МІНІСТЭРСТВА АДУКАЦЫІ РЭСПУБЛІКІ БЕЛАРУСЬ
Беларускі нацыянальны тэхнічны універсітэт

Факультэт тэхналогій кіравання і гуманітарызацыі
Кафедра «Філасофскія вучэнні»

А. І. Лойка

Філасофія і метадалогія кібербяспекі

Падручнік па агульнаадукацыйнай дысцыпліне

«Філасофія і метадалогія навукі» для студэнтаў усіх форм навучання

Электронны навучальны матэрыял

Мінск

БНТУ

2024

Аўтар:

А. І. Лойка, загадчык кафедры «Філасофскія вучэнні» Беларускага нацыянальнага тэхнічнага ўніверсітэта, доктар філасофскіх навук, прафесар.

Рэцэнзенты:

Кандрычына І.М. загадчык кафедры «Менеджмент» Беларускага нацыянальнага тэхнічнага унверстэта, кандыдат сацыялагічных навук, дацэнт.

Некрашэвіч Ф.А. дацэнт кафедры філасофіі і ідэялагічнай працы Установы адукацыі «Акадэмія Міністэрства ўнутраных спраўў Рэспублікі Беларусь», кандыдат гістарычных навук, дацэнт.

Падручнік дапаўняе лекцыйны матэрыял пытаннямі філасофіі і метадалогіі кібербяспекі. Разгледжаны адметнасці кібербяспекі ў сацыяльных сетках, лічбавай эканоміцы, інжынернай дзейнасці. Апісана тэматыка кібербяспекі праграмнага забеспячэння. Матэрыял запатрабаны для спецыялістаў менеджменту, маркетынгу, лагістыкі і інжынерна-эканамічных спецыяльнасцей.

УВОДЗІНЫ

Паняцце бяспекі шырока выкарыстоўваецца ў розных сферах прафесійнай дзейнасці, а таксама на ўзроўні фарміравання стратэгій развіцця дзяржавы, ацэнкі міжнароднай сітуацыі і асабістай бяспекі.

Паколькі гаворка ідзе пра сістэмны феномен, мы вылучаем такія канцэптуальныя ўзроўні яго разумення, як прыватныя тэорыі бяспекі, агульная тэорыя бяспекі і філасофія бяспекі.

На ўзроўні практычнай дзейнасці дзяржавы асаблівай тэмай з'яўляюцца пытанні забеспячэння дэмаграфічнай, інфармацыйнай, харчовай, энергетычнай, прамысловай, ваенна-палітычнай, інтэлектуальнай бяспекі і правапарадку. На ўзроўні карпаратыўных структур важную ролю адыгрываюць пытанні інфармацыйна-тэхналагічнай бяспекі. На асабістым узроўні важную ролю адыгрываюць паняцці прававой бяспекі.

Аб'ектыўныя кампаненты прыродных і тэхналагічных небяспек актуалізавалі ўяўленне аб рызыках і пагрозах. Гэтыя ідэі аформлены матэматычным апаратам тэорыі імавернасцей, тэорыі катастроф і тэорыі рызыкі.

Разам са стыхійнымі бедствамі сучасны перыяд развіцця чалавецтва характарызуецца цэлым комплексам катаклізмаў, пагроз і небяспек, якія носяць сацыяльны характар і маюць якасна іншую прыроду. Гэтыя пагрозы і небяспекі ўласцівы як глабальнаму, так і рэгіянальнаму і лакальнаму ўзроўням. Гэта праблема новай галечы, пагроза дэмаграфічнага выбуху, экалагічная небяспека, агрэсіўны этнічны нацыяналізм і сепаратызм.

Філасофія бяспекі

Філасофія бяспекі канцэнтруе ўвагу на асаблівасцях функцыянавання:

1. прыродных сістэм у рамках канцэпцый іх лінейнага і нелінейнага развіцця;
2. тэхніка-тэхналагічных комплексаў (філасофія тэхнікі);
3. індывідуальнай і грамадскай свядомасці людзей (філасофія свядомасці);
4. сацыяльных інфармацыйных сістэм (філасофія інфармацыі);
5. карпаратыўных структур (філасофія кіравання).

Вектар філасофскага пазнання перамяшчаецца да феноменаў, звязаных з прадухіленнем пагроз штодзённасці і забеспячэннем асабістай і сацыяльнай бяспекі. Патрэба ў бяспецы – адна з антрапалагічных канстант чалавечага існавання. Яна суправаджае чалавека на працягу ўсёй гісторыі. Забеспячэнне бяспекі – гэта сацыяльны вопыт, які з'яўляецца важным для чалавека. Уменне прадухіляць пагрозы і фармуляваць стратэгію бяспекі служыць паказчыкам сацыякультурнага развіцця грамадства.

Ўяўленні аб бяспецы адлюстроўваюць складаныя працэсы ў структуры архетыпаў. Узровень бяспекі – своеасаблівы паказчык стану грамадства. Ўяўленні аб тым, што небяспечна, а што бяспечна, адлюстроўваюць самасвядомасць грамадства і дамінуючыя ў ім каштоўнасныя арыентацыі.

Зместавая характарыстыка бяспекі – актыўнасць. Бяспека – гэта пэўны набор умоў працы. Таму кажуць пра бяспечныя ўмовы працы, пра знаходжанне каго-небудзь ці чагосьці ў бяспечных умовах. Неабходна адрозніваць аб'ектыўна бяспечныя, спрыяльныя ўмовы ад ўяўлення суб'екта аб сукупнасці падкантрольных яму умоў, якія ў рэчаіснасці такімі не з'яўляюцца. Апісанне бяспекі як стану абароненасці каго-небудзь ці чаго-небудзь ад сукупнасці пагроз з'яўляецца выражэннем суб'ектыўных, побытавых уяўленняў аб бяспецы.

Забеспячэнне бяспекі – гэта працэс стварэння спрыяльных умоў для дзейнасці, працэс авалодання суб'ектам неабходнымі ўмовамі для ўласнага існавання. Забеспячэнне бяспекі суб'екта – гэта стварэнне ўмоў, пры якіх рэалізоўваліся б яго інтарэсы, рэалізоўваліся б пастаўленыя ім мэты, зыходзячы з яго каштоўнасных арыентацый. Гэта азначае, што бяспека – гэта ўмовы, у якіх суб'екты захоўваюць і ўзнаўляюць свае каштоўнасці.

Забеспячэнне бяспекі як працэс асваення ўмоў існавання адначасова з’яўляецца і працэсам рэалізацыі свабоды суб’екта як здольнасці кіраваць умовамі ўласнага існавання. Свабода і бяспека – цесна ўзаемазвязаныя феномены, якія ўтвараюць фундаментальныя аспекты сацыяльнага быцця, найважнейшыя характарыстыкі сацыяльных суб'ектаў.

Анталогія бяспекі і філасофія прыроды

Любы чалавек, думаючы пра бяспеку, непазбежна ўводзіць у поле зроку свайго мыслення паняцці небяспекі, рызыкі і пагрозы. Ён таксама сустракаецца з паняццем «крыніца небяспекі, рызыкі і пагрозы». Анталогія і філасофія прыроды вывучаюць аб'ектыўныя крыніцы небяспекі, рызыкі і пагрозы чалавецтву і асобе. У гэтым кантэксце даследаванняў было заяўлена, што аб'ектыўнай крыніцай небяспекі, рызык і пагроз з'яўляецца дынаміка прыродных сістэм. Большасць крыніц небяспекі і рызыкі для чалавецтва знаходзіцца ў сістэмах нежывой прыроды.

Менш у сістэмах біялагічнай прыроды, паколькі адной з умоў іх існавання і эвалюцыі ў лакальных прасторах планет з'яўляецца наяўнасць рэсурсу адаптацыі да гэтых прасторах. Самаарганізацыя адыгрывае ключавую ролю ў стварэнні экасістэм і іх дынамічнай раўнавагі. Гэта відаць на прыкладзе біясферы Зямлі.

Антычныя філосафы разумелі, што нават невялікія змены, якія парушаюць гармонію, могуць істотна змяніць свет і пагрузіць яго ў хаос. На працягу многіх стагоддзяў іх увагу займалі менавіта законы гэтай гармоніі, бо ў ёй яны бачылі праяву боскай волі, якая трымае свет у парадку.

Пачынаючы з піфагарэйцаў, якія адкрылі, што гэтыя законы можна запісаць на мове лікаў і геаметрычных фігур, матэматыка пачала выкарыстоўвацца як сродак адлюстравання ідэальных законаў прыроды, у якіх усе супрацьлегласці суразмерныя і ўраўнаважаныя. Магчыма, гэтым тлумачыцца ўпартае нежаданне «класічных» матэматыкаў разглядаць нестабільныя матэматычныя мадэлі, у якіх магчымы рэзкі дысбаланс.

Любая сістэма па меры свайго развіцця праходзіць этапы перабудовы, рэзкіх змен, падчас якіх адбываецца перагрупоўка сіл і рэарганізацыя раўнавагі. Гэтыя этапы характарызуюцца часовым перавагай адной з сіл, што прыводзіць да хаосу, які разбурае папярэднія структуры. Затым адбываецца гарманізацыя, аднаўляецца раўнавагу, але ўжо ў новым, якасна іншым стане.

Адной з матэматычных тэорый, што апісвае рэзкія пераходы, з'яўляецца тэорыя катастроф. Як навуковая дысцыпліна яна з'явілася ў 70-х гадах XX ст. Вартасцю гэтай тэорыі з'яўляецца тое, што яна не патрабуе падрабязных матэматычных мадэляў і можа апісваць сітуацыі не колькасна, а якасна, а яе вынікі і высновы ілюструюцца геаметрычнымі выявамі.

Тэорыя катастроф на якасным узроўні тлумачыць мноства з'яваў. Яна, нараўне з іншымі сучаснымі тэорыямі дынамічных сістэм, змяніла звыклыя ўяўленні аб устойлівасці і інэрцыйнасці фізічнага свету.

Паколькі ў пэўных сітуацыях – у кропках катастроф – нават нязначныя рухі могуць паўплываць на ход развіцця, вельмі карысным апынецца ўменне вызначаць, наколькі далёка ад такой кропкі знаходзіцца сістэма. Фармальна для гэтага трэба вывучыць залежнасць сістэмы ад знешніх параметраў у матэматычных мадэлях. Аднак на практыцы нярэдка сустракаюцца выпадкі, калі ў даследніка няма нават імглістых меркаванняў аб тым, якім эвалюцыйным раўнаннем апісваецца развіццё сістэмы.

Нават у гэтых сітуацыях, паталагічных з пункта гледжання матэматычнага мадэлявання, можна паказаць некаторыя ўскосныя прыкметы таго, што якая вывучаецца сістэма знаходзіцца зблізку кропкі катастрофы. Гаворка ідзе аб так званых "сцягах катастроф" – асаблівасцях паводзін сістэмы, па якіх

можна меркаваць аб набліжэнні крытычнага пункту. Гэта наяўнасць некалькіх розных устойлівых станаў; існаванне няўстойлівых станаў, з якіх сістэма выводзіцца слабымі "штуршкамі"; магчымасць хуткай змены сістэмы пры малых зменах вонкавых умоў; незваротнасць сістэмы (немагчымасць вярнуцца да ранейшых умоў); гістарэзіс.

Тэорыя катастроф з'яўляецца адной з частак больш агульнай матэматычнай тэорыі – якаснай тэорыі складаных нелінейных сістэм. Гэтая тэорыя вывучае агульныя прынцыпы, якія выяўляюцца ў розных сітуацыях, і дапамагае лепш зразумець механізм дзеяння прыродных сіл. Уяўляюць цікавасць адрозненні паміж лінейнымі і нелінейнымі сістэмамі. Лінейны погляд у фізіцы ў агульным выпадку выказвае прынцып суперпазіцыі – сіла ўздзеяння на элемент будзе роўная суме ўздзеяння сіл. З пункту гледжання матэматыкі лінейнай будзе ўзаемасувязь, калі колькасці змен адной незалежнай велічыні адпавядае такая ж колькасць змен у іншай, залежнай ад яе.

Сістэма, якая падпарадкоўваецца лінейным законам – гэта сістэма, роўная суме яе частак. Ведаючы такія заканамернасці элементаў і сістэмы нескладана прадказваць паводзіны і канструяваць аб'екты. Лінейны погляд на свет лёгкі для разумення, лагічны і адпавядае разумнаму сэнсу. З механістычных сістэм яго імкнуліся перанесці на ўвесь навакольны свет.

Але лінейныя працэсы аказваюцца хутчэй за выключэннем, бо прыродныя з'явы значна складаней. Нелінейныя залежнасці ў розных прыродных з'явах і навуках апісваюцца падобнымі мадэлямі, прадказваючы аднолькавыя канчатковыя вынікі. Лінейнае апісанне аказваецца толькі прыватным выпадкам нелінейных працэсаў.

Нелінейнасць апісвае фундаментальныя і ўніверсальныя сувязі і адносіны паміж аб'ектамі. Яе можна назваць супрацьлегласцю лінейнасці. Нелінейнасць перакрэслівае прынцып суперпазіцыі і нічога не прапануе ўзамен. У нелінейных сістэмах з'яўляецца якасна іншыя ўласцівасці, якія не прысутнічаюць у складальных сістэму частках. Варта адрозніваць выпадковы працэс і дэтэрмінаваны хаос.

Самаарганізацыяй называюць узнікненне парадку з хаосу. Гэты працэс, які часта згадваецца ва ўпраўленні арганізацыяй, таксама назіраецца ў нежывых, жывых і сацыяльных сістэмах.

Падтрыманне парадку патрабуе энергіі, якая паступае ў адчыненую сістэму звонку. Пасля гэтага энергія рассейваецца.

Ва ўмовах бязладзіцы адбываецца змена парадку выпадковым чынам. Некаторыя змены хутка павялічваюцца і адымаюць энергію ў астатняй сістэмы за рахунак нелінейнага ўзаемадзеяння. Якія растуць змены падпарадкоўваюць сабе энергетычна слабыя. Фармуецца спарадкаваная кагерэнтная структура сістэмы. Паміж сілай уздзеяння і рэакцыяй дысіпатыўнай сістэмы існуе нелінейная сувязь. Нягледзячы на вялікія намаганні, вынік можа аказацца нікчэмным. З іншага боку, слабы сігнал у вызначаных умовах здольны паскарацца, і паўстане які разгойдваецца працэс.

Такія з'явы магчымыя дзякуючы станоўчай якая ўзмацняе і адмоўнай супрацьдзеіць зваротным сувязям. Структура сістэмы ўяўляе сабою мноства зваротных сувязяў і адносін паміж імі. Таму навязванне нелінейнай сістэме нейкага плана развіцця можа прывесці да непрадказальных вынікаў.

Як толькі сістэма апісваецца самым простым нелінейным матэматычным раўнаннем, у яе адразу з'яўляюцца альтэрнатыўныя шляхі эвалюцыі.

Нелінейная сістэма пэўны час якасна не змяняецца. Але пры дасягненні парогавага значэння надыходзіць крызісная сітуацыя, калі для складаных адкрытых сістэм характэрна няўстойлівыя паводзіны. У такія крытычныя моманты нават маленькія змены здольныя змяніць траекторыю развіцця.

Пад біфуркацыяй разумеюць выбар якасна іншага шляху развіцця, які з'яўляецца выпадковым. Дзве аднолькавыя складаныя сістэмы з цягам часу будуць адрознівацца. Таму што сістэмы аказваюцца ў розных умовах, няхай нават нязначна адрозных.

Пры гэтым сістэма мае толькі абмежаваную колькасць альтэрнатыўных шляхоў развіцця. Спектр магчымых эвалюцыйных шляхоў вызначаецца ўласцівасцямі сістэмы.

Фундаментальныя ўласцівасці касмічных прыродных сістэм: катастрафізм

У разуменні прыродных сістэм абгрунтаваны два канцэптуальныя падыходы. Адзін з іх пазначаецца як катастрафізм. Ён указвае на тое, што любая прыродная сістэма змяшчае небяспеку і рызыкі для чалавецтва. Падобную небяспеку і рызыкі дэманструе тэматыка Сусвету, звязаная з абмеркаваннем яе фармавання і наступнай дынамікі. Зыходным пунктам гісторыі Сусвету лічыцца Вялікі Выбух.

Тэорыя Вялікага Выбуху – гэта касмалагічная мадэль, якая апісвае раннія стадыі развіцця Сусвету. У пачатку XX стагоддзі астраномы выявілі, што галактыкі разлятаюцца ў розныя бакі. З гэтага вынікае, што Сусвет пашыраецца. Момант, з якога пачалося пашырэнне Сусвету, называюць "Вялікім выбухам". Адбылося гэта 13/08 мільярдаў гадоў таму.

Тэорыя Вялікага Выбуху апісвае раннія стадыі пашырэння Сусвету. Падзеі, якія адбываліся непасрэдна пасля Вялікага Выбуху. Працэсы пасля Вялікага Выбуху былі абумоўлены тым, што Сусвет паступова астываў і рабіўся менш шчыльным.

Як мы ведаем, тэмпература – гэта мера руху часціц. Чым павольней рухаюцца часціцы, тым прасцей ім сябар з сябрам злучацца. Па меры астывання Сусвету, спачатку асобна якія лётаюць кваркі змаглі аб'яднацца ў пратоны, нейтроны і іншыя адроны і лептоны. Затым ужо атрыманыя часціцы, працягваючы запавольвацца, пачалі фармаваць першыя ядры атамаў.

Перыяд фарміравання першых атамаў у Сусвеце называецца першасным нуклеасінтэзам. Працягваўся ён прыкладна 20 хвілін пасля Вялікага Выбуху. У гэты перыяд Сусвет быў разагрэты да стану, як унутры зорак. У гэты перыяд у асноўным фармаваліся ядры вадароду і гелія ў суадносінах 3 да 1. Такія дзелі вадароду і гелія, двух самых распаўсюджаных элементаў у Сусвеце, назіраюцца і ў наш час.

Пасля таго, як скончыўся першасны нуклеасінтэз, і новыя ядры атамаў ужо амаль не фармаваліся, Сусвет усё яшчэ заставалася гарачай настолькі,

што рэчыва ў ёй знаходзілася ў стане плазмы. У ёй электроны ляталі асобна ад ядраў. Дзякуючы свабодна лятаючым электронам у гэты перыяд Сусвет быў непразрыстым для святла. Фатоны ўвесь час сутыкаліся з электронамі і не маглі ляцець прама, як быццам іх зачынілі ў люстраным лабірынце.

Сусвет працягваў астываць, і праз прыкладна 300 000 гадоў пасля Вялікага Выбуху тэмпература апусцілася дастаткова, каб электроны маглі далучыцца да ядраў атамаў, і, як следства, Сусвет стаў празрыстым. Гэты момант называецца рэкамбінацыяй. Фатоны, якімі было напоўнена ўсё вакол, больш не бачылі перашкод у выглядзе электронаў і змаглі ляцець адразу адусюль і ва ўсе бакі. Фатоны, якія былі вызваленыя ў момант рэкамбінацыі, бачныя і сёння. Праз 13 мільярдаў гадоў яны далятаюць у выглядзе рэліктавага выпраменьвання.

Выяўленне рэліктавага выпраменьвання – адно з галоўных пацвярджанняў Тэорыі Вялікага Выбуху. Важнай яго асаблівасцю з'яўляецца аднастайнасць. На вялікіх маштабах Сусвет аднолькавы ва ўсіх напрамках.

У самой тэорыі ёсць недакладнасці, якія трэба будзе ўстараняць далейшымі больш дакладнымі і падрабязнымі астранамічнымі назіраннямі і распрацоўкай больш дасканалых фізічных мадэляў. Але тая колькасць незалежных крыжаваных дадзеных, якія ўжо ёсць у сучаснай касмалогіі, дазваляюць з упэўненасцю казаць аб тым, што Вялікі Выбух, які стаў адпраўной кропкай пашырэння Сусвету, сапраўды адбыўся.

Паводле вынікаў новых даследаванняў адны з самых магутных касмічных катаклізмаў, выбухаў, якія калі-небудзь назіраліся навукоўцамі-астраномамі, прыводзяцца ў дзеянне масіўнымі касмічнымі аб'ектамі, якія валодаюць неверагодна моцным магнітным полем. Гама-выбухі уяўляюць сабой інтэнсіўныя ўспышкі высокаэнергетычнага рэнтгенаўскага выпраменьвання, зарэгістраваныя астраномамі ў самых розных кутках Сусвету.

Яны з'яўляюцца самымі магутнымі высокаэнергетычных падзеямі, у выніку якіх за кароткі час, ад мілісекунд да некалькіх секунд, у космас вывя-

ргаецца энергія, эквівалентная энергіі, якая выпраменьваецца Сонцам за 10 мільярдаў гадоў.

Прычынамі гама-выбухаў могуць з'яўляцца дзве розныя крыніцы энергіі. Гама-выбухі падзяляюцца на дзве групы па іх працягласці, на кароткія і доўгія адпаведна. Парогам падзелу з'яўляецца час у 2 секунды. Кароткія выбухі ўзнікаюць звычайна пры зліцці дзвюх ці большай колькасці нейтронных зорак, рэштак ад звычайных зорак, мелых неверагодна шчыльную матэрыю і моцнае магнітнае поле. Больш за доўгія гама-выбухі звычайна звязаныя з выбухамі звышновых.

Навукоўцы вылучылі здагадку аб існаванні яшчэ аднаго тыпу гама-выбухаў – звышдоўгага, такія выбухі доўжацца больш за 10 тысяч секунд (2 гадзіны 46 хвілін і 40 секунд). Навукоўцы выявілі чатыры такія падзеі і паспрабавалі высветліць прычыну іх узнікнення, крыніца іх энергіі і іншыя параметры.

Некаторыя падказкі навукоўцам забяспечыў паглыблены аналіз дадзеных гама-выбуху GRB 111209A, зарэгістраванага касмічным апаратам Swift у 2011 годзе. Гэты выбух з'яўляецца самым яркім і самым працяглым з усіх зарэгістраваных гама-выбухаў, працягласць якога склала 15 400 секунд, а энергія выбуху была эквівалентная энергіі, у 500 разоў праўзыходнай энергію, выпраменьваную Сонцам за ўвесь час яго жыццёвага цыклу.

Паколькі ў цяперашні час ужо спынілася нават послесвечение ад гамам-выбуху GRB 111209A, навукоўцы зрабілі назіранні за гэтай часткай космасу пры дапамозе прылады GROND, усталяванага на 2.2-метровым тэлескопе MPG/ESO і прылады X-shooter тэлескопа Very Large Telescope, якія ўваходзяць у Еўрапейскай Паўднёвай Абсерваторыі. Гэтыя назіранні далі вельмі выразны подпіс наяўнасці звышновай зоркі, якая атрымала назву SN 2011kl, і гэта з'яўляецца першым разам у гісторыі астраноміі, калі выбух звышновай быў наўпрост звязаны са звышдоўгім гамам-выбухам. Выбух звышновай адбыўся прыблізна 06/03 мільярда гадоў таму на адлегласці 13

мільярдаў светлавых гадоў ад Зямлі і ён быў выкліканы "смерцю" зоркі, маса якой перавышае масу Сонца ў 8 – 25 разоў.

Раней астраномы меркавалі, што звышновыя зоркі, якія нараджаюць працяглыя гама-выбухі, у канчатковым рахунку ператвараюцца ў чорныя дзюры. Аднак спектр святла, выпраменьванага звышновай SN 2011kl, максімальна набліжаны да спектру выпраменьвання аднаго з радыеактыўных ізатопаў нікеля. Акрамя гэтага, інтэнсіўнасць свячэння SN 2011kl мінімум у тры разы вышэй, чым інтэнсіўнасць свячэння астанкаў звышновых, звязаных з доўгімі гама-выбухамі.

Крыніцай звышдоўгага гама-выбуху з'яўляецца магнетар. Гэта хутка якая верціцца нейтронная зорка, якая валодае моцным магнітным полем, якое мінімум у 5000 трыльёнаў разоў мацней магнітнага поля Зямлі. Далейшыя назіранні за вобласцю выбуху GRB 111209A і іншых звышдоўгіх гама-выбухаў дазволяць навукоўцам праз некаторы час або пацвердзіць гэтую тэорыю, або абвергнуць яе, высунуўшы новую, больш прыдатную да рэаліямі, тэорыю аб паходжанні такіх выбухаў.

Цеплавая смерць Сусвету – гэта канцэптуальная ідэя ў касмалогіі, вылучаная Рудольфам Клаўзіусам у 1865 годзе, якая прадугледжвае, што з часам Сусвет будзе імкнуцца да стану максімальнай энтрапіі аднастайнасці. У гэтым стане ўся энергія і матэрыя ў Сусвеце будзе раўнамерна размеркавана і ізалявана. Такім чынам, усе працэсы і формы жыцця стануць немагчымымі.

З ідэі Цеплавой смерці Сусвету вынікае ідэя аб тым, што ў бясконцай прасторы, маючы бясконцую колькасць часу можа адбыцца ўсё, што заўгодна. У тым ліку і ўзнікненне сапраўды такі ж, як сёння, Сусвету. Гэтая ідэя вынікае таксама з квантавай механікі. Пустая прастора не з'яўляецца зусім пустой, існуюць квантавыя палі, значэнне якіх у любым пункце прасторы заўсёды крыху падрыгвае. Дрыготкі называюць «Квантавымі флуктуацыямі».

Пры бясконцай колькасці часу і прасторы, рана ці позна зноў паўстане стан мінімальнай энтрапіі (ці мінімальнай упарадкаванасці), што можа паслужыць узнікненню асобнай галактыкі, ці новага Сусвету. Гэтак жа ў такой

мадэлі Сусвету высокая верагоднасць узнікнення проста асобнага мозгу ў прасторы, гэтая гіпатэтычная з'ява завецца «Больцманаўскім мозгам».

Тэорыя цеплавой смерці Сусвету не пазбаўлена супярэчнасцей, і яна таксама мае сваіх крытыкаў. Некаторыя з асноўных супярэчнасцяў і крытыкі, звязаныя з гэтай тэорыяй, уключаюць: інфармацыйны парадокс: У тэорыі цеплавой смерці Сусвету мяркуецца, што энтрапія Сусвету будзе імкнуцца да максімуму, і гэта прывядзе да страты інфармацыі.

Аднак паводле прынцыпу захавання інфармацыі ў фізіцы, інфармацыя не можа быць знішчана або страчана беззваротна. Гэты парадокс узнімае пытанне аб тым, якім чынам інфармацыя будзе захоўвацца або аднаўляцца ў меркаванай цеплавой смерці Сусвету.

Тэорыя цеплавой смерці Сусвету заснавана на існуючай фізіцы. Але ў будучыні могуць быць адкрыты новыя фізічныя працэсы або законы, якія могуць змяніць уяўленне аб канчатковым лёсе Сусвету.

Нягледзячы на тое, што цеплавая смерць Сусвету з'яўляецца адным з магчымых сцэнарыяў, існуюць і іншыя гіпотэзы і мадэлі, якія прадказваюць розныя канчатковыя лёсы Сусвету. Некаторыя з іх уключаюць сцэнары "Вялікага разрыву" або магчымасць цыклічных Сусветаў. Крытыкі цеплавой смерці Сусвету зважаюць на неабходнасць разгляду і аналізу гэтых альтэрнатыўных мадэляў.

Дынаміка экасістэм жывой прыроды ў катэгорыях катастрафізму і эвалюцыянізму

Усе прыродныя экасістэмы сфармаваліся натуральным шляхам, без уздзеяння якіх-небудзь антрапагенных фактараў. Яны характарызуюцца ўзаемазвязанасцю ўсіх кампанентаў (клімат, неарганічныя рэчывы і арганічныя злучэнні, расліны і жывёлы), паміж якімі адбываецца абмен рэчывам і энергіяй. Сярод усёй разнастайнасці існуючых прыродных экасістэм вылучаюць 3 асноўныя групы: наземныя, марскія і прэснаводныя.

У сучаснай біялагічнай навуцы Жан Батыст Ламарк лічыцца заснавальнікам эвалюцыйнага падыходу, хаця многія яго здагадкі не пацвердзіліся. У прыватнасці, аказалася, што набытыя ў выніку ўздзеяння на арганізм навакольнага асяроддзя прыкметы не ўспадкоўваюцца. Эвалюцыйная тэорыя, як тэорыя паступовага пераўтварэння відаў жывёл і раслін, паслядоўна была распрацавана Чарльзам Робертам Дарвінам.

Вынікі сваіх навуковых даследаванняў ён выклаў у кнізе: "Паходжанне відаў шляхам натуральнага адбору" (1859 г.). Механізмам эвалюцыі ён лічыў натуральны адбор у барацьбе за існаванне, падчас якога любыя змены, спрыяльныя для выжывання ў дадзеных умовах (абмежаванасць прасторы, ежы, цяпла і святла), павялічваюць здольнасць да размнажэння.

Барацьба за існаванне можа быць міжвідавай, унутрывідавай і барацьбой з неспрыяльнымі ўмовамі навакольнага асяроддзя. Самай вострай з'яўляецца ўнутрывідавая барацьба, паколькі ў асобін дадзенага віду існуюць аднолькавыя патрэбы. У працэсе натуральнага адбору адбываецца выбарчае знішчэнне адных асобін і размнажэнне іншых, а карысныя прыкметы, набытыя ў ходзе эвалюцыі, успадкоўваюцца.

Фактар спадчыннасці забяспечвае ўстойлівасць віду. Кірунак натуральнага адбору можа змяняцца пры змене вонкавых умоў, калі якія-небудзь іншыя прыкметы апыняюцца найважнымі для выжывання. У дзеянне ўступае фактар зменлівасці, які вызначае з'яўленне новых відаў.

Эвалюцыя, па Дарвіне, з'яўляецца павольным працэсам, паколькі, прырода не церпіць скокаў. Аднак павольная эвалюцыя не тлумачыць шэраг асаблівасцяў, злучаных з распаўсюджанасцю выглядаў на Зямлі. Сучасныя навуковыя ўяўленні аб развіцці жывых арганізмаў некалькі адрозніваюцца ад уяўленняў Ч. Дарвіна.

Так, у XX ст. была ўстаноўлена роля ДНК у перадачы спадчыннай інфармацыі, а тэорыя натуральнага адбору дапоўнена тэорый мутацый. Навукоўцы дашлі да высновы, што мутацыі спантанна ўзнікаюць у генах, навакольнае асяроддзе заахвочвае ўдалыя мутацыі, і ў выніку такога адбору

адбываецца эвалюцыя. У канчатковым рахунку, эвалюцыя ўяўляе сабой вынік чарады мутацый, носьбіты якіх альбо выжываюць, альбо гінуць.

У тэорыю эвалюцыі ўключаны дадзеныя генетыкі, палеанталогіі, экалогіі, малекулярнай біялогіі і канцэпцыі дарвінізму, таму яна атрымала назву "сінтэтычная тэорыя эвалюцыі". Строгія законы эвалюцыі да гэтага часу яшчэ не сфармуляваны. Навукоўцы аперуюць гіпотэзамі, мелымі дзелі практычныя пацверджанні. Сінтэтычную тэорыю эвалюцыі прынята падзяляць на дзве структурныя часткі: тэорыю мікраэвалюцыі і тэорыю макраэвалюцыі. У рамках тэорыі мікраэвалюцыі вывучаюцца незваротныя пераўтварэнні папуляцый, якія прыводзяць да фарміравання новага віду.

Папуляцыя з'яўляецца сукупнасцю арганізмаў (асабін) аднаго віду з адзіным генафондам, якія займаюць пэўную тэрыторыю. Усё жывое існуе ў папуляцыях. У кожнай папуляцыі ёсць колькасныя межы: мінімальная колькасць, неабходная для ўзнаўлення і лімітава дасягальны максімум колькасці.

Выгляд – гэта група скрыжаваных паміж сабой арганізмаў, якія не могуць скрыжоўвацца з прадстаўнікамі іншых такіх груп. Выгляд фармуецца толькі ў межах адной папуляцыі. Рэальна выгляд існуе ў форме папуляцый. Тэорыя макраэвалюцыі вывучае паходжанне над краявідных таксонаў, а таксама кірункі і заканамернасці развіцця жыцця на Зямлі ў цэлым, уключаючы паходжанне чалавека.

Тэрмін «таксон» вызначае агульную назву груп арганізмаў. Універсальная класіфікацыя формаў жыцця ўключае наступныя таксоны: выгляд, род, сямейства, атрад (парадак у раслін), клас, тып (аддзел у раслін) і царства. Найменшай ступенню валодае выгляд, найбольшай – царства.

У тэорыі мікраэвалюцыі элементарнай эвалюцыйнай структурай лічыцца папуляцыя. Н. В. Цімафееў-Расоўскі паказаў, што для ўзнікнення эвалюцыйных з'яў патрабуецца дзеянне наступных фактараў: мутацый, флуктуацый колькасці асобін, ізаляцыі папуляцый і натуральнага адбору. Генныя змены – мутацыі – толькі пастаўляюць элементарны эвалюцыйны матэрыял, але самі па сабе не забяспечваюць эвалюцыю.

Атрыманыя ў выніку мутацыі якасці могуць апынуцца разбуральнымі для ўсіх асобін і ў цэлым для папуляцыі. Эвалюцыйная роля флуктуацый колькасці праяўляецца ў двух напрамках. Па-першае, зніжэнне колькасці прыводзіць да павелічэння блізкароднасных скрыжаванняў. Па-другое, памяншэнне разнастайнасці генатыпаў уплывае на кірунак адбору.

Флуктуацыі колькасці могуць працякаць у розных кірунках і не вызначаюць рэчышча спадчынных пераўтварэнняў. Ізаляцыя папуляцый парушае свабоднае скрыжаванне і замацоўвае ўзніклыя адрозненні ў наборах і колькасці генатыпаў у папуляцыі. Ізаляцыя мае як тэрытарыяльна-геаграфічныя, так і біялагічныя прычыны, напрыклад, перавага месцаў харчавання, адрозненне ў тэрмінах размнажэння.

Роля натуральнага адбору ў эвалюцыі выяўляецца на ўзроўні фенатыпу ў цэлым, а не на асобнай фенатыпічнай прыкмеце. Яго генетычны сэнс складаецца ў захаванні ўсярэдзіне папуляцыі вызначаных генатыпаў і выбарчы іх удзел у перадачы генаў наступным пакаленням. Натуральны адбор можа выяўляцца ў дзвюх формах: рухаючы адбор і які стабілізуе адбор.

Рухаючы натуральны адбор дае кірунак, вызначае своеасаблівы вектар папуляцыі, стварае новыя генатыпы. Які стабілізуе натуральны адбор удасканальвае працэсы індывідуальнага развіцця асобін, не змяняючы генатып, у выніку чаго вызначаецца пераважны ў дадзеных умовах фенатып. У цэлым сучасная тэорыя эвалюцыі здавальняюча тлумачыць развіццё жыцця на Зямлі.

Аднак многія працэсы жыцця на нашай планеце носяць катастрафічны характар і не ўкладваюцца ў схему паступовых змен. Па-першае, тэорыя эвалюцыі не можа цалкам растлумачыць феномен зараджэння жыцця. Так, першасная форма жыцця – бактэрыя – мае дзве тысячы энзімаў, або ферментаў-каталізатараў. Падлічана, што шляхам выпадковага супадзення для выдзялення гэтых энзімаў з "першаснага булёна" можа спатрэбіцца ад 40 да 100 млрд. гадоў. Аднак Зямля існуе ўжо 4, 6 млрд. гадоў. Такім чынам, жыццё ўзнікла на нашай планеце гістарычна раптоўна.

Па-другое, эвалюцыя жывой істоты адбываецца ва ўзгодненай змене шматлікіх яго элементаў, якія эвалюцыянуюць адначасова.

Па-трэцяе, эвалюцыя, закранаючы асобныя віды і экалагічныя нішы, у той жа час не закранае іншыя віды і нішы. Напрыклад, на працягу апошніх 165 млн. гадоў зусім не змяніліся акулы. Каля 3 млн. гадоў назад у Афрыцы, у зоне Ўсходне-Афрыканскага разлома, адбываліся катастрафічныя працэсы геалагічнай актыўнасці, і тамака паўсталі лакальныя зоны працяглага ўздзеяння на флору і фауну радона – радыёактыўнага газу магматычнага паходжання. Высокі радыеактыўны фон гэтых месцаў у шмат разоў узмацніў мутацыйныя змены, што паскорыла развіццё ўсходнеафрыканскіх прыматаў і, у канчатковым рахунку, прывяло да з'яўлення чалавека.

Натуральны адбор уздзейнічае на жывых істот інтэгральна і камбінавана. Ён адначасова ўплывае на іх цела, развіццё і паводзіны. Але, верагодна, у развіцці выяўляе сябе і іншая сіла эвалюцыі – самаарганізацыя. Самаарганізацыя – фундаментальнае паняцце сінэргетыкі, якое азначае парадкаванне, г.зн. пераход ад хаосу да структураванага стану, тое, што адбываецца спантанна ў адкрытых нелінейных сістэмах. Адкрытасць уяўляе сабой уласцівасць сістэм, якое праяўляецца ў іх здольнасці да абмену рэчывам, энергіяй і інфармацыяй з навакольным асяроддзем, а нелінейнасць мяркуе шмат варыятыўнасць шляхоў эвалюцыі.

Самаарганізацыя азначае, што любыя жыццёвыя працэсы адбываюцца не за кошт унутранага ўздзеяння, а за кошт унутраных змен самой сістэмы. Цяпер на нашай планеце існуе каля 50 млн. відаў жывёл і раслін. Аднак з моманту з'яўлення жыцця на Зямлі жывёльны і раслінны светы мелі прыблізна 50 млрд. відаў. Адсюль вынікае, што з усіх відаў, якія калі-небудзь існавалі, ацалеў толькі адзін з тысячы, г.зн. да гэтага часу 99,9% відаў загінулі. Пры гэтым знішчэнні, звязаныя са станаўленнем чалавецтва, склалі ўсяго толькі 5%, астатнія віды жывых арганізмаў загінулі самі.

Аптымальная працягласць жыцця асобна ўзятага віду складае 4 млн. гадоў, а ў млекакормячых – толькі 1 млн. гадоў. На працягу некалькіх мільё-

наў гадоў кожны від фармуецца, памнажаецца і квітнее, а затым вымірае. У сярэднім за ўсю гісторыю жыцця на планеце ў дзень гінула па адным відзе.

Што ж прыводзіць віды да знікнення з рэгулярнасцю ў 4 млн. гадоў? Галоўным фактарам гэтага працэсу з'яўляецца геалагічная актыўнасць Зямлі. Так, за апошнія 50 тыс. гадоў трапічныя лясы рэзка скараціліся.

З прычыны гэтага ў дажджавых экватарыяльных лясах паступова зменшылася разнастайнасць, стала знікаць непаўторная флора і фауна. 10 тыс. гадоў таму леднікі даходзілі да тэрыторыі цяперашняга Нью-Йорка, а зараз адступілі далёка на поўнач. Віды жывуць, развіваюцца і знікаюць у вельмі зменлівым навакольным асяроддзі. Гэтым, відаць, тлумачыцца 90% усіх выпадкаў іх вымірання.

Але з буйнымі жывёламі (напрыклад, дыназаўрамі) справа ідзе значна складаней. Магчыма, што гэтыя жывёлы вымірaюць не з-за няздольнасці адаптавацца да зменлівых умоў жыцця, а з-за ўласных паводзін. Не толькі навакольнае асяроддзе, але і самі складаныя жывыя істоты здольныя мяняцца і не заўсёды ў лепшы для іх бок. У адных выпадках іх паводзіны могуць так хутка змяніць навакольнае асяроддзе, што прывядзе гэтых жывёл да знікнення. У іншых выпадках жывёлы перастаюць прыстасоўвацца да змен у навакольным асяроддзі і таксама хутка гінуць.

Ідэям аб бесперапынным эвалюцыйным развіцці жывой прыроды супрацьстаіць тэорыя катастроф, распрацаваная Жоржам Кюўе. Даследуючы выкапняў жывёл, навуковец ўсталяваў сувязь паміж іх будовай і палеанталагічнымі перыядамі.

Ён заўважыў, што пры пераходзе ад старажытных да пазнейшых геалагічных пластоў будынак выкапняў жывёл ускладняецца. Гэтыя ўскладненні прыродазнаўца звязаў з катастрафічнымі зменамі ў навакольным асяроддзі. Паколькі сярод марскіх утварэнняў сустракаюцца пласты, запоўненыя рэшткамі сухапутных і прэснаводных жывёл і раслін, разважаў ён, то часткі сушы перыядычна затаплялiся.

Разрывы і заломы, назіраныя ў найстаражытных пластах Зямлі, сведчаць аб дзеяннях раптоўных і грандыёзных з'яў прыроды. Спасылаючыся на адсутнасць пераходных формаў жывых істот, Кюўе прыйшоў да высновы, што біялагічныя віды самі па сабе нязменныя, а зніклыя віды былі гэтак жа пастаянныя, як і сучасныя. У 1786 г. ён першым заявіў аб вымiранні відаў. Першапрычынай глабальных вымiранняў Жорж Кюўе лічыў марскія патопы, але гэтая гіпотэза сучаснымі біёлагамі і геолагамі не пацвердзілася.

Акіян надыходзіць не спяшаючыся, адваёўваючы ў сушы па міліметры ў год. Да такога тэмпу раслінны і жывёльны свет паспявае прыстасавацца, і хуткага масавага вымірання не адбываецца. Лакальныя паводкі, хуткія затапленні сушы, былі ў мінулым неаднаразова, але на вельмі абмежаванай прасторы. Прыкладам стала Міжземнае мора.

Яго дно паступова запоўнілася трохкіламетровым пластом гіпсу і солі, утвораным падчас выпарэння марской вады, а ў цёплых расолах неглыбокіх азёр, якія захаваліся ў некаторых месцах, маглі выжыць толькі адмысловыя бактэрыі – галархеі. Гэты этап у гісторыі рэгіёна называюць Месінскім крызісам. 5,33 млн. гадоў назад воды Атлантычнага акіяна пачалі пранікаць па тэктанічных расколін праз заходні борт катлавіны.

Вада пратачыла ў пародах даволі шырокае рэчышча – цяперашні Гібралтарскі праліў – і лінула ў сухую, засоленую нізіну. Напаўненне Міжземнага мора адбывалася вельмі хутка, усяго 15-20 тыс. гадоў, на працягу якіх у ім пасяліліся звычайныя марскія арганізмы.

Тэорыя эвалюцыі грунтуецца на дадзеных палеанталогіі – навукі, якая займаецца вывучэннем захаваных рэштак жывых істот. У палеанталогіі выкарыстоўваецца геахраналагічная шкала часу, прынятая ў 1881 г. у Балонні на Міжнародным геалагічным кангрэсе, якая адлюстроўвае асноўныя даты ў гісторыі нашай планеты.

Найбольш старажытная частка гісторыі Зямлі называецца крыптазоем. Яна ахоплівае інтэрвал ад 570 да 3800 млн. гадоў таму. У гэты перыяд ар-

ганічнае жыццё знаходзілася ва ўтоеным стане. Наступная частка, працягласцю ў 570 млн. гадоў, называецца фанеразоем.

Фанерозай падзелены на тры эры: палеозай (эра «старажытнага жыцця»), мезазой (эра «прамежкавага жыцця») і кайнозой (эра «новага жыцця). Эры падзяляюцца на перыяды. Першыя жывыя арганізмы з'явіліся на Зямлі прыкладна 3,5 млрд гадоў таму. Гэта былі найпростыя істоты - мікраарганізмы. Для кембрыйскага перыяду характэрны арганізмы больш высокай складанасці.

Жыццё развівалася ў асноўным у морах і была прадстаўлена прымітыўнымі ракападобнымі, малюскамі, караламі. Марскія пазваночныя жывёлы – шчытковыя рыбы, марскія зоркі – з'явіліся 450 млн. гадоў таму.

Жыццё, бурна якая развівалася ў морах у ардовікскій перыяд, 440 млн. гадоў назад стала згасаць з-за абледзянення. У сілуры і дэвоне жыццё ўпершыню выйшла на сушу. Да істотных змен у абліччы планеты прывяло ўзбагачэнне раслiннага покрыва Зямлі дрэвамі і хмызнякамі, якія даюць насенне, якое адбылося прыкладна 360 – 385 млн. гадоў назад. Лічыцца, што сотні тысяч гадоў таму было дастаткова, каб шырокія лясы пакрылі аголеныя да таго скалы, пяскі і землі ўсіх кантынентаў.

Самае масавае за ўсю гісторыю нашай планеты выміранне жывых істот адбылося 251 млн. гадоў таму, у канцы палеазойскай эры. Звыш 90% марскіх і 70% наземных відаў назаўжды зніклі з твару Зямлі – засталіся толькі самыя дробныя і прымітыўныя. У Сусветным акіяне спынілася адукацыя рыфаў, датуль распаўсюджаных па ўсіх морах, а на сушы – назапашванне вугалю, бо зніклі якія пакрывалі яе пышныя лясы з дрэвападобных дзеразы, папараці і разнастайных старажытных голанасенных.

Ацалелі некаторыя наземныя амфібіі, а таксама рэптыліі, напрыклад, протерозухіі – продкі дыназаўраў, цынадонты – зверападобныя яшчары, продкі млекакормячых, і листрозавры – іх аддаленыя сваякі. Гэта былі жывёлы невялікага памеру, якім на падтрыманне актыўнасці патрабавалася менш энергетычных затрат, а значыць, яны спажывалі менш кісларoду. Сярод мар-

скіх жывёл катастрофу перажылі таксама самыя дробныя форамініферы, брахіапады, двухстворкі, паколькі ім патрабавалася менш ежы і кісларо-ду.

Наземная флора пацярпела не менш, чым фауна, – якія змяшчаюць хлор вылучэння вулканаў руйнавалі азонавы пласт, цвёрдае ўльтрафіялетавае выпраменьванне калечыла яшчэ не праслыя спрэчкі, сернокіслой дажджы выпальвалі лістоту, а апошнія сокі з адміраючых дрэў высмоктвалі распладзіліся грыбы. Былы ўзровень біяразнастайнасці на Зямлі аднавіўся толькі праз 60 млн. гадоў, да сярэдзіны юрскага перыяду.

Раслінны і жывёльны светы загінулі з-за недахопу кісларо-ду, якая ўзнікла пры раскладанні мёртвай арганікі, пакінутай акіянам пры адступленні ад мацерыка. Адходы жыццядзейнасці лясных масіваў выносіліся ў мора. Утвараліся вялізныя плантацыі багавіння, якое, адміраючы, падалі на дно. Працэс іх раскладання паглынаў кісларод, які знаходзіцца ў вадзе. Насельнікі акіянаў сталі задыхацца, марское дно апусцела. У выніку пермскі перыяд скончыўся грандыёзным катаклізмам.

Сярод вонкавых чыннікаў вымірання навукоўцы таксама завуць катастрофу, выкліканую магутнымі вулканічнымі выліваннямі на тэрыторыі Ўсходняй і збольшага Заходняй Сібіры. Гэта была кароткачасовая па геалагічным маштабе падзея, якая моцна паўплывала на біясферу. Яго сляды адлюстраваны ў выглядзе шырокай тоўшчы базальтаў, магутнасцю некалькі кіламетраў, званых Сібірскімі трапамі.

Апошняя ў гісторыі Зямлі глабальная катастрофа адбылася 65,5 млн гадоў таму. Прычынай катастрофы стаў гіганцкі метэарыт, які ўпаў на Зямлю. Метэарыт меў у даўжыню каля 10 км., ён урэзаўся ў Зямлю са скорасцю 20 км. у секунду і пакінуў катлаван глыбінёй 20 км. Месца падзення гэтага нябеснага цела – паўночны бераг паўвострава Юкатан у Мексіцы.

Пра гэта сведчыць размешчаны там кратэр Чыксулуб, час з'яўлення якога прыкладна супадае з дадзенай падзеяй. Адбыўся жахлівы выбух, які суправаджаўся выкідам энергіі, які ў 10000 разоў перавышае ўсе цяперашнія ядзерныя запасы.

У выніку магутнага катаклізму ў атмасферу было выкінута 100 млрд. тон серы, паветра напоўнілася сярністымі злучэннямі, а лясы ахапілі пажары. Вялікая частка насельнікаў мезазоя загінула ад ударнай і цеплавой хваляў, атрутных выкідаў, кіслотных дажджоў, ураганаў і цунамі. Аблокі пылу і клубы дыму, якія паднялiся ў атмасферу, на доўгія месяцы агарнулі планету. Яны адлюстроўвалі сонечныя промні; у выніку пачалося рэзкае пахаладанне, і расліннасць, пакінутая без святла і цеплыні, стала гінуць.

Затым адбылося масавае выміранне пазбаўленых ежы жывёл. З гэтай катастрофай звязваюць гібель 35% відаў насельнікаў акіянаў, а таксама ўсіх буйных рэптылій: марскіх яшчараў, дыназаўраў і птэразаўраў. У неа катастрафізме – так зараз называецца абноўленая тэорыя Жоржа Кюўе – вельмі шмат здагадак, якія да гэтага часу не маюць дакладных эмпірычных доказаў.

Калі існаванне эпох магутнага вулканізму, якія пакінулі прыкметныя сляды ў зямной кары, не падлягае сумневу, тое даказаць падзенне астэроіда і ўсталяваць час яго выбуху не так ужо проста. Акрамя таго, надзвычай складана зразумець, якім чынам наступствы катастрофы прывялі да вымірання відаў. Пры кожнай глабальнай катастрофе нараўне са зрынутымі відамі знаходзіліся і пераможцы, якія пасля запаўнялі сабой жыццёвую прастору, якая вызвалілася.

Але ніводны від не быў датычны ні да самой катастрофы, ні да выжывання іншых відаў. Якая пагражае Зямлі глабальная катастрофа, калі яна адбудзецца, верагодна, будзе злучана не з уплывам вонкавых касмічных сіл або ўнутраных працэсаў у зямной кары і біясферы, а з дзейнасцю чалавека.

Чалавек як крыніца небяспекі

З часам у іх сталі з'яўляцца небяспекі, стваральнікам якіх стаў сам чалавек. Чалавек жыве і дзейнічае ва ўмовах пастаянна змяняюцца патэнцыяльных небяспек. Гэта дазваляе сфармуляваць аксіёму аб тым, што любая дзейнасць або бяздзейнасць патэнцыйна небяспечная.

У цяперашні час чалавек больш за ўсё пакутуе ад сваёй дзейнасці, ад тых небяспек, якія ён сам стварае. Па меры таго, як развіццё тэхналогій паскарае прагрэс, уплыў эканамічнай дзейнасці чалавека на навакольнае асяроддзе становіцца ўсё больш разбуральным. Усё больш і больш трапляе ў прыроду і ўсё больш чужародных для яе рэчываў, часам вельмі таксічных для жывых арганізмаў.

Чалавека з пазіцыі бяспекі жыццядзейнасці неабходна разглядаць як патэнцыйна небяспечны фактар, уздзеянне якога на навакольныя аб'екты можа вывесці іх за межы ўстойлівасці. Ёсць дзве асаблівасці праявы ўздзеяння чалавека на прыроднае асяроддзе: тэхналагічнае развіццё чалавецтва суправаджаецца перадачай чалавеку ўсё большай колькасці функцый кіравання, што дазваляе яму ўсё далей і далей адыходзіць ад гармат працы і пераходзіць ад выканання да орган кіравання сістэмай вытворчасці. Такое пераўтварэнне ролі чалавека прыводзіць да замены фізічнага разумовай працы, зніжэння патрэбы ў мышачнай працы і адпаведных энергетычных выдаткаў. Аднак гэта значна павялічвае нагрузку на псіхіку чалавека.

Галоўным вінoўнікам няшчасных выпадкаў становіцца, як правіла, не тэхніка, не арганізацыя працы, а сам працуючы чалавек, які па тых ці іншых прычынах не выконваў правілы тэхнікі бяспекі.

Больш за 60% няшчасных выпадкаў тлумачыцца няведаннем або парушэннем патрабаванняў аховы працы, дысцыпліны, нездавальняючай арганізацыяй вытворчасці.

Агульны разгляд заканамернасцей развіцця і жыццядзейнасці чалавека дазваляе заўважыць, што акалічнасці спрыяюць росту колькасці няшчасных выпадкаў, якія адбываюцца па цалкам аб'ектыўных прычынах. Першая прычына выяўляецца з аналізу эвалюцыі чалавека. З развіццём прылад працы пашыраецца дыяпазон уздзеяння чалавека на навакольны свет. У той жа час спектр адказаў пашырыўся рэакцыямі знешняга свету.

Калі першабытны чалавек па сваіх індывідуальных фізічных характарыстыках быў здольны супрацьстаяць якія ўзнікаюць у той час у працэсе працоўнай дзейнасці небяспекам, то магчымасці сучаснага чалавека істотна адстаюць па ўзроўні павышанай небяспекі. З развіццём тэхналогій небяспека расце хутчэй, чым чалавечае супраціўленне ім. Другая прычына, якая робіць умовы чалавечай працы і жыцця больш жорсткімі і небяспечнымі, – павелічэнне кошту памылкі.

Адплата за памылку першабытнага чалавека была не такой вялікай, а вось памылкі сучаснага чалавека каштавалі яму значна даражэй. Трэцяя прычына – адаптацыя чалавека да небяспекі. Карыстаючыся перавагамі тэхналогіі, людзі часта забываюць, што тэхналогія таксама з'яўляецца крыніцай высокай небяспекі, і інтэнсіўнае яе выкарыстанне павялічвае магчымасць рэалізацыі небяспекі. З-за выгод чалавек свядома парушае правілы бяспекі. Не кожнае парушэнне цягне за сабой ДТЗ. Людзі, якія адноўчы беспакарана парушалі правілы і, атрымаўшы за гэта нейкія выгоды, паўтараюць падобныя парушэнні.

Паступова адбываецца адаптацыя не толькі да небяспекі, але і да парушэнняў правілаў бяспекі. Акрамя агульных прычын, выяўляецца мноства індывідуальных фактараў, якія спрыяюць наўмысным парушэнням правілаў бяспекі працы і павелічэнню колькасці няшчасных выпадкаў.

Праблемы, звязаныя з праявамі чалавечага фактару, разглядаюцца як аналіз надзейнасці чалавека, які ўключае ў сябе вызначэнне магчымых крыніц чалавечых памылак на працягу ўсяго перыяду, які папярэднічаў аварыям. Гэтыя памылкі можна падзяліць на памылкі, недагляды і праявы злога намеру. Значная частка небяспек рэалізуецца пад уздзеяннем і непасрэдным удзелам самога чалавека, абумоўленых яго паводзінамі, наяўнымі псіхафізіялагічнымі асаблівасцямі і магчымасцямі арганізма чалавека.

Так, 45% аварый на АЭС, 60% авіякатастроф, 80% марскіх і 90% аўтамабільных аварый адбываюцца выключна па віне персаналу пастаўшчыка паслуг па розных прычынах.

Прычыны ўзнікнення небяспечных сітуацый і вытворчага траўматызму, звязаныя з чалавечым фактарам, можна разбіць на розныя ўзроўні: пры аднолькавых абставінах для ўсіх работнікаў вызначальнае значэнне ў фарміраванні паводзінаў кожнага чалавека маюць яго індывідуальныя якасці, якія адлюстроўваюць сукупнасць сацыяльна-псіхалагічныя і фізіялагічныя ўласцівасці. Да іх ставяцца тып нервовай сістэмы, тэмперамент, характар, асаблівасці мыслення, адукацыя, вопыт, адукаванасць, здароўе і іншыя якасці. Шырокі спектр асаблівасцяў асобы, сацыяльных абставін і вытворчых умоў працы фармуецца псіхалагічнымі прычынамі наўмыснага парушэння правілаў бяспекі працы. У кожным дзеянні чалавека вылучаюць тры функцыянальныя часткі: пабуджальную, арыентыровачную і выканаўчую.

Шырокі спектр уласцівасцяў асобы, сацыяльных абставінаў і вытворчых умоў працы фармуюць псіхалагічныя прычыны свядомага парушэння правілаў бяспечнай працы. У кожным дзеянні чалавека вылучаюць тры функцыянальныя часткі: матывацыйную, арыенціровачную і выканаўчую.

Парушэнне ў любой з гэтых частак цягне за сабой парушэнне дзеяння

у цэлым. Чалавек парушае правілы і інструкцыі: альбо ён не хоча іх выконваць, альбо ён не ведае, як гэта зрабіць, альбо ён не ў стане гэта зрабіць. На аснове такіх даследаванняў вырашаюцца задачы не толькі прыстасаванні тэхнікі і асяроддзя да чалавека, але і фарміравання ў работнікаў здольнасцяў у адпаведнасці з патрабаваннямі, якія прад'яўляе тэхніка.

Прычыны памылак

Памылка – гэта вынік дзеяння, здзейсненага недакладна ці няправільна, насуперак плану. У тых выпадках, калі небяспечныя ці неадэкватныя дзеянні

здзяйсняюцца чалавекам свядома (наўмысна), яны класіфікуюцца як парушэнні і ў дадзеным тэксце не аналізуюцца. Памылка вызначаецца як невыкананне пастаўленай задачы (або выкананне чалавекам забароненага дзеяння), якое можа з'явіцца прычынай цяжкіх наступстваў – траўмаў, гібелі людзей, пашкоджанні абсталявання або маёмасці або парушэнні нармальнага ходу запланаваных аперацый.

Памылкі па віне чалавека могуць адбывацца ў розных сферах і ўмовах яго жыццядзейнасці: на адпачынку, у час падарожжа, пры занятку спортам. Напрыклад, памылкі часта ўзнікаюць пры кіраванні аўтатранспартам; пры неасцярожным абыходжанні з агнём, вострымі прадметамі, са зброяй; пры купанні ў вадаёмах; пры падарожжы ў гарах; на трэніроўках і спаборніцтвах па розных відах спорту.

У побыце памылкі маюць месца пры выкарыстанні электрапрыбораў, бытавога газу, адчыненага агню. Яны адбываюцца пры ўжыванні ядахімікатаў, прылады і прынад; пры абыходжанні з бытавымі адходамі, кіпячымі вадкасцямі, з прадметамі, якія змяшчаюць ртуць; пры спажыванні недабраякасных прадуктаў, алкаголю, медыкаментаў.

У сферы вытворчай дзейнасці памылкі ўзнікаюць, калі чалавек дзейнічае з парушэннем устаноўленага рэжыму працы або бяздзейнічае ў момант, калі яго ўдзел у працэсе дзейнасці неабходны.

У надзвычайных сітуацыях натуральнага і тэхнагеннага паходжання памылкі звычайна звязаны з непадрыхтаванасцю людзей да дзеянняў ва ўмовах НС; з няўменнем іх прадбачыць вынікі сваіх дзеянняў, напрыклад, пры абыходжанні з гаручымі і выбуховымі рэчывамі або пры кіраванні складанымі тэхнічнымі сістэмамі; пры сходзе лавін, селяў і да т.п.

Пры зносінах людзей паміж сабой крыніцамі памылак могуць быць непрыстойнасць, нядбайнасць, помста, рэўнасць, абразы, рэлігійныя і нацыянальныя канфлікты і да т.п.

Пры кіраванні эканомікай і іншай дзяржаўнай дзейнасцю памылкі абумоўлены імкненнем людзей парушыць законы прыроды. Да іх варта

аднесці будаўніцтва ЦПК на востраве Байкал; праекты павароту паўночных рэк на поўдзень.

Уласцівасць чалавека памыляцца з'яўляецца функцыяй яго псіхалагічнага стану, а інтэнсіўнасць памылак шмат у чым залежыць ад стану навакольнага асяроддзя і дзейных нагрузак. Устаноўлена, што залежнасць частаты з'яўлення памылак ад дзеючых нагрузак з'яўляецца нелінейнай. Так, пры вельмі нізкім узроўні нагрузак большасць аператараў працуюць неэфектыўна (заданне здаецца сумным і не выклікае цікавасці), а якасць працы далёка ад жаданага. Пры ўмераных нагрузках якасць працы аператара аказваецца аптымальным, таму ўмераную нагрузку можна разглядаць як умовы, дастатковыя для забеспячэння ўважлівай працы чалавека-аператара.

Пры далейшым павелічэнні нагрузак якасць працы чалавека зноў пагаршаецца, што тлумачыцца, галоўным чынам, праявамі фізічнага стрэсу, такімі як страх, неспакой, пачашчэнне пульса і частаты дыхання, павышэнне тэмпературы, выкіду ў кроў адрэналіну.

У сістэме "чалавек – асяроддзе пасялення" чалавек з'яўляецца самым зменлівым складнікам. Яго паводзіны вызначаюцца масай індывідуальных фактараў. Розныя аператары аналагічныя заданні выконваюць не аднолькавымі дзеяннямі.

Асноўныя асаблівасці асобы і станы арганізма чалавека, якія штурхаюць яго да здзяйснення памылак, можна падзяліць на прыроджаныя асаблівасці і часовыя станы.

Да прыроджаных асаблівасцяў адносяцца фізіялагічныя характарыстыкі чалавека і асаблівасці, абумоўленыя яго спадчыннасцю. У іх ліку органы пачуццяў (слых, зрок, нюх, дотык, густ), апорна-рухальная сістэма (цягліцавая сіла, хуткасць руху, каардынацыя і да т.п.). Сюды ж можна ўключыць псіхаматорную сістэму чалавека (рэфлексы, рэакцыі) і яго інтэлект (узровень ведаў, здольнасць арыентавацца ў навакольным асяроддзі).

Часавыя станы, такія як фізічная і псіхалагічная стомленасць, якія прыводзяць да зніжэння ўвагі і цягліцавай сілы, пагаршэнню стану здароўя і працаздольнасці, спрыяюць узнікненню памылак. Чыннікі памылак падзяляюць на непасрэдныя, галоўныя і спрыяльныя.

Непасрэдныя памылкі залежаць ад псіхалагічнай структуры дзеянняў аператара. Гэта памылкі ўспрымання, памылкі памяці, памылкі мыслення (не зразумеў, не прадугледзеў, не абагульніў).

Галоўныя прычыны памылак звязаны з працоўным месцам, арганізацыяй працы, падрыхтоўкай аператара, станам арганізма, псіхалагічнай устаноўкай, псіхічным станам арганізма.

Якія спрыяюць чыннікі памылак залежаць ад асаблівасцяў асобы (характару, тэмпераменту, камунікатыўных асаблівасцяў), станы здароўя, вонкавых умоў, прафесійнага адбору, навучанні і трэніроўкі.

Прычыны памылак можна таксама класіфікаваць, выкарыстоўваючы кібернетычную схему: памылкі ў арыентацыі (неатрыманне інфармацыі); памылкі ў прыняцці рашэння (няправільныя рашэнні); памылкі ў выкананні дзеянняў (няправільныя дзеянні). Памылкі ў арыентацыі найболей распаўсюджаныя і ўзнікаюць звычайна з-за адсутнасці сігналу, з-за слабога сігналу, з-за мноства адначасовых сігналаў.

Памылкі ў прыняцці рашэння могуць узнікаць, калі атрымана ўся неабходная, дакладная інфармацыя і ў дастатковым аб'ёме, але працэс аналізу, перапрацоўкі і асэнсавання яе быў няслушным; або з-за неадэкватнай адзнакі сітуацыі; непрыстасаванасці да працы з-за недахопу ведаў, досведу.

А часам інфармацыя і прынятае рашэнне могуць быць правільнымі мі, але зваротнае дзеянне памылковым. Няправільнае дзеянне можа выяўляцца і ў бяздзейнасці аператара ў той момант, калі яго дзеянне неабходна (няздольнасць да дзеяння, парушэнне паслядоўнасці дзеянняў), ці ў няправільным выбары дзеянняў (неадэкватнае размяшчэнне прыбораў, недастатковасць увагі, стомленасць і г.д.).

Віды памылак, якія дапускаюцца чалавекам на розных стадыях стварэння і выкарыстання тэхнічных сістэм, можна класіфікаваць наступным чынам. Памылкі праектавання абумоўлены нездавальняючай якасцю праектавання. Напрыклад, кіравальныя прылады і індыкатары могуць быць размешчаны настолькі далёка сябар ад сябра, што аператар будзе выпрабоўваць цяжкасці пры адначасовым карыстанні імі.

Могуць мець месца памылкі выраба і рамонту, напрыклад, няправільнай зваркі, няправільнага выбару матэрыялу, вырабы выраба з адхіленнямі ад канструктарскай дакументацыі; памылкі тэхнічнага абслугоўвання падчас эксплуатацый з прычыны недастатковай падрыхтаванасці абслуговага персанала, нездавальняючага абсталявання неабходнай апаратурай і прыладамі.

Таксама могуць мець месца памылкі звароту. Яны ўзнікаюць з прычыны нездавальняючага захоўвання вырабаў або іх транспарціроўкі з адхіленнямі ад рэкамендацый вытворцы.

З памылак у арганізацыі працоўнага месца вынікаюць цесната працоўнага памяшкання, падвышаная тэмпература, шум і недастатковая асветленасць. Памылкі ў кіраванні калектывам прыводзяць да недастатковага стымулявання спецыялістаў і іх псіхалагічнай несумяшчальнасці.

Адбываецца пашкоджанне арганізма, якое пры дасягненні вызначанай ступені змен кваліфікуецца як няшчасны выпадак (траўма) ці захворванне. Пашкоджанне арганізма можа, адбыцца ў выніку як непасрэдных кантактных вонкавых уздзеянняў (механічных, электрычных і хімічных), так і дыстанцыйных (цеплавога і светлавога). Пашкоджанні могуць узнікаць адразу пасля ўздзеяння або праз пэўны час пасля яго (напрыклад, пасля радыяцыйнага апрамянення).

Небяспечныя і шкодныя фактары звычайна маюць вонкава вызначаныя прасторавыя вобласці іх праявы, так званыя небяспечныя зоны. Знаходжанне чалавека ў небяспечнай зоне з'яўляецца адной з умоў узнікнення

пашкоджання арганізма. Пры гэтым небяспечны фактар (небяспека) павінен валодаць дастатковай энергіяй, каб выклікаць пашкоджанне арганізма.

Але ў большасці выпадкаў людзі самі не надаюць належнага значэння ўтоенай небяспекі і паступаюць сабе на шкоду. Характэрны прыклад грэблівага стаўлення да небяспекі – парушэнне правіл вулічнага руху. Небяспекі могуць выяўляцца ў выглядзе аварый тэхнічных сістэм, пажараў, выбухаў і іншых цяжка прадказальных падзей. Пападаючы ў зону дзеяння падобных экстрэмальных сітуацый, людзі рызыкуюць атрымаць траўмы рознай ступені цяжкасці. Чалавек і сам часта з'яўляецца крыніцай небяспекі.

Сваімі дзеяннямі або бяздзейнасцю ён можа стварыць для сябе і навакольных рэальную пагрозу жыццю і здароўю. Небяспекі, якія ствараюцца чалавекам, вельмі разнастайныя. Войны, канфлікты, злачынствы, прастытуцыя, наркаманія, голад, галеча і бескультур'е чалавечага грамадства фармуюць сацыяльныя небяспекі.

Які б дзейнасцю ні займаўся чалавек, дзе б ён ні знаходзіўся, заўсёды побач з ім існуюць схаваныя сілы, якія ўяўляюць для яго пагрозу. Чыннікам няшчаснага выпадку вельмі часта служыць бестурботнасць ці неасцярожнасць навакольных. Для захавання здароўя і жыцця неабходна добра ведаць і своечасова ўстараняць прычыны, пры якіх адбываецца ператварэнне патэнцыйных небяспек у сапраўдныя небяспекі.

Уберагчыся ад няшчасця ўдаецца не заўсёды, паколькі некаторыя небяспекі не залежаць ад дзеянняў людзей, выяўляюцца раптоўна, не пакідаючы часу на разважанне, на выратаванне, напрыклад, выбух, землятрус і ўраган. Небяспека можа быць ацэнена колькасна, напрыклад, велічынёй рызыкі.

Пад рызыкай як колькаснай мерай небяспекі звычайна маюць на ўвазе магчымасць (або верагоднасць) узнікнення непажаданай падзеі за пэўны адрэзак часу. У ліку рызык аўтамабільныя катастрофы, злачынствы, атручэнне, наўмыснае забойства, утапленне, падзенне, пажар і апёк і авіякатастрофа.

Крымінальныя небяспекі і віктымалогія

Віктымалогія – гэта вучэнне аб паводзінах ахвяры, якое тлумачыць, чым кіруецца вулічны рабаўнік або гвалтаўнік падчас выбару ахвяры.

Бэці Грейсан шляхам серыі даследаванняў паказала, што злачынцу патрабуецца ў сярэднім сем секунд для візуальнай ацэнкі патэнцыйнага аб'екта для нападу – яго фізічнай падрыхтоўкі і тэмпераменту. Злачынец адзначае няўпэўненасць погляду, млявую выправу, нясмеласць рухаў, псіхічную прыгнечанасць, фізічныя недахопы і стома.

У выніку матэматычнага аналізу высветлілася, што патэнцыйную ахвяру злачынцы часта вылучаюць па некаторых адметных асаблівасцях, рухаў. Гэта можа быць іх агульная няўзгодненасць, нязграбнасць хады – занадта размашыстая або семянючая, якая прыцягвае ўвагу на фоне адзінага людскога патоку.

Джоўл Кірх і Джорджам Леанарда вызначылі дзве абагульненыя катэгорыі людзей: так званую «групу рызыкі» і тых, каму практычна не пагражае небяспека стаць аб'ектам нападу. Першыя з іх дрэнна фізічна арганізаваны, расслабленыя і несабраныя псіхічна. Другія ўпэўненыя ў сабе. Яны глядзяць і ідуць упэўнена.

Чалавеку, які пачуваецца які адносіцца да групы рызыкі, для пачатку варта вывучыць уласную хаду, жэсты, міміку і заняцца іх карэкцыяй. Выбіць сабе ўпэўнены стыль паводзін і прытрымлівацца яму сярод вулічнага натоўпу можа любы.

Лічбавае насілле

Лічбавым гвалтам называюцца маніпулятыўныя дзеянні над чалавекам з мэтай кантролю, запалохвання або прычынення шкоды з прымяненнем інтэрнэт-платформ. Такі гвалт на сённяшні дзень распаўсюджаны ў сям'і, у школе, універсітэце, на працы, у дадатках знаёмстваў. Лічбавае насілле можа

выяўляцца ў розных формах. Калі гэта датычыцца дзяцей (да 18 гадоў), то часцей сустракаецца кібербулінг (траўленне ў інтэрнэце) і кібергрумінг (калі дарослы чалавек спрабуе завесці знаёмства з дзіцем).

Жанчыны сутыкаюцца з апкертынгам (фотаздымка інтымных месцаў без згоды), латшэймінгам (калі навакольныя асуджаюць спробы жанчыны выглядаць прывабна і сэксуальна) і порнамесцю (размяшчэнне ў інтэрнэце матэрыялаў сэксуальнага характару без згоды людзей, намаляваных на іх). Па статыстыцы жанчыны падвяргаюцца лічбаваму гвалту часцей за мужчын.

Лічбавае насілле ў партнёрскіх адносінах распазнаць асабліва складана. Яно часта маскіруецца пад клопат: «Чаму не бярэш трубку? Я ж перажываю» ці «Ты дзе? Ужо паўгадзіны прайшло, а ты да гэтага часу не дома».

У гэтых выпадках партнёр спрабуе падпарадкаваць іншага партнёра, кіраваць ім і стаць галоўным у пары. Таму другому партнёру прасцей стала паведамляць, дзе ён і з кім своечасова адказваць у мэсэнджарах, паказваць перапіскі з сябрамі.

Як выяўляецца лічбавае гвалт. Не пытаючыся дазволу, партнёр чытае перапіскі, правярае часопіс званкоў і паведамленняў. Партнёр сочыць. Без вашага ведама устанаўлівае на тэлефон прыкладанні для адсочвання месцазнаходжання або схаваныя камеры ў кватэры. Партнёр кантралюе доступ да інтэрнэт-платформ, просіць паролі і коды, вырашае з кім мець зносіны, а з кім не варта. Партнёр увесь час спрабуе быць на сувязі.

Званкі і паведамленні кожныя 5-10 хвілін з патрабаваннем даслаць фатаграфіі людзей, якія з вамі побач, і месцаў, дзе вы знаходзіцеся. Партнёр дзеліцца з вамі інтымнымі фатаграфіямі ці відэа, нават калі вы пра гэта не прасілі, і чакае падобнае ў адказ. Партнёр пагражае падзяліцца вашымі інтымнымі фота з грамадскасцю дзеля аднаўлення адносін ці з мэтай вымагання грошай. Партнёр размясціў у інтэрнэце вашыя адкрытыя фота, каб абразіць або прынізіць вас. Як пазбегнуць лічбавага гвалту:

1. Дамовіцеся з партнёрам аб межах дазволенага

Павага асабістых меж – гэта паказчык здаровых адносін. Камусьці дастаткова аднаго смс або званка за цэлы дзень, а камусьці трэба перапісвацца нашмат часцей. Гэта трэба абмеркаваць з партнёрам.

2. Памятайце, што вы самі вырашаеце, што вам рабіць

Нават калі партнёр настойвае, а вам не хочацца, вы маеце права гэтага не рабіць. Гэта датычыцца любых дзеянняў. Вы адстойваеце свае асабістыя межы, за гэта не можа быць сорамна ці няёмка. Вам мусіць быць бяспечна.

3. Не забывайце аб тым, што выдаліць нешта з прасторaў інтэрнэту амаль немагчыма

Асабліва гэта датычыцца адкрытых фота і відэа. Дзелячыся такімі медыяфайламі з кімсьці, пераканайцеся ў тым, што гэта бяспечна для вас. У адваротным выпадку гэта можа стаць падставай для шантажу ці помсты былога партнёра.

4. Захоўвайце канфідэнцыяльнасць

Паролі павінны быць надзейнымі. Некаторыя прыкладанні зараз працуюць з двухфактарнай аўтэнтыфікацыяй. Смартфоны можна разблакаваць не толькі з дапамогай лічбавага кода, але і выкарыстоўваючы адбітак пальца або функцыю распазнання асобы. Калі на тэлефоне ёсць прыкладанні для адсочвання геапазіцыі, то іх лепш выдаліць.

Што рабіць, калі вы сутыкнуліся з лічбавым гвалтам

• Ізноў пагаварыце з партнёрам аб асабістых межах.

• Будзьце акуратныя з інфармацыяй, якую падаеце партнёру (фота, відэа, аўдыё-файлы).

• Запісвайце размовы з партнёрам, рабіце здымкі экрана падчас перапіскі, калі на ваш адрас ідуць абразы, знявагі ці пагрозы.

• Падзяліцеся сваімі перажываннямі з кім-небудзь: сваякі, сябры, псіхолагі, цэнтры падтрымкі.

• Завядзіце новы рахунак у сацыяльных сетках, зменіце электронную пошту.

• Прыбярыце галачку з пазіцыі «Паказваць маё месцазнаходжанне» ў настройках тэлефона.

• Папытаеце сяброў не выкладваць медыя файлы з вашай прысутнасцю.

Лічбавае насілле вельмі моцна падрывае псіхічнае здароўе. Людзі перастаюць давяраць, баяцца новых адносін, замыкаюцца ў сабе.

З лічбавым гвалтам можна сутыкнуцца ў дэйтынгавых дадатках. Акцёрамі такога гвалту могуць быць незнаёмцы ці ж знаёмыя і нават блізкія людзі: сваякі ці партнёры. Нават калі вы давяраеце свайму партнёру ці ведаеце, што ён неадкладна выдаліць гэтыя матэрыялы, адпраўляць інтымныя фота ўсё роўна небяспечна, таму што дадзеныя аб іх могуць застацца ў інтэрнэце.

Для гаджэтаў і сацыяльных сетак выбірайце надзейны пароль, двухфактарную ідэнтыфікацыю, разблакоўку прылад і прыкладанняў па адбітку або Face ID. Праверце, ці не стаіць на вашых прыладах шпіёнскіх праграм, якія адсочваюць геолокацию. Прыкметамі наяўнасці сталкерскага ПА могуць быць рэзкае пагаршэнне прадукцыйнасці, змена налад без вашага ведама, з'яўленне незнаёмых прыкладанняў, збоі ў праграмах, якія раней працавалі звычайна.

Паспрабуйце спачатку растлумачыць сітуацыю ў дыялогу, калі гэта магчыма і бяспечна. Бывае так, што адбываецца непаразуменне. Напрыклад, чалавек лічыць, што кожную гадзіну тэлефанаваць свайму партнёру і цікавіцца яго справамі – правільна. Ён можа не падазраваць, што для другога чалавека ў пары гэта выглядае як спробы кантролю ці ціск.

Калі стане зразумела, што партнёр лічыць тое, што адбываецца, нормай і імкнецца такім чынам усталяваць свой кантроль у адносінах: Асцярожна звяртайцеся з інфармацыяй, якой хочаце падзяліцца, будзь гэта тэкст, галасавое паведамленне, фота.

Шукайце дапамогу ў сваякоў, сяброў, спецыялістаў па хатнім гвалце. Важна дзяліцца тым, што адбываецца, нават калі ў вас няма магчымасці пайсці. Звернецеся да псіхолага, ён дапаможа скласці план бяспекі. Можна

пракансультавацца з юрыстам: калі дзеянні акцёра гвалту трапляюць пад нейкі артыкул Крымінальнага кодэкса, ён дапаможа вам падрыхтаваць дакументы для суда.

Рабіце запісы тэлефонных размоў, скрыншоты перапісак, у якіх вас абражаюць, шантажуюць, вам пагражаюць. Па магчымасці стварыце новыя аккаўнты пошты, сацсетак, месэнджараў з прылады, доступ да якога ёсць толькі ў вас. Выкарыстоўвайце браўзэр у рэжыме "інкогніта", пры якім не будзе захоўвацца гісторыя пошуку.

Праверце настройкі тэлефона. Паказ месцазнаходжання лепш выключыць наогул ці пакінуць толькі пры выкарыстанні канкрэтнага дадатку. Варта перыядычна змяняць паролі і PIN-коды для прыкладанняў і аккаўнтаў. Яны будуць розныя. Усталюйце двухфактарную аўтэнтыфікацыю, дзе гэта магчыма, і ў наладах прыватнасці на тэлефоне праверце, якім прыкладанням вы дазволілі захоўваць інфармацыю аб месцы і часе здымкі.

Папрасіце блізкіх людзей не дзяліцца інфармацыяй пра вас у сацыяльных сетках. Няхай яны не публікуюць фатаграфіі з вамі і не адзначаюць месцы, у якіх разам з вамі бывалі. Калі адносіны скончыліся, гвалт спыніўся. Паназірайце за сваім ментальным здароўем. Нейкія наступствы ўзнікаюць адразу, нейкія, напрыклад сімптомы ПТСР, могуць узнікаць на працягу паўгода.

Калі вы назіраеце змены свайго псіхаэмацыйнага стану, паспрабуйце звярнуцца за дапамогай да псіхолага. Калі ўзнікла падазрэнне аб сачэнні, то вам можа спатрэбіцца спецыяліст па лічбавай бяспецы. Варта насцярожыцца, калі ваш партнёр або былы партнёр аб'яўляецца ў тым месцы і ў той час, пра якія ён ніяк не мог даведацца. Ці ён як быццам выпадкова вымаўляе словы з вашага дыялогу з іншымі людзьмі, няўзнак пытаецца пра месца, якое вы абмяркоўвалі са сваім суразмоўцам.

Часам акцёры гвалту могуць проста дасылаць скрыншоты вашага месцазнаходжання ці перапісак з іншымі людзьмі, маніпулюючы тым, што ўсё пра вас ведаюць. Можна праверыць машыну ў аўтамайстэрні на

наяўнасць якія адсочваюць прылад, а гаджэты аднесці кампутарнаму майстру.

Ідэнтыфікуйце свае пачуцці і думкі аб тым, што адбылося. Памятайце, што ўсе вашыя рэакцыі – гэта нармальныя рэакцыі на ненармальныя акалічнасці. Нагадвайце сабе аб сваіх моцных баках і дасягненнях, якія застаюцца нязменнымі нягледзячы на той гвалт, які з вамі адбыўся.

Практыкуйце клопат пра сябе: старайцеся высыпацца, добра харчавацца, уключаць у свой штодзённы распарадак актыўнасць, якая вам падабаецца: ёгу, бег, медытацыі, праслухоўванне музыкі, маляванне.

Пазбягайце самаабвінавачванняў. Лепш укласці энергію ў тое, што вы можаце кантраляваць у сваім жыцці. Магчыма, дапаможа пераасэнсаванне досведу і навучанне навыкам усталявання асабістых меж. Будзьце да сябе добрыя, усведамляйце свае думкі і пачуцці, вучыцеся прымаць свае недасканаласці без асуджэння. Пазбягайце злоўжыванні псіхаактыўных рэчываў і ўсяго, што можа прычыніць вам фізічную або эмацыйную шкоду. Не саромейцеся звяртацца па прафесійную дапамогу.

Шукайце падтрымку там, дзе вас пачуюць, зразумеюць і прымуць. Лічбавае насілле можа пакінуць такі ж траўматычны след, як і больш відавочны гвалт у выглядзе абраз, пагроз, збіцця, тлумачыць Парсаданян. Але ў некаторых выпадках, па словах эксперткі, яно здольна паўплываць нават мацней, бо лічбавы гвалт можна здзейсніць ананімна, у любы час і ў любым месцы. Праз гэта пацярпелы бок можа не разумець сувязі паміж дзеяннямі крыўдзіцеля і зменамі свайго псіхалагічнага стану.

Лічбавае насілле можа працягвацца, нават калі актор гвалту ўжо не робіць ніякіх дзеянняў. Інтэрнэт памятае ўсё, таму, калі чалавек толькі адзін раз выклаў інтымныя здымкі пацярпелай у сетку і больш нічога не рабіў, распаўсюджвацца ў сетцы гэтыя кадры могуць яшчэ вельмі доўга.

Наступствы ад лічбавага гвалту дэманструюць высокі ўзровень трывогі. Гэта можа быць дэпрэсія, панічныя напады, праблемы з канцэнтрацыяй увагі, зніжэнне самаацэнкі і якасці жыцця ў цэлым. Можа

мець месца фарміраванне негатыўнага погляду на будучыню, адсутнасць даверу, спробы самаізалявацца ад зносін з іншымі людзьмі, адчуванне немагчымасці ўзяць жыццё назад пад кантроль; злоўжыванне псіхаактыўнымі рэчывамі.

Юрыдычна абараніцца ад лічбавага гвалту цяжка. З'яўляецца ўсё больш лічбавых інструментаў і спосабаў для кантролю, уплыву і запалохвання ў анлайн-асяроддзі, а заканадаўства мяняецца павольна.

Так, у 2009 годзе Філіпіны сталі адной з першых краін, дзе ўвялі крымінальную адказнасць за такія дзеянні: чалавек за публікацыю чужых інтымных матэрыялаў можа сесці ў турму на тры гады. У Англіі і Уэльсе «парнамесца» стала злачынствам у красавіку 2015 года, за яе можна атрымліваць турэмнае зняволенне тэрмінам да двух гадоў. А ў Ізраілі ў 2014 годзе абнародаванне інтымных фатаграфій без згоды тых, хто на іх намаляваны, прызналі сэксуалізаваным злачынствам. Яно караецца турэмным зняволеннем тэрмінам да 5 год. 40% карыстальнікаў інтэрнэту хаця б раз пацярпелі ад лічбавага аб'юзу, а 73% станавіліся яго сведкамі.

У той час як мужчыны часцей перажываюць абразы ў сетцы, жанчыны больш схільныя да сэксуалізаваных дамаганняў і анлайн-сталкінгу. Самая ўразлівая група - маладыя жанчыны ад 18 да 24 гадоў, на іх прыпадае каля 70% выпадкаў харассмента ў інтэрнэце. 54% жанчын, якія паведамлялі аб тым, што яны падвергліся лічбаваму гвалту, былі знаёмыя з крыўдзіцелем.

Лічбавае насілле можа суправаджаць партнёрскія адносіны і суіснаваць паралельна з іншымі відамі гвалту. Жанчыны ў спробе ахаваць сябе ад анлайн-харасмента, кібербулінгу і іншых праяў лічбавага гвалту пазбаўляюць сябе паўнавартаснага доступу да інфармацыі, працы, адукацыі, клопату аб здароўі і зносінах. Пагрозы, абразы ў адрас дзяржаўных служачых, членаў выбарчых камісій у сувязі з ажыццяўленнем імі службовых і службовых абавязкаў, а таксама ў адрас іх сем'яў, якія размяшчаюцца ў інтэрнэце, падпадаюць пад крымінальную адказнасць.

Паводле ч.1 арт. 366 КК Рэспублікі Беларусь пагроза гвалтам, знішчэннем або пашкоджаннем маёмасці ў дачыненні да службовай асобы, якая выконвае службовыя абавязкі, або іншай асобы, якая выконвае грамадскі абавязак па ахове грамадскага парадку або спыненні правапарушэнняў, або іх блізкіх у мэтах перашкоды законнай дзейнасці або прымусу да змянення характару гэтай дзейнасці, або з помсты за выкананне службовых абавязкаў або грамадскага абавязку караюцца штрафам, або папраўчымі работамі на тэрмін да двух гадоў, або арыштам, або абмежаваннем волі на тэрмін да пяці гадоў, або пазбаўленнем волі на тэрмін да пяці гадоў.

Крымінальна-караным дзеяннем таксама з'яўляецца прымус асобы да выканання або невыканання якога-небудзь дзеяння, здзейсненае пад пагрозай прымянення гвалту да яго або яго блізкім, знішчэння або пашкоджання іх маёмасці, распаўсюджвання паклёпніцкіх або абвяшчэння іншых звестак, якія яны жадаюць захаваць у таямніцы, або пад пагрозай ушчамлення правоў, свабод і законных інтарэсаў гэтых асоб, пры адсутнасці прыкмет больш цяжкага злачынства. Санкцыя артыкула 185 КК Рэспублікі Беларусь прадугледжвае максімальнае пакаранне да 2 год абмежавання волі. За размешчаныя ў «глабальным павуцінні» паклёп і абразы артыкула 188, 189 КК Рэспублікі Беларусь прадугледжваюць пакаранне аж да 3 гадоў абмежавання волі. Для звароту ў міліцыю юрысты раяць максімальна дакументаваць гвалт, які перажываецца: рабіць скрыншоты, запісы экрана, захоўваць выявы, аўдыё з пагрозамі і іншыя матэрыялы, якія дапамогуць даказаць віну акцёра гвалту. Forbes Woman расказвае пра паняцці, якія апісваюць спосабы ажыццяўлення лічбавага гвалту.

Формы лічбавага гвалту

Апскертынг (Upskirting): здымка інтымных частак цела незнаёмай жанчыны ці партнёркі без згоды. Апскертынг адбываецца не ў віртуальнай

прасторы, але з дапамогай тэлефона ці любой іншай камеры. Вядомы выпадак, калі мужчына, каб застацца незаўважаным, замацаваў мініяцюрную камеру на чаравіку. Адна з апошніх гучных спраў аб апкертынгу – арышт былога супрацоўніка парку забаў Disney World, які за шэсць гадоў працы ў парку зрабіў больш за 500 здымкаў і відэа жанчын "пад спадніцай".

У Расіі апкертынг не прызнаны правапарушэннем і не цягне за сабой адказнасці, хаця многія краіны паступова ўводзяць пакаранне за здымку аж да рэальнага тэрміну.

Доксінг (Doxing): публікацыя ў сетцы канфідэнцыйнай асабістай інфармацыі – хатняга адрасу, адрасы электроннай пошты, нумары тэлефона, дакументаў – з мэтай пераследу, запалохвання або вымагальніцтва. У 2014 годзе амерыканская распрацоўніца відэагульняў Зоуі Куін стала ахвярай доксінгу. Хлопец, з якім яна расталася, апублікаваў у сваім блогу запіс, у якім абвінаваціў Куін у тым, што яна змяніла яму з журналістам, каб атрымаць у прэсе дадатныя водгукі аб яе працы.

З гэтага пачалася цэлая кампанія па анлайн-доксінгу распрацоўшчыц: ім паступалі пагрозы расправы, згвалтаванняў і нават забойства – гэты скандал назвалі «Геймергейт». «Хакеры не проста рассылалі мне заклікі памерці або казалі пра тое, якая я тоўстая шлюха, яны дзяліліся маёй асабістай інфармацыяй: маім старым адрасам у Канадзе, нумарамі старых мабільных тэлефонаў, маім бягучым нумарам мабільнага тэлефона і маім бягучым хатнім адрасам», – распавядала Куін аб перажытым.

Зумбамбінг (Zoom-bombing): захоп відэаканферэнцыі і перапыненне зносін шляхам запуску відэа (часта парнаграфіі), аўдыё або трансляцыі ўласнага экрана. Сітуацыя з лічбавым гвалтам пагоршылася на фоне пандэміі каранавіруса ў 2020 годзе, калі людзі сталі праводзіць больш часу анлайн, маючы зносіны і працуючы. У той жа час былі зафіксаваны першыя выпадкі зумбамбінга на фоне набыцця папулярнасці платформай Zoom.

Кібersталкінг (Cyberstalking): працяглыя абразлівыя паводзіны ў адносінах да карыстача інтэрнэту, дакучлівая адпраўка паведамленняў, фота і

відэа, у тым ліку пагроз, з мэтай запалохаць яго. Анлайн-пераслед можа працягвацца гадамі. Бывае, што кібersталкер пераследуе ахвяру ў рэальным жыцці: напрыклад, усталяваўшы GPS-трэкер або проста высочваючы чалавека па сацсетках, геатэгам і фатаграфіям. Каля 26% маладых жанчын ва ўзросце 18-24 гадоў перажылі анлайн-сталкінг.

Кібербулінг (Cyberbullying): цкаванне з дапамогай лічбавых тэхналогій. Да яе адносяцца, напрыклад, абразлівыя паведамленні, няхай гэта будзе асабістая перапіска, каментар пад фатаграфіяй або ўзаемадзеянне на форуме.

Таксама кібербулінг можа выяўляцца праз пагрозы – калі чалавек заяўляе аб намеры прычыніць цялесныя пашкоджанні або нават забіць іншага. Жанчын часта запалохваюць пагрозамі ўчынення сэксуалізаванага гвалту, у тым ліку згвалтавання.

Анлайн-трафіку (Online trafficking): гандаль людзьмі з дапамогай інтэрнэту, пераважна сацсетак. Інтэрнэт стаў зручным інструментам для гандляроў людзьмі па ўсім свеце, 72 працэнты ахвяр якіх складаюць жанчыны і дзяўчынкі. Пры гэтым 77% выяўленых сярод ахвяр трафікінга жанчын былі прададзены ў сэксуальнае рабства. З-за пандэміі каранавіруса і закрыцця межаў гандляры людзьмі сталі больш актыўна анлайн і ўсё часцей шукаюць ахвяр для сэксуальнай эксплуатацыі ў інтэрнэце, у тым ліку з дапамогай вэбкама і анлайн-парнаграфіі.

Адным з найболей пераважных спосабаў пошуку ахвяр анлайн-трафікінгу стала размяшчэнне падробленых прапаноў аб працы, якія абяцаюць магчымасці працаўладкавання, часта ў падаленых краінах. Распаўсюджванню такой вярбоўкі спрыяе таргетынг. Ананімнасць і хуткасць перадачы інфармацыі анлайн дазваляюць злачынцам неўзаметку і хутка арганізоўваць транспарціроўку і размяшчэнне ахвяр, а таксама хаваць даходы ад сваіх злачынстваў.

Порнамесца (Revenge porn): публікацыя інтымных відэа ці фатаграфій з мэтай помсты, звычайна былым партнёрам ці мужам. Порнамесца можа быць заснавана на дыпфейцы: з дапамогай штучнага інтэлекту можна стварыць

малюнак, аўдыё або відэа, якое будзе праўдападобна імітаваць знешнасць або голас чалавека. Свотынг (Swatting): гэта ілжывы выклік на хату ахвяры спецпрызна, атрада паліцыі ў поўным узбраенні пад маркай таго, што ёй пагражае сур'ёзная небяспека. Да сватынгу можа звярнуцца кіберсталкер. Слова паходзіць ад SWAT – назвы падраздзялення амерыканскіх праваахоўных органаў.

Секстынг (Sexting): абмен інтымнымі паведамленнямі і фатаграфіямі - гэта не толькі прыемная ролевая гульня, але і вялікая рызыка. Секстынг можа таць сэксуалізаваным гвалтам у выпадку, калі партнёр выпрошвае фота супраць волі жанчыны. Чалавек, які атрымаў аголеныя здымкі, можа апублікаваць іх, выкарыстоўваць для шантажу ці для помсты пасля растання ці сваркі. Секстаршэн (Sextortion): шантаж з дапамогай інтымных фатаграфій і відэа, якія аўтар гвалту пагражае размясціць у сацсетках, адправіць калегам, сваякам ці сябрам ахвяры, калі яна не пагодзіцца на яго ўмовы. Таксама аўтар гвалту можа дасылаць ахвяры няпрошаныя аголеныя фота і відэа, пісаць ёй паведамленні з сэксуалізаваным падтэкстам ці прамым пасланнем сэксуальнага характару.

Сярод відаў лічбавага гвалту найбольш часта сустракаюцца:

− анлайн-пераследу – адпраўка непажаданых электронных лістоў, аўдыё/відэа ці тэкставых паведамленняў, дакучлівыя званкі, адсочванне месцазнаходжання;

− анлайн-дамаганні – шырэйшая катэгорыя пагроз ці іншых абразлівых паводзін, накіраваная на зневажэнне, прыніжэнне, абраза асобы ў публічнай анлайн-прасторы і асабістых паведамленнях;

− кібербулінг – сумяшчае ў сабе аспекты анлайн-пераследаў і анлайн-дамаганняў, часцей за ўсё сустракаецца сярод падлеткаў і здзяйсняецца групай асоб;

− крыпшот (англ. creepshot, гэта значыць «брыдкі здымак») і апкертынг (англ. upskirting, літаральна перакладаецца як «пад спадніцай») –

стварэнне фота/відэа інтымных частак цела партнёркі або незнаёмых жанчын (спіны, ягадзіц, ног, дэкальтэ) без іх згоды;

− кібергрумінг – размяшчэнне да сябе дзіцяці / падлетка дарослым чалавекам з мэтай ўстанаўлення даверу для далейшых сэксуальных адносін;

− узлом кампутара ці іншых тэхнічных прылад без згоды ўладальніка – звычайна ўзлом вэб-камеры, што часцей за ўсё негатыўна адбіваецца на жанчынах;

− сэксуалізаваны гвалт на аснове фота/відэа выяў – стварэнне, перадача, распаўсюджванне гэтых матэрыялаў без згоды пацярпелай. Важна ўлічваць, што яна магла даваць згоду на здымку фота/відэа кантэнту. Часта прыводзіць да самаабвінавачання, калі выявы былі распаўсюджаныя без згоды;

− паклёп – наўмыснае прычыненне шкоды рэпутацыі праз зацвярджэнне ілжывых заяў (напрыклад, распаўсюджванне чутак у сацсетках);

− слатшэймінг – анлайн-крытыка людзей, звычайна жанчын і дзяўчынак, якія парушаюць чаканні ў стаўленні паводзін і вонкавага выгляду, злучанага з іх сэксуальнасцю;

− анлайн-трафіку – гандаль людзьмі, асабліва жанчынамі, з дапамогай тэхналогій і сацыяльных сетак, часта якая прыводзіць да прастытуцыі.

Самы высокі ўзровень урону наносіцца ментальнаму здароўю. У жанчыны могуць з'явіцца трывога, дэпрэсія, панічныя напады, праблемы з канцэнтрацыяй увагі, зніжэнне самаацэнкі і якасці жыцця ў цэлым.

У выпадках лічбавага сэксуалізаванага гвалту, напрыклад, вырабу і распаўсюджвання інтымных фота/відэа без дазволу пацярпелай, наступствы могуць быць яшчэ больш сур'ёзнымі: дэпрэсія, якая можа прывесці да злоўжывання псіхаактыўных рэчываў, сімптомаў ПТСР.

Пацярпелая можа ізаляваца ад зносін з іншымі людзьмі, у тым ліку анлайн, выпрабоўваючы пачуцці віны і сораму, адчуваць адзіноту і думаць, што ёй ніхто не паверыць. Ёсць таксама верагоднасць, што лічбавы гвалт

перарасце ў гвалт у афлайн, напрыклад, у выпадках анлайн-сталкінгу ці пагроз прычынення шкоды жыццю і здароўю.

Фактары, якія дапамагаюць хутчэй аднавіцца пасля гвалтоўнага ўздзеяння, – гэта магчымасць падзяліцца перажытым з блізкімі і бяспечнымі людзьмі, наведаць тэматычныя групы падтрымкі, атрымаць псіхалагічную і пры неабходнасці юрыдычную дапамогу ад спецыяліста.

Калі пра вас распаўсюджваюць загадзя ілжывыя звесткі, якія ганьбяць ваш гонар і годнасць або падрываюць вашу рэпутацыю, за гэта прадугледжана крымінальная адказнасць. Загадзя ілжывымі прызнаюцца такія звесткі, якія не адпавядаюць рэчаіснасці, сцвярджаюць аб фактах (гэта значыць гэта павінна быць не ацэначнае меркаванне або меркаванне чалавека) або падзеях, якія не мелі месца ў рэальнасці, напрыклад, аб здзяйсненні злачынства або наяўнасці захворвання.

Заведамасць – гэта абавязковая прыкмета, які мяркуе, што асоба дакладна ведала аб ілжывасці паведамляных ім звестак.

Калі агрэсар распаўсюджвае (напрыклад, перадае скрыншоты, у тым ліку ў надрукаваным выглядзе, рассылае па электроннай пошце, у сацыяльных сетках або месэнджарах, публікуе на розных сайтах) вашых інтымныя фатаграфіі, відэа ці іншую інфармацыю, якая складае вашу асабістую ці сямейную таямніцу, яго дзеянні трапляюць пад гэты артыкул.

Пад гэты склад таксама можа трапляць незаконнае збіранне звестак аб вашым прыватным жыцці, якія складаюць асабістую ці сямейную таямніцу, без вашай згоды. Пад незаконным збіраннем можа разумецца, напрыклад, выкраданне ці незаконнае набыццё звестак. Парады раяць асцярожна звяртацца з інфармацыяй, якой вы хочаце падзяліцца:

- тэкстам, галасавым паведамленнем, фота;
- шукаць дапамогі ў сваякоў, сяброў і спецыялістаў па хатнім гвалце.

Важна дзяліцца тым, што адбываецца. Зварот да псіхолага дапаможа скласці план бяспекі, кансультацыя юрыста – падрыхтаваць дакументы для падачы ў

суд, калі дзеянні крыўдзіцеля нясуць у сабе склад правапарушэння або злачынства;

− рабіць запісы тэлефонных размоў, скрыншоты перапісак, у якіх змяшчаюцца або могуць змяшчацца пагрозы, абразы, шантаж;

− стварыць новыя аккаўнты пошты, сацсетак, месэнджараў з прылады, доступ да якой ёсць толькі ў вас;

− выкарыстоўваць браўзэр у рэжыме «інкогніта», каб не захоўваць гісторыю пошуку;

− праверыць настройкі тэлефона: месцазнаходжанне і канфідэнцыяльнасць. Налады месцазнаходжання лепш выключыць наогул ці пакінуць толькі пры выкарыстанні пэўных прыкладанняў. У наладах канфідэнцыйнасці ўдакладніце, якім дадаткам вы дазволілі захоўваць інфармацыю аб месцы і часе здымкі;

− мяняць свае паролі і PIN-коды, зрабіць іх рознымі для розных прыкладанняў і аккаўнтаў. Наладзьце двух фактарную аўтэнтыфікацыю, дзе гэта магчыма;

− праверыць, хто можа адзначаць вас на фатаграфіях і відэа;

− папрасіць блізкіх людзей не дзяліцца анлайн інфармацыяй пра вас дзеля вашай бяспекі. Пры неабходнасці пра гэта можна папрасіць калег і аднакурснікаў.

Каля 55% карыстальнікаў дэйтынгавых прыкладанняў сутыкаліся з рознымі відамі праблем парушэння бяспекі. Ашуканцаў у дейтинговых прыкладаннях можна вызначыць па мадэлі паводзін. Часцяком яны правакуюць на адкрытыя размовы і спрабуюць занадта хутка перавесці зносіны на іншыя платформы.

Распрацоўнікі прыкладанняў імкнуцца выбудаваць абарону для сваіх карыстальнікаў. Калі алгарытм бачыць, што перапіска патэнцыйна можа стаць небяспечнай, ён адпраўляе папераджальнае апавяшчэнне з рэкамендацыямі аб тым, як засцерагчы сябе.

Дэйтынгавыя прыкладанні становяцца падобныя на сацыяльныя сеткі. Стваральнікі прыкладанняў імкнуцца да гейміфікацыі сэрвісаў. У будучыні папулярным спосабам зносін стане камунікацыя ў пакоях дапоўненай рэальнасці. Людзі змогуць мяняць аватары і пакоі па настроі.

Лічбавыя наркотыкі

Лічбавыя наркотыкі – гэта аўдыётрэкі з пэўным наборам гукаў. Коратка "лічба". Дадзеныя аўдыётрэкі завуць "наркотыкамі" з-за эфекту, параўнальнага з уздзеяннем сапраўдных псіхатропных сродкаў на арганізм. Для таго каб "злавіць кайф" зараз зусім неабавязкова нешта паліць ці нюхаць, сцвярджаюць іх вытворцы. Досыць мець ПК, стэрэаслухаўкі і адмысловую праграму для прайгравання гэтых аўдыёфайлаў.

"Лічба" аказвае ўплыў на мозг чалавека дзякуючы бінауральным рытмам. Дакладней, уздзеянне адбываецца, калі ў кожным вуху раздаюцца гукі рознай частаты, ствараючы пэўную камбінацыю ў мозгу.

Частата гуку, супадаючы з частатой мазгавых хваль, можа выклікаць у чалавеку пэўныя эмоцыі: эйфарыю, трывогу, спакой, прыліў энергіі. І пры праслухоўванні пэўных гукаў абодва паўшар'і мозгу пачынаюць працаваць сінхронна, што і выклікае ў чалавека адчуванні, параўнальныя з прыёмам наркатычных прэпаратаў.

Ваганні мозгу выяўляюцца ў бінауральных біццях. Лічыцца, што апошнія аказваюць станоўчы ўплыў на псіхафізіялагічныя стан чалавека.

Не гледзячы на сумнеўны ў сваёй карыснасці эфект, лічыцца, што лічбавыя дозы прывыкання не выклікаюць. А таму не варта баяцца і наступстваў, напрыклад, ломкі. "Вытворцы" наркоты запэўніваюць спажыўцоў і ў тым, што чым часцей чалавек будзе праслухоўваць дозу, тым карацей становіцца перыяд для атрымання эфекту.

Ідэя "лічбы" належыць амерыканскаму праекту I-Doser Labs, буйному вытворцу аўдыяпраграм, якія могуць кантраляваць актыўнасць мозгу.

Распрацоўнікі называюць сябе стваральнікамі сэрвісу, які з'яўляецца легальнай альтэрнатывай псіхатропным рэчывам.

У Інтэрнэце можна знайсці даволі вялікі спіс трэкаў. Часцей за ўсё іх назва гаворыць сама за сябе: гераін, марыхуана, антымігрэнь і іншыя. Іх "вытворцы" сцвярджаюць, што гукі аказваюць уплыў, адпаведнае іх назве і апісанні, якое суправаджаецца парушэннем каардынацыі і галюцынацыямі. Па гэтых прычынах іх праслухоўванне забаронена, напрыклад, пры ваджэнні аўтамабіля, бо, відавочна, небяспечна.

Зрэшты, можа быць другі варыянт: "лічбавая наркота" сапраўды ніякай небяспекі не ўяўляе, але толькі ў сувязі з тым, што не аказвае эфекту. І сапраўды, многія сцвярджаюць, што ні падчас, ні пасля праслухоўвання нічога не адчулі. Таксама ёсць і трэцяя катэгорыя, на якіх "лічба" эфект аказала, але не той, што чакаўся. Гэта могуць быць проста лёгкае галавакружэнне ці галаўны боль.

Спрэчкі вакол бяспекі ці шкоды лічбавых наркотыкаў яшчэ доўга не сціхнуць. З аднаго боку, бінауральный эфект даўно прымяняецца ў некалькіх абласцях (для паляпшэння памяці, лячэння хвароб, паслаблення, вызначэння пашкоджаных абласцей мозгу). З іншага боку, ці адэкватна яны ўспрымаюцца ахвотнікамі іх праслухаць? Асцярога, у асноўным, выклікае доступ да аўдыёзапісаў непаўналетніх. Бо любы школьнік можа спампаваць і ўсталяваць I-Doser для праслухоўвання «доз» ці спампаваць mp3-пакі, прыдатныя для любога mp3-прайгравальніка. Калі ўсёткі які-небудзь малалетка прасякнецца і зловіць кайф - ці не пацягне яго на сапраўдную наркату? "Лічбу" і рэальнасць можа падзяляць усяго адзін крок.

Маюцца таксама супрацьпаказанні для людзей з парушанай псіхікай і псіхічнымі захворваннямі. Праслухоўванне можа справакаваць абвастрэнне і далейшае развіццё працэсу. Спецыялісты, якія даследуюць "наркатычныя" гукі, забараняюць эксперыментаваць з гэтымі эфектамі дзецям, падлеткам і хворым людзям. Але справа ў тым, што чалавек, які хварэе на псіхічнае захворванне, не ўсведамляе таго, што ён хворы.

У нашым свеце занадта шмат фактараў, ад якіх мы залежым. Нашай свядомасці дастаткова перыядычна паўтаральных падзей, падмацаваных эмоцыямі. А эмацыйная «прывязка» – вельмі моцная прылада ўздзеяння на чалавека. Прывязаўшыся да «наркатычных» адчуванняў, няхай гэта будзе каханне, шчасце ці нават дэпрэсія, чалавек апускаецца ў свет перажыванняў, у якім яму па нейкім чынніку лепш, чым у рэальным. Па сутнасці гэта – самападман. І, як вядома, чым мацнейшае ў чалавека жаданне сысці ад рэальнасці, тым лягчэй на яго ўздзейнічаць.

Адзін са спосабаў уздзеяння – гэта залежнасць псіхікі ад кампутара. Ужо даўно вядома, што ў нашу прытомнасць можна даволі грубіянска без попыту ўціснуцца з дапамогай розных эфектаў: хутка мільготкіх каляровых плям, вызначанай музыкі, гульнявых сюжэтаў, спрыяльных выкіду адрэналіну ў кроў.

Цяпер новы спосаб – гукі. Пры гэтым ніхто нават не падумае адмовіцца ад свайго "захаплення", не прызнаючы сваёй залежнасці ад яго, таму што гэта выклікае ў нас пэўныя адчуванні, ад якіх няма бачных прычын адмаўляць.

Небяспека ў форме падману: інфацыгане

Інфацыгане – гэта прадпрымальнікі, якія прадаюць пераважна навучальныя анлайн-прадукты без нейкага вымеранага ККД. Яны не вучаць канкрэтным навыкам працаваць з персаналам або прыцягваць канкрэтную мэтавую аўдыторыю, а расказваюць аб важнасці ўпэўненасці ў сабе, мэтапакладання. Іх прадукт – гэта сумесь матывацыйных практык, псіхалагічных фішак і эзатэрычнага туману. Так, многія распавядаюць аб тым, як важна выкінуць старое і пайсці пакуль хаця б пакратаць новае – брэндавае і дарагое. Станоўчы эфект пасля такіх праграм, а ён часам бывае, ніяк не звязаны з іх зместам.

Інфацыгане пакажуць вам прыгожыя карцінкі, прывабяць яркай рэкламай, згуляюць на любові да статусных рэчаў і эксклюзіўнасці,

прагавораць соты раз вялікія ісціны аб тым, як важна верыць у сябе і фармуляваць блізкія і далёкія мэты.

Яны напампуюць матывацыяй, але не дадуць ніякіх практычных інструментаў, як гэтых мэт дасягнуць. Сацыяльныя сеткі сталі пажыўным асяроддзем. Тысячы людзей гатовы купляць што заўгодна з рук паспяховых і высокааплатных "спецыялістаў".

За карцінкай з майбахам або кадрамі з Балі не стаіць нічога, што б казала аб кампетэнцыі і рэальных дасягненнях аўтараў кантэнту. Прывабныя фота і відэа разам з гісторыямі пра шлях «гуру» з хрушчоўкі ў правінцыйным мястэчку да вяршыняў багацця, а таксама навык пераканання – гэта адзіны іх капітал. Мяркуючы па лічбах заробку самых папулярных «прадаўцоў паветра» і зараджальнікаў самых паспяховых будучых бізнэс-лідэраў – гэтага цалкам дастаткова.

Большасць інфацыган працуе па агульнай схеме: ствараюць асабістае трызненне, яго базавыя рысы – гэта прыгожае жыццё, дарагія рэчы і аўто, круізы, знешнія атрыбуты поспеху. І пачынаюць прадаваць свой "вопыт".

Анлайн-кавучы з нізкаякасным прадуктам добра ўлоўліваюць трэнды і зарабляюць на іх. Яны першымі запускаюць марафоны, платныя каналы, сеткавыя продажы нікому не вядомага які чысціць сродкі, якім можна паліваць кветкі. Краса навізны + яркая абгортка = поспех першых продажаў. А большага гэтым псеўдапрадпрымальнікам і не трэба – ім важны прыбытак тут і цяпер.

Ашуканцы лёгка прададуць рашэнне праблем, якія нельга вырашыць практычна. Калі чалавек страціў волю да жыцця, то нават прафесійны псіхолаг паспрабуе некалькі методык, каб вызначыць, што дапаможа вывесці чалавека са стану застою. Часам і матывацыйны фразы з календара трапляюць у кропку, але гэта не значыць, што трэнінг, складзены з такіх фраз, – якасны.

Навыкі пераканання, аратарскія прыёмы дазваляюць зрабіць першае ўражанне, стварыць адчуванне прафесіяналізму. Калі вы ідзяце на навучанне,

у вас ёсць канкрэтны запыт: навучыцца нечаму вызначанаму, асвоіць практычныя навыкі. Большасць людзей, якія звяртаюцца да псеўдакавучаў, не могуць сфармуляваць такі запыт. Партрэт мэтавай аўдыторыі інфамашэнцаў:

• людзі, якія стаміліся ад цяперашняй працы;

• жанчыны, якія выходзяць з водпуску па догляду за дзіцем;

• прадпрымальнікі, якія страцілі бізнэс;

• маладыя людзі без жыццёвага досведу.

Людзі ва ўразлівым стане, летуценнікі і наіўныя навічкі заўсёды былі лёгкай здабычай варажбітак, прадаўцоў неправераных лекаў для пахудання і іншых аферыстаў. Так што інфацыгане проста працягнулі справу Ката Базіліо на новым полі.

Лекцыі інфацыган – гэта адсутнасць канкрэтыкі і жаданне атрымаць хуткі прыбытак. Першае, што робяць перад запускам продажаў, – выграваюць аўдыторыю. Звычайна гэта прымітыўная дэманстрацыя поспеху аўтара кантэнту. Блогер дапамагае камусьці са сваіх падпісчыкаў здзейсніць мару: купляе яму смартфон або адпраўляе на адпачынак. Гісторыя поспеху, "як я стаў багатым": заўсёды сам, з дапамогай розуму і таленту гэты малады "мільянер" ("мільянерка") сабраў(-ла) стан на паспяховых праектах і гатовы(-а) дзяліцца вопытам з іншымі. Далей ідуць просьбы загадзя ўдзячных (па) чытачоў. "Спецыяліст" распавядзе, як цяжка змясціць у адзін паток усіх жадаючых, адкрые ліст чакання і прапануе зніжку для ста самых першых пакупнікоў. Самыя ўважлівыя коучы ведаюць, што апрацоўваюць безграшовую аўдыторыю, і прапануюць ім набыць цуд-праграму для заробку.

Паняцце крыніцы падвышанай небяспекі

Асаблівасцю крыніцы падвышанай небяспекі з'яўляецца нявызначанасць развіцця працэсу. У якасці прыкметы крыніцы павышанай небяспекі вылучаюць верагоднасць прычынення шкоды людзям.

Найважнейшай прыкметай некаторых крыніц падвышанай небяспекі з'яўляецца незваротнасць разбуральнага працэсу, які яны выклікаюць. Пасля таго як крыніца пачынае функцыянаваць, умяшацца ў ход падзей і змяніць развіццё гэтага працэсу ўжо нельга ці вельмі цяжка. Для прыкладу назавём ядзерную рэакцыю.

У залежнасці ад паходжання крыніца небяспекі можа быць: прыродны, антрапагенны або змяшаны – прыродна-антрапагенны. Да прыродных адносяцца: землятрусу, вывяржэння, ураганы, паводкі, маланкі, дзікія жывёлы (звяры, змеі), атрутныя расліны і мінеральныя яды. Значная і хутка якая расце доля крыніц небяспекі, мае антрапагеннае паходжанне. Гэта значыць з'яўляецца вытворным чалавека і яго дзейнасці. Нездарма старажытныя сцвярджалі, што чалавек сам сабе вораг.

У цывілістыцы праглядаюцца два падыходы да вызначэння крыніцы павышанай небяспекі, якія абазначаюцца тэрмінамі «тэорыя аб'екта» і «тэорыя дзейнасці». У адпаведнасці з першай з іх крыніцамі падвышанай небяспекі лічацца прадметы матэрыяльнага свету, якія валодаюць небяспечнымі для навакольных уласцівасцямі, якія не паддаюцца поўнаму кантролю са боку чалавека.

Крыніцай падвышанай небяспекі можа быць дзейнасць, ажыццяўленне якой дае падвышаную верагоднасць прычынення шкоды з-за немагчымасці поўнага кантролю за ёй з боку чалавека. Таксама дзейнасць па выкарыстанні, транспартаванні, захоўванні прадметаў, рэчываў і іншых аб'ектаў вытворчага, гаспадарчага ці іншага прызначэння, якія валодаюць такімі ж уласцівасцямі.

Крыніца падвышанай небяспекі – гэта ўласцівасць адной, часцей за ўсё няўстойлівай, сістэмы (рэчывы, механізму, з'явы, працэсу, арганізма, асобы, сацыяльнай групы), развіццё або праява якога слаба паддаецца ці не паддаецца кантролю і можа вырабіць незваротныя разбуральныя змены ў гэтай ці іншай сістэме. Гэтая крыніца валодае высокім паражальным эфектам. Пачаты разбуральны працэс слаба паддаецца ці зусім не паддаецца кантролю, і яго наступствы часта незваротныя.

У прынцыпе любая дзейнасць чалавека адначасова і карысная, і шкодная. Сфармуляваная аксіёма патэнцыйнай небяспекі дзейнасці чалавека, з якой вынікаюць дзве найважнейшыя высновы: 1) немагчыма распрацаваць абсалютна бяспечны від дзейнасці чалавека, 2) ні ў адным відзе дзейнасці чалавека не можа быць нулявых рызык.

Тым не менш, некаторыя віды дзейнасці аб'ектыўна ўяўляюць сабой вялікую ў параўнанні з іншымі небяспеку. Напрыклад, злачынная дзейнасць. Вылучаюць «крыніцу крымінальнай небяспекі», «крымінальную небяспеку», маючы на ўвазе небяспеку ад злачыннасці. Відавочнымі прыкметамі крыніцы падвышанай небяспекі валодае дзейнасць тэрарыстычных арганізацый.

Крыніцай небяспекі могуць быць таксама прадукты дзейнасці чалавека. У гэтую групу ўваходзіць большая частка наркатычных сродкаў, псіхатропных рэчываў, радыеактыўных матэрыялаў, зброя, небяспечныя вытворчыя аб'екты і небяспечныя грузы.

З'явіліся крыніцы, небяспека якіх грамадскай свядомасцю яшчэ не ўспрымаецца. Напрыклад, адной з наймагутных нявывучаных, а таму непрадказальных крыніц небяспекі становіцца электрамагнітнае забруджванне. З развіццём кампутарных тэхналогій расце іх грамадская значнасць, але, нажаль, і іх патэнцыйная небяспека. У сучасным інфармацыйным грамадстве крыніцамі падвышанай небяспекі могуць быць кампутарныя вірусныя эпідэміі.

Адмысловай увагі заслугоўваюць сацыяльныя крыніцы псіхалагічнай небяспекі. Крыніцай падвышанай небяспекі можа быць асоба, сацыяльная група ці іншы суб'ект дзейнасці і кіраванні. Бо любая дзейнасць мяркуе не толькі аб'ект, але і суб'ект.

З пазіцый тэорыі суб'екта асаблівымі крыніцамі небяспекі могуць выступаць пэўныя ўласцівасці асобы біялагічнага паходжання або сфармаваліся пад уплывам негатыўных сацыяльных фактараў. Да іх адносіцца грамадская небяспека, якая сфармавалася ў выніку псіхічнага

захворванне або выклікана адмоўнымі маральнымі і сацыяльнымі якасцямі, жорсткасцю, карысцю і іншымі індывідуалістычнымі ўстаноўкамі.

Крыніцай падвышанай небяспекі можа быць крымінагенная асоба, якая выяўляецца ў сукупнасці ўласцівасцяў і якасцяў суб'екта, якія паказваюць на схільнасць да здзяйснення злачынства і яго паўтарэння.

Псіхічныя ўласцівасці асобы могуць выступаць у якасці крыніцы небяспекі пры трансфармацыі псіхічнай энергіі ў энергію грамадска небяспечнага дзеяння, з дапамогай псіхічнага ўмяшання, напрыклад, гіпнатычнага, экстрасэнсавага характару.

Крыніцамі падвышанай небяспекі, з'яўляюцца злачынныя, тэрарыстычныя, экстрэмісцкія арганізацыі. Крыніцай падвышанай небяспекі могуць быць і суб'екты кіраўнічых, адміністрацыйна-ўладных адносін. У рэальнай адзнацы і ранжыраванні крыніц небяспекі немалую ролю гуляе суб'ектыўнае ўспрыманне.

Вельмі часта нашы ўяўленні пра гэта істотна скажоныя. У аўтакатастрофах гіне значна больш людзей, чым у авіякатастрофах ці ад рук забойцаў-маньякаў. Аднак расейскія абывацелі трымцяць ад жаху перад маньякамі, але ехаць з п'яным кіроўцам для іх, як паказвае практыка, – звычайная справа.

Другое паняцце, якое мае патрэбу ў такой жа пільнай увазе правазнаўцаў, – гэта аб'ект павышанай аховы. Нельга сказаць, што ў юрыдычнай навуцы яна зусім не выкарыстоўваецца. Маюцца заканадаўчыя акты аб асабліва ахоўных тэрыторыях, абароне камп'ютарных праграм, помнікаў культуры. Аднак статусу агульнаправавой і крыміналагічнай катэгорыі словазлучэнне "аб'ект павышанай аховы" яшчэ не мае.

У якасці аб'екта аховы можна разглядаць любую сістэму: асобу, сацыяльную групу, грамадства, чалавецтва; віды і прадукты дзейнасці чалавека; прыродныя аб'екты: фауну і флору, мінералы і тэрыторыі і да т.п. Аб'ектам аховы з'яўляюцца як самі матэрыяльныя субстанцыі (арганізм,

прадметы, участкі тэрыторыі), так і грамадскія адносіны або пэўная дзейнасць, якія склаліся з гэтай нагоды.

Значнасць і каштоўнасць аб'ектаў аховы не аднолькавая. У ходзе эвалюцыі складаюцца «ядзерныя» адносіны і галоўныя каштоўнасці, разбурыўшы і знішчыўшы якія, чалавецтва вырача сябе на згубу. Гэта – навакольнае асяроддзе, веды, мараль, права і іншыя каштоўнасці.

Да іх адносяцца людзі старэйшага пакалення як захавальнікі і праваднікі назапашанага чалавецтвам вопыту, а таксама дзеці як будучыня чалавечай цывілізацыі.

Аб'ектамі падвышанай аховы павінны быць найважныя ўласцівасці (адносіны) сістэмы, страціўшы якія, яна альбо разбурыцца, альбо трансфармуецца ў іншую і не зможа дасягнуць пастаўленай перад ёй мэты. Каб сістэма функцыянавала як якая развіваецца, неабходна абарона яе сутнасных элементаў.

У ходзе жыццядзейнасці выкрышталізавалася, што для бяспечнага функцыянавання асобы, грамадства і чалавецтва такімі аб'ектамі павышанай аховы з'яўляюцца жыццё, здароўе, свабода, гонар, годнасць, палавая недатыкальнасць, уласнасць і іншыя канстытуцыйныя правы і свабоды асобы; здароўе насельніцтва, грамадская бяспека і маральнасць; экалогія, канстытуцыйны лад і бяспека дзяржавы; мір і бяспека чалавецтва.

Па сутнасці, гэта тыя аб'екты, якія ў сілу сваёй асаблівай каштоўнасці падлягаюць крымінальна-прававой ахове. Дзеючае заканадаўства ў разрад такіх вылучае асабліва ахоўныя тэрыторыі і аб'екты, віды флоры і фауны, мінералы, палеанталагічныя аб'екты, службовую, камерцыйную, дзяржаўную таямніцу і закрытыя адміністрацыйна-тэрытарыяльныя ўтварэнні.

Адным з аб'ектаў павышанай аховы павінна быць культура, бо па-сапраўднаму бяспечным можа быць грамадства, абсалютная большасць чальцоў якога культурныя, свядома і мэтанакіравана выконвае агульнапрынятыя нормы жыццядзейнасці.

Канцэпцыя псіхалагічнай бяспекі павінна разглядаць псіхіку чалавека ў двух аспектах. Як аб'ект абароны і як крыніцу небяспекі. Абмежаванне дзеяздольнасці псіхічна хворага – адначасова сродак стрымання выходнай ад яго небяспекі і сродак аховы яго інтарэсаў.

Паняцце мер бяспекі

Для забеспячэння жыццядзейнасці грамадства здаўна і вельмі шырока выкарыстоўваюцца меры прымусу, якія па сваіх сутнасных характарыстыках не адносяцца да мераў юрыдычнай адказнасці (пакарання), – меры бяспекі. Выкарыстанне катэгорый "крыніца павышанай небяспекі" і "аб'ект павышанай аховы" тлумачыць сацыяльную абумоўленасць, неабходнасць і акрэслівае межы выкарыстання гэтай абмежавальна-прымусовай меры.

Ужо на світанку развіцця чалавецтва стала ясна, што пагроза прычынення шкоды арганізму чалавека, сістэмным прынцыпам арганізацыі супольнасці, чальцом якога ён з'яўляецца, павінна быць спынена цвёрда, адназначна. Варта адрозніваць меры бяспекі ў шырокім і ў вузкім сэнсе: меры забеспячэння бяспекі і меры бяспекі.

У шырокім сэнсе меры бяспекі – гэта ўвесь комплекс забеспячэння жыццядзейнасці сістэмы. Для нармальнага існавання чалавечага арганізма патрэбны здаровыя зубы, але страта аднаго з іх ці нават некалькіх да смяротнага зыходу не прывядзе, у той час як страта печані, сэрца ці іншых жыццёва важных органаў прывядзе да неадкладнай смерці.

У кожнай сістэме ёсць элементы першарадныя, якія вызначаюць яе сутнасць і своеасаблівасць, а ёсць другасныя, перыферыйныя. Крыніца ўяўляе падвышаную небяспеку для сістэмы менавіта таму, што пагражае сістэмаўтваральным элементам. Спецыялізаваныя меры для абароны гэтых сутнасных элементаў сістэмы і ёсць тое, што мы называем мерамі бяспекі.

Права як сацыяльны рэгулятар забяспечвае бяспеку сацыяльных сувязей праз усе свае інстытуты. Аднак спосабы забеспячэння розныя, і ў

рамках сродкаў, якія прадстаўляюцца правам, маюцца прававыя інстытуты, якія выконваюць асаблівую ролю – засцярога сістэмы ад разбурэння, выкліканага крыніцай падвышанай небяспекі.

У кантэксце доследнай праблемы ўвесь комплекс жыццезабеспячэння можна назваць мерамі забеспячэння бяспекі (мерамі бяспекі ў шырокім сэнсе), а спецыяльны прававы інстытут для прадухілення шкоднага ўплыву крыніц падвышанай небяспекі – мерамі бяспекі (мерамі бяспекі ў вузкім сэнсе). Апошнія спецыяльна створаны і накіраваны на абарону сістэмаўтваральных адносін аб'екта ад шкоднаснага ўздзеяння крыніцы павышанай небяспекі.

Меры бяспекі прымяняюцца спецыяльна для прадухілення шкоднаснага ўздзеяння пэўнай крыніцы павышанай небяспекі або агароджы аб'екта павышанай аховы ад шкоднага ўплыву любых крыніц небяспекі. Змест мер бяспекі складаюць спецыяльныя абавязкі і забароны, якія ўскладаюцца на фізічных асоб або сацыяльныя групы.

Яны ўзніклі як рэфлексы бяспекі. З развіццём не генетычных формаў памяці меры бяспекі замацоўваліся ў выглядзе табу, а затым – у выглядзе правіл, прадугледжаных у першай разнавіднасці сацыяльнай нормы, так званай мона норме. Падчас станаўлення цывілізацыі ахоўныя рэакцыі выкрышталізаваліся ў паводніцкія стэрэатыпы і правілы бяспекі, абавязковасць якіх падмацоўвалася санкцыямі.

Правілы бяспекі – гэта сукупнасць абавязкаў і забарон, якія суб'ект павінен выконваць, каб выключыць або звесці да мінімуму шкоду, якая прычыняецца крыніцай падвышанай небяспекі, або прадухіліць прычыненне шкоды аб'екту падвышанай аховы любой крыніцай небяспекі. Не ўсе правілы, якія рэгламентуюць жыццядзейнасць, можна назваць правіламі бяспекі. Да іх адносяцца толькі правілы абыходжання чалавека з крыніцай павышанай небяспекі і з аб'ектам павышанай аховы.

Паколькі ўлада з'яўляецца адначасова крыніцай падвышанай небяспекі і аб'ектам падвышанай аховы, то суцэль правамерна патрабаваць з

дзяржаўных службоўцаў захавання антыкарупцыйных правіл бяспекі. Па меры падзелу грамадскай працы вылучыліся два асноўныя тыпы санкцый: стымулявання (пазітыўныя) і абмежаванні (негатыўныя).

Апошнія ў сваю чаргу падзяляюцца на санкцыі аднаўлення (кампенсацыі), пакарання і бяспекі.

Санкцыі аднаўлення – гэта рэакцыя на парушэнне правіла (у тым ліку – правілы бяспекі), у выніку якога нанесены ўрон. Яны накіраваныя на «ліквідацыю шкоды, прычыненай супрацьпраўным дзеяннем грамадскім адносінам, на выкананне нявыкананых абавязкаў».

Яны ўключаюць: прымусовае выкананне абавязку, адмену незаконных актаў і абавязак пакрыць урон. Тым самым узнаўляецца сістэма праваадносін, парушаная не выкананнем прадпісанняў закона суб'ектамі.

Гэта група мер уласціва грамадзянска-прававой галіны. Але яны выкарыстоўваюцца і ў крымінальным праве, дзе аднаўленне ажыццяўляецца шляхам ўскоснага стымулявання або прамым ускладаннем абавязкі загладзіць прычыненую шкоду. Ідэя кампенсацыі ўрону, аднаўлення парушаных адносін, прымірэння ахвяры і злачынца ляжыць у аснове так званага аднаўленчага правасуддзя.

Санкцыі пакарання – гэта прымусовае пазбаўленне пэўных выгод суразмерна цяжкасці здзейсненага правапарушэння. Шляхам пагрозы або рэальнага прычынення пазбаўленняў і пакут правапарушальніку дасягаюцца мэты агульнага і спецыяльнага папярэджання. Разлік просты: сам пакараны, асцерагаючыся паўтарэння кары, будзе пазбягаць і паўторы злачынстваў, а для стрымлівання злачынных памкненняў большасці навакольных досыць досведу чужых пакут.

Пакаранне разглядаецца як адзін з найважнейшых сродкаў папярэджання злачыннасці. Механізм карнага ўздзеяння ў юрыдычнай літаратуры добра вывучаны. Гістарычна склалася так, што агульная тэорыя права і галіновыя юрыдычныя навукі маюць пакаральны акцэнт і з'яўляюцца па сутнасці тэорыямі адказнасці-пакарання, у той час як сацыяльна-

псіхалагічны механізм і эфектыўнасць іншых відаў прававога рэгулявання даследаваны недастаткова.

Прыкладамі санкцый у крымінальным праве з'яўляюцца прымусовыя меры медыцынскага характару, частка прымусовых мер выхаваўчага ўздзеяння, спецыяльныя абавязкі, якія ўскладаюцца на ўмоўна асуджанага або ўмоўна-датэрмінова вызваленага.

Абмежаванне можа ажыццяўляцца рознымі спосабамі: фізічным, механічным, арганізацыйным, псіхалагічным. У сувязі з асаблівасцямі заканадаўчай тэхнікі, а таксама ў сілу спецыялізацыі галін права, правілы і санкцыі бяспекі могуць размяшчацца не толькі ў розных артыкулах, раздзелах, раздзелах аднаго нарматыўна-прававога акта, але і ў розных галінах заканадаўства.

Меры бяспекі могуць быць накіраваны на саму крыніцу небяспекі (атамная электрастанцыя), ізалюючы або абмяжоўваючы яго шкоднае ўздзеянне на чалавека і навакольнае асяроддзе, – меры стрымання, або на агароджу аб'екта абароны (асоба, таямніцу, уласнасць) ад знешніх крыніц небяспекі – меры аховы. Паколькі адзін і той жа аб'ект можа быць адначасова аб'ектам аховы і крыніцай небяспекі, могуць быць і меры падвойнага прызначэння, якія спалучаюць у сабе адначасова функцыю стрымання і функцыю аховы – меры стрымання і аховы.

Класіфікацыйнымі падставамі могуць служыць характар крыніцы небяспекі або аб'екта аховы. Калі крыніцай небяспекі з'яўляецца злачыннасць, злачынства або асоба злачынцы, ёсць падставы выдзяляць антыкрымінальныя меры бяспекі.

Па ўзроўні меры бяспекі можна падзяліць на меры агульнага, асаблівага і адзінкавага ўзроўню. У залежнасці ад сферы прымянення меры бяспекі класіфікуюцца на эканамічныя, сацыяльна-палітычныя, ідэалагічныя. Да эканамічных мер ставяцца, напрыклад, антыманапольныя абмежаванні; да сацыяльна-палітычных – падзел уладаў; да ідэалагічных – забарона прапаганды фашызму.

Па спосабе можна вылучыць фізічныя, тэхнічныя, арганізацыйныя і інфармацыйныя меры бяспекі. Меры стрымання ў залежнасці ад моманту прымянення можна падзяліць на неадкладныя і прэвентыўныя. Першыя ўжываюцца для спынення ўжо распачатага шкоднага ўздзеяння, другія для спынення шкоднага ўздзеяння, якое яшчэ не пачалося, але верагоднасць якога вельмі высокая.

У залежнасці ад віду сацыяльнай нормы, у якую надзелена мера бяспекі, іх можна падраздзяліць на прававыя і пазаправавыя. Меры бяспекі ў праве – гэта міжгалінавы інстытут, парадкаваны інстытутам пакарання, заахвочванні, кампенсацыі. Ён прадстаўлены ва ўсіх галінах заканадаўства.

Па галіне заканадаўства, у рамках якой рэгламентуюцца меры бяспекі, іх можна падпадзяліць на міжнародна-, канстытуцыйна-, адміністрацыйна-, грамадзянска-, крымінальна-прававыя, працоўныя (вытворчыя), а таксама грамадзянска-, адміністрацыйна-, крымінальна-працэсуальныя і крымінальна- выканаўчыя.

У міжнародным праве яны дазваляюць асудзіць дзяржаву - крыніцу агрэсіі. У канстытуцыйным праве праз падзел уладаў ахаваць уладу ад узурпацыі. У адміністрацыйным праве ўсталяваць адмысловыя рэжымы ў стаўленні крыніц небяспекі (зброя) і аб'ектаў аховы.

У грамадзянскім праве абмежаваць дзеяздольнасць. У сямейным праве з дапамогай пазбаўлення бацькоўскіх правоў ахаваць непаўналетняга ад шкоднага ўплыву.

У працоўным праве не дапусціць да пэўных прафесій некваліфікаваных людзей і забяспечыць тэхніку бяспекі. У крымінальным праве ізаляваць маньяка. У крымінальным працэсе затрымаць падазраванага.

Праблема заключаецца не столькі ў тым, каб прызнаць меры бяспекі, а хутчэй у тым, каб правільна вызначыць сферу і падставы іх прымянення. Для гэтага прапануецца выкарыстоўваць асобасны, тэрытарыяльны і часавы падыходы, якія дапаўняюць адзін аднаго.

Дакладнае абазначэнне межаў дзеяння мер бяспекі па коле асоб, на якіх яны распаўсюджваюцца, па тэрыторыі, на якой яны дзейнічаюць, і па часе іх дзеяння неабходна не толькі для таго, каб пазбегнуць злоўжыванняў, але і для аптымальнага размеркавання праваахоўных рэсурсаў.

Можна вылучыць тыпавыя прыкметы асобы, якая можа быць крыніцай падвышанай небяспекі і (або) аб'ектам падвышанай аховы (узрост, грамадзянства, захворванне, крымінальнае мінулае), а таксама пазначыць тыпавыя прыкметы тэрыторыі, на якіх павінен ажыццяўляцца рэжым бяспекі ў прасторы (дзяржаўная мяжа, закрытая) адміністрацыйна-тэрытарыяльнае ўтварэнне, зона контртэрарыстычнай аперацыі).

Аналагічнай выявай варта распрацаваць правілы дзеянні мер бяспекі ў прасторы. Для абмежавання часовых межаў антыкрымінальных санкцый бяспекі варта ўвесці ў тэорыю права і ў заканадаўства паняцце «тэрміны крыміналагічнай даўнасці» і ўсталяваць, па заканчэнні якога тэрміна, які мінуў з моманту здзяйснення грамадска небяспечнай дзеі, нельга ўжываць меры бяспекі.

Абмежаваць межы мер бяспекі дазваляе дынамічная мадэль шматузроўневых падстаў мер бяспекі, іерархію якой складаюць: сацыяльная, нарматыўна-прававая, фактычная (матэрыяльная) і арганізацыйна-юрыдычная падставы.

Сацыяльная падстава мер бяспекі ўтварае неабходнасць спынення шкоднага ўплыву крыніцы павышанай небяспекі або агароджы аб'екта аховы ад шкоднага ўздзеяння праз абмежаванне канстытуцыйных правоў і свабод асобы. Пры гэтым шкода, вымушана прычыняецца асобы, якая валодае падвышанай небяспекай, або трэцім асобам, павінен быць менш прадухіляемай шкоды. Суразмеранне шкоды ажыццяўляецца па прынцыпах, падобных на правілы крайняй неабходнасці або неабходнай абароны.

Фактычнымі падставамі мер бяспекі могуць выступаць падзеі і дзеянні (не толькі правамерныя, але і неправамерныя). Для прымянення санкцый бяспекі фактычнымі падставамі будуць грамадска небяспечныя дзеянні,

прадугледжаныя федэральным законам. Ужываючы санкцыі бяспекі, права прымяняльнік павінен зыходзіць з прэзумпцыі адсутнасці грамадскай небяспекі асобы да таго часу, пакуль гэтая ўласцівасць не будзе выяўлена ў канкрэтным грамадска небяспечным дзеянні.

Арганізацыйна-юрыдычнымі падставамі служаць акты прымянення ў форме прыгавору, вызначэння суда, пастановы суддзі, пракурора або іншага кампетэнтнага рашэння, у якім адбываецца індывідуалізацыя адносін бяспекі.

Выдзеленыя групы падстаў маюць значэнне на розных стадыях прымянення мер бяспекі: сацыяльная – для заканатворчасці, нарматыўна-прававая і фактычная – для прызначэння, а арганізацыйна-юрыдычная – для выканання мер бяспекі.

Найважнейшай умовай абмежавання межаў мер бяспекі павінна быць належная працэдура іх прызначэння і выкананні. Чым больш адчувальная мера абмяжоўвае правы і свабоды асобы, тым больш аўтарытэтным павінен быць орган, які прымае рашэнне аб яе прымяненні, і тым больш гарантый ад самавольства павінна прадугледжваць працэдура прыняцця і выканання рашэння. Выключэнне магчыма толькі для прымянення неадкладных мер бяспекі (контртэрарыстычная аперацыя).

Але і ў гэтым выпадку постфактум абавязкова павінна праводзіцца старанная праверка абгрунтаванасці прымянення мераў бяспекі. Аптымальны для такіх выпадкаў парламенцкі і судовы кантроль. Калі працэдура прымянення мер бяспекі змяшчае моманты, якія абмяжоўваюць канстытуцыйныя правы і свабоды, яна павінна быць прадугледжана толькі ў федэральным законе. Рашэнне працэдурных пытанняў, якія ўшчамляюць правы і свабоды грамадзян, у падзаконных нарматыўных актах недапушчальна.

І, нарэшце, неабходнай перадумовай ужывання мер бяспекі павінен служыць прагноз, які, нажаль, адсутнічае пры выкарыстанні гэтага інстытута як у глабальным, так і індывідуальным маштабе.

Асноўныя этапы развіцця тэорыі рызык

Тэрмін «рызыка» мае старажытную этымалогію. У першапачатковай сваёй літаральнай трактоўцы, якая згадваецца яшчэ Гамерам, ён характарызаваўся як «небяспека лавіравання паміж скал». З такой яго трактоўкай звязаны грэцкі тэрмін "ridsikon", лацінскі – "ridsicare", французскі – "risdoe". Першыя спробы асэнсавання паняцця рызыка адносяцца да 13 стагоддзя. Гэта адбылося дзякуючы азартным гульням. Азартныя гульні былі вядомыя яшчэ ў старажытнасці і развіваліся ў розных варыянтах. Ніхто не спрабаваў рабіць разлік магчымай колькасці зыходаў. Асноўная прычына была ў тым, што не было зацікаўленых асоб у такім падліку.

Ігральныя косці шырока выкарыстоўваліся для кідання жэрабя і прадказанняў, таму ўсякая спроба прадбачыць вынік кідка магла быць разгледжана як спроба прадказаць адпаведнае боскае дзеянне. Самая ранняя вядомая спроба падлічыць колькасць магчымых зыходаў пры кіданні трох ігральных костак, уключаючы перастаноўкі, сустракаецца ў паэме Рычарда дэ Форніваля.

У `XVI стагоддзі асэнсаваць заканамернасці гульні паспрабаваў Кардано. У яго трактаце "Кніга аб выпадковых гульнях" былі зроблены спробы распрацаваць статыстычныя прынцыпы тэорыі верагоднасці. Ён сфармуляваў уяўленне аб верагоднасці як стаўленне спрыяльных зыходаў да агульнай колькасці магчымых. Пры гэтым ён сам практычна не ўжываў дадзенае паняцце, а выкарыстоўваў слова "шанц". У XVII стагоддзі Блез Паскаль даследаваў азартныя гульні. У супрацоўніцтве з П'ерам дэ Ферма ён вырашыў матэматычную задачу аб размеркаванні банка паміж двума гульцамі ў выпадку спынення нясканчанай гульні пры адназначнай перавазе аднаго з гульцоў да моманту заканчэння гульні.

Простае рашэнне – падзяліць банк пароўну – Ферма і Паскаль адпрэчылі, лічачы яго абсалютна несправядлівым, такім чынам, упершыню матэматычнае рашэнне было спалучана з праблемай маральнага права. У выніку Блез Паскаль і П'ер дэ Ферма распрацавалі тэорыю верагоднасці, якая

дала новыя магчымасці адзнакі велічыні рызыкі. Таксама Паскаль і Ферма прапанавалі сістэмны метад вылічэння імавернасці будучых падзей. Гэта дазволіла навукова ажыццяўляць колькасныя прагнозы будучыні. Аднак выкарыстанне апарата тэорыі верагоднасці патрабавала наяўнасці верагоднасцяў, якія неабходна вылічаць на аснове наяўных дадзеных.

Геніяльным вырашэннем гэтай праблемы з'явілася прапанова Джона Гранта аб магчымасці выкарыстання выбаркі пры прыняцці рашэнняў. У 1662 годзе ў Лондане ён апублікаваў кнігу «Натуральныя і палітычныя назіранні, якія тычацца сведчанняў аб смерці», у якой упершыню былі скарыстаны выбарачныя і імавернасны метады, якія з'яўляюцца асновай кіравання рызыкай.

Пазней Эдмунд Галлей, выкарыстоўваючы навуковыя падыходы Гранта, правёў статыстычнае даследаванне ў г. Брэслаў за 1687 – 1691 гады. Маючы падрабязныя дадзеныя аб нараджальнасці і смяротнасці, ён атрымаў унікальныя вынікі: ацаніў агульную колькасць людзей, якія пражываюць у дадзеным горадзе.

Таксама Галей правёў дэталёвы матэматычны аналіз велічыні розных відаў рэнты. У цяперашні час кіраванне страхавымі рызыкамі неймаверна без выкарыстання ідэй Гранта і Галлея. Развіццё страхавога бізнэсу мела яшчэ адзін важны напрамак – страхаванне марскіх рызык. Пры гэтым была неабходна інфармацыя аб новых маршрутах, краінах і ўмовах мараплаўства.

У той час не было сродкаў масавай інфармацыі, а асноўным месцам збору былі кавярні ў партовых гарадах, дзе збіраліся маракі, гандляры і страхавальнікі. Эдвард Лойд, уладальнік кавярні на беразе

Тэмзы, заўважыў цікавасць сваіх кліентаў да пэўнай інфармацыі і ў 1696 годзе пачаў выпускаць інфармацыйны ліст, у якім збіраліся звесткі аб судах, якія прыплываюць і адплываюць, аб становішчы за мяжой і на морах, аб караблекрушэннях. Стала відавочна, што дадатковая інфармацыя аб умовах мараплаўства спрыяе значнаму зніжэнню рызык.

Да канца першага этапу развіцця навуковых ведаў аб рызыцы чалавецтва навучылася вызначаць велічыню рызыкі з ужываннем метадаў тэорыі верагоднасці. Аднак не былі вырашаны пытанні ўліку ўплыву суб'ектыўнага фактара на дакладнасць ацэнкі рызыкі. Акрамя таго, разлік верагоднасці па ўжо адбыўшыхся фактах абцяжарваў прыняцце рашэнняў, звернутых у будучыню.

У пачатку XVIII стагоддзя Готфрыд Вільгельм Лейбніц высунуў ідэю, а Якаб Бярнулі абгрунтаваў закон вялікіх лікаў і асноўныя працэдуры статыстыкі. У працы «Закон вялікіх лікаў» Я. Бярнулі паказаў, як, размяшчаючы абмежаваным наборам дадзеных, можна разлічыць верагоднасць і статыстычную значнасць падзей. Ён упершыню сфармуляваў задачу аб вызначэнні верагоднасці на аснове інфармацыі аб абмежаваным выбары рэальных падзей, таксама ён прапанаваў дапушчэнне, што пры роўных умовах наступ або не наступ падзеі ў будучыні будзе прытрымлівацца тым жа заканамернасцям, якія назіраліся ў мінулым.

У 1738 г. Данііл Бернулі, заўважыўшы, што пры выбары рашэння больш увагі надаецца наступствам рызыкі, чым яго верагоднасці наступу, прапанаваў паняцце "карыснасць рызыкі", на якім у значнай меры пабудавана сучасная тэорыя партфельных інвестыцый. Карыснасць у кожным асобным выпадку залежыць ад асобы, якая робіць ацэнку, бо людзі, якія трапілі ў адно і тое ж становішча, напрыклад, няштатная сітуацыя падчас палёту самалёта, паводзяць сябе па-рознаму.

У XVIII стагоддзі пачалі фармавацца асноўныя прынцыпы тэорыі рызыкі ў прадпрымальніцкай дзейнасці, звязаныя з парадыгмай эканамічнага аналізу класічнай палітычнай эканоміі, у першую чаргу, з працамі А. Сміта. У сваёй кнізе "Даследаванне аб прыродзе і прычынах багацця народаў" (1784 г.) ён разглядаў тэорыю прадпрымальніцкай рызыкі на прыкладах аплаты працы наёмных працоўных, функцыянавання латарэй і практыкі страхавой справы. Характарызуючы з пазіцый фактара рызыкі адрознення ва

ўзроўнях заработнай платы, ён сцвярджаў, што рабочыя патрабуюць больш высокай аплаты ў тых выпадках, калі пастаянная занятасць ім не гарантавана.

Такі прынцып фарміравання ўмоў працоўнага кантракта стаў пазней асновай адной з вядомых тэорый, які разглядаецца як здзелка паміж работнікам, які пазбягае рызыкі, і фірмай, нейтральнай да рызыкі. А. Сміт адным з першых паказаў, што прадпрымальніцкая рызыка мае не толькі эканамічную, але і псіхафізічную прыроду, і прыйшоў да высновы аб тым, што прафесіі з высокім узроўнем рызыкі гарантуюць у сярэднім больш высокую аплату, чым прафесіі з нізкім узроўнем рызыкі. Гэты вывад пазней быў пакладзены ў аснову сучаснага пастулату тэорыі рызыкі – аб узаемасувязі узроўняў даходнасці і рызыкі.

У гэты час фармулюецца класічная тэорыя, якая звязвае паняцці рызыкі і прадпрымальніцкага прыбытку, які належыць Джону Сцюарту Мілю. У сваёй кнізе "Прынцыпы палітычнай эканоміі" Міль разглядае прадпрымальніцкі прыбытак як суму заработнай платы капіталіста, долі (працэнта) на ўкладзены капітал і платы за рызыку. Плата за рызыку па Мілю, гэта кампенсацыя магчымага ўрону, звязанага з небяспекай страты капіталу ў выніку прадпрымальніцкай дзейнасці.

У далейшым і Джон Морыс Кларк стаў лічыць рызыку адзінай крыніцай прадпрымальніцкага прыбытку. Прамую залежнасць ступені гатоўнасці прадпрымальніка рызыкаваць ад чаканага прыбытку адзначаў Карл Маркс. Далейшае развіццё тэорыі рызыкі звязана з даследаваннямі Й. фон Цюнена. У сваёй працы "Ізаляваная дзяржава ў яе адносінах да сельскай гаспадаркі і нацыянальнай эканомікі" (1850 г.) ён упершыню разгледзеў сутнасць інавацыