалпыға қол жетімді компьютерлерді пайдаланбау. Егер сіз жалпыға қол жетімді компьютерді қолдансау, тіркелгі деректерін бұзу қаупі жоғары болады. Алайда, егер сіз осындай жерлерден кіруу керек болса, кэш пен шолу журналын тазалап, компьютерден барлық уақытша файлдарды жойғануға көз жеткізу. Сондай-ақ, ешқашан шолғыштың идентификаторы мен паролін есте сақтауына жол бермеңіз.

8. Өз шотуды үнемі тексеріп отыру. Көптеген банктердің веб-сайттарында "соңғы кіру" немесе "кіру тарихы"қойындысы бар. Сонымен, егер сіз бұзушылықтарды байқасау, парольді өзгертіп, дереу банкке хабарласу.

Мобильді банкинг пен банкоматтарды пайдалану кезінде не нәрсеге назар аудару керек

1. "Мобильді банкинг үшін тұтынушылар тек Apple, Google және Windows Қосымшаларының ресми дүкендерінен жүктелген және банк ұсынған ресми қосымшаны пайдалануы керек. Олар барлық банктерге шоғырландырылған шот-фактураларды қарауды талап ететін агрегатор

қосымшаларына ерекше назар аударуы керек. "олардың құрамында вирустар / зиянды бағдарламалар болуы мүмкін", - деп кеңес береді Кинг.

2. Жұмыс әдістерін және карталарды алып тастамау тәсілдерін түсіндіре отырып, Кинг: "егер карта алынып тасталса, алаяқтар банкомат жабдығымен үйлесетін және несие / дебеттік картаны сақтайтын банкоматтарда карта оқу құрылғысының жоғарғы жағына құрылғы орнатады. Содан кейін бұл ақпаратты алаяқтық басқа бос картаның магниттік жолағына көшіру арқылы алады және нақты шот иесінің атынан сатып алу немесе қолма-қол ақшаны алу үшін қолданылады.

ҚОРЫТЫНДЫ

Біздің жеке мәліметтеріміздің көпшілігі интернетте сақталады, сондықтан киберқауіпсіздік өте маңызды. Әсіресе, қаржылық қызметтерге қатысты ақпаратты қорғау мәселесі маңызды. Банктердің ақпараттық қауіпсіздігі өзектілігі ішкі және сыртқы қауіптерді іске асырудан банк жүйелерінің тәуекел деңгейін төмендету және сайып келгенде, зиянкестердің деструктивті әрекеттерінен болатын зиянды азайту қажеттілігімен байланысты. Мұндай жағдайда базалық рәсім тәуекел-талдау болып табылады, ол банк жүйелерін жан-жақты зерттеуге, АҚ жай-күйінің ағымдағы деңгейін бағалауға, банкті қорғау жүйесіндегі осал жерлерді анықтауға, ықтимал қауіптердің модельдерін жасауға, шабуылдарды іске асыру кезінде қорғау құралдарын таңдау мен күйге келтірудің дұрыстығын тексеруге мүмкіндік береді. Дипломдық жұмыста қарастырылған мәселелер нақты кибершабуылдардан қорғанудың жолдары мен әдістері көрсетілді. Нақты іс-әрекеттерге байланысты қауіпті факторлардың барлығы талданып көрсетілді.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. - Москва: **Наука**, **2015**. - 552 с.
2. https://www.alacriti.com/the-rules-and-regulations-of-online-payments/
3. https://neilpatel.com/blog/easy-payment-process/
4. Бабаш, А. В. Информационная безопасность (+ CD-ROM) / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2013. - 136 с.
5. https://economictimes.indiatimes.com/wealth/spend/8-tips-to-use-internet-banking-safely/articleshow/55113849.cms?from=mdr
6. https://www.nbrb.by/legislation/documents/koncepciya-kiberbezopasnosti.pdf
7. Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Основы информационно-психологической безопасности: моногр. . - М.: Международный гуманитарный фонд "Знание", **2014**. - 416 с.
8. Безопасность ребенка. Информационный стенд. - М.: Сфера, Ранок, 2013. - **787** с.
9. http://nbj.ru/publs/upgrade-modernizatsija-i-razvitie/2018/03/03/kiberbezopasnost-prioritet-dlja-bankov-v-tekuschem-godu/index.html
10. Васильков, А. В. Безопасность и управление доступом в информационных системах / А.В. Васильков, И.А. Васильков. - М.: Форум, **2015**. - 368 с.
11. Гафнер, В. В. Информационная безопасность / В.В. Гафнер. - М.: Феникс, **2014**. - 336 с.
12. Гришина, Н. В. Информационная безопасность предприятия. Учебное пособие / Н.В. Гришина. - М.: Форум, 2015. - 240 с.
13. Девянин, П.Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах / П.Н. Девянин. - М.: Радио и связь, **2013**. - 176 с
14. Ефимова, Л. Л. Информационная безопасность детей. Российский и зарубежный опыт / Л.Л. Ефимова, А С. А, Кочерга. - М.: Юнити-Дана, 2013. - 240 с.
15. Информационная безопасность открытых систем. В 2 томах. Том 1. Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников и др. - Москва: **Машиностроение**, **2016**. - 536 с.
16. Информационная безопасность открытых систем. В 2 томах. Том 2. Средства защиты в сетях / С.В. Запечников и др. - Москва: **СПб. [и др.] : Питер**, **2014**. - 560 с.

17. Мельников, В. П. Информационная безопасность / В.П. Мельников, С.А. Клейменов, А.М. Петраков. - М.: Academia, **2017**. - 336 с.

18. Мельников, В. П. Информационная безопасность / В.П. Мельников, С.А. Клейменов, А.М. Петраков. - М.: Академия, 2013. - 336 с.

19. Партыка, Т. Л. Информационная безопасность / Т.Л. Партыка, И.И. Попов. - М.: Форум, Инфра-М, **2016**. - 368 с.

20. Партыка, Т.Л. Информационная безопасность / Т.Л. Партыка, И.И. Попов. - М.: ИНФРА-М, **2015**. - 368 с.

21. Петров, Сергей Викторович; Кисляков Павел Александрович Информационная Безопасность / Александрович Петров Сергей Викторович; Кисляков Павел. - Москва: **СПб. [и др.] : Питер**, **2013**. - 329 с.

22. Рассел, Джесси Honeypot (информационная безопасность) / Джесси Рассел. - М.: VSD, 2013. - **686** с.

23. Сальная, Л. К. Английский язык для специалистов в области информационной безопасности / Л.К. Сальная, А.К. Шилов, Ю.А. Королева. - М.: Гелиос АРВ, **2016**. - 208 с.

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Сәтбаев университеті

Ғылыми жетекшінің пікірі

Дипломдық жұмыс

Ким Таңшолпан Берікқызы

5В100200 – Ақпараттық жүйелер қауіпсіздігі

Тақырыбы: Банк құрылымдарының клиенттерін оқытудың ақпараттық жүйесін және әлеуметтік инженерия әдістеріне қарсы әрекет ету әдістемесін әзірлеу

Бұл дипломдық жұмыстың ерекшелігі ө оның логикалық құрылымы. Түсіндірме жоба кіріспеден, 4 бөлімнен, қорытындыдан, әдебиеттер тізімінен және қосымшадан тұрады.

Менің ойымша, диплом жобалаушы алдына қойылған міндеттерді толығымен орындады.

Жалпы дипломдық жоба профессионалдық деңгейде орындалған. Түсіндірме жазба тиісті түрде орналастырылған және жоба туралы барлық қажетті ақпаратты қамтиды.

Қорытындылай келе, «Банк құрылымдарының клиенттерін оқытудың ақпараттық жүйесін және әлеуметтік инженерия әдістеріне қарсы әрекет ету әдістемесін әзірлеу» тақырыбындағы дипломдық жоба Ким Таңшолпан Берікқызымен жақсы деңгейде орындалған және жұмыс қорғауға жіберіле алады.

Ғылыми жетекші
Лектор, т.ғ.м. Зиро А.А. « 25» мая 2021 ж.

Протокол анализа Отчета подобия Научным руководителем

Заявляю, что я ознакомился(-ась) с Полным отчетом подобия, который был сгенерирован Системой выявления и предотвращения плагиата в отношении работы:

Автор: Ким Таңшолпан Берікқызы.
Название: Банк құрылымдарының клиенттерін оқытудың ақпараттық жүйесін және әлеуметтік инженерия әдістеріне қарсы әрекет ету әдістемесін әзірлеу
Координатор: Зиро Аасо
Коэффициент подобия 1: 0,07
Коэффициент подобия 2: 0
Замена букв: 1
Интервалы: 0
Микропробелы: 20
Белые знаки: 0

После анализа Отчета подобия констатирую следующее:

☐ обнаруженные в работе заимствования являются добросовестными и не обладают признаками плагиата. В связи с чем, признаю работу самостоятельной и допускаю ее к защите;

☐ обнаруженные в работе заимствования не обладают признаками плагиата, но их чрезмерное количество вызывает сомнения в отношении ценности работы по существу и отсутствием самостоятельности ее автора. В связи с чем, работа должна быть вновь отредактирована с целью ограничения заимствований;

☐ обнаруженные в работе заимствования являются недобросовестными и обладают признаками плагиата, или в ней содержатся преднамеренные искажения текста, указывающие на попытки сокрытия недобросовестных заимствований. В связи с чем, не допускаю работу к защите.

Обоснование:

После анализа отчета по плагиату и работы дипломника выявлено, что заимствования являются добросовестными и не обладают признаками плагиата, так в основном связаны с применением общеизвестных терминов.

Дата 26.05.2021  Подпись Научного руководителя

Протокол анализа Отчета подобия заведующего кафедрой

Заяведующий кафедрой заявляет, что я ознакомился(-ась) с Полным отчетом подобия, который был сгенерирован Системой выявления и предотвращения плагиата в отношении работы:

Автор: Ким Таңшолпан Берікқызы.
Название: Банк құрылымдарының клиенттерін оқытудың ақпараттық жүйесін және әлеуметтік инженерия әдістеріне қарсы әрекет ету әдістемесін әзірлеу
Координатор: Зиро Аасо
Коэффициент подобия 1: 0,07
Коэффициент подобия 2: 0
Замена букв: 1
Интервалы: 0
Микропробелы: 20
Белые знаки: 0

После анализа Отчета подобия констатирую следующее:

☐ обнаруженные в работе заимствования являются добросовестными и не обладают признаками плагиата. В связи с чем, признаю работу самостоятельной и допускаю ее к защите;

☐ обнаруженные в работе заимствования не обладают признаками плагиата, но их чрезмерное количество вызывает сомнения в отношении ценности работы по существу и отсутствием самостоятельности ее автора. В связи с чем, работа должна быть вновь отредактирована с целью ограничения заимствований;

☐ обнаруженные в работе заимствования являются недобросовестными и обладают признаками плагиата, или в ней содержатся преднамеренные искажения текста, указывающие на попытки сокрытия недобросовестных заимствований. В связи с чем, не допускаю работу к защите.

Обоснование: После анализа отчета по плагиату и работы дипломника выявлено, что заимствования являются добросовестными и не обладают признаками плагиата, так в основном связаны с применением общеизвестных терминов.

Дата 27.05.2021  Сейлова Н. А., подпись зав. кафедрой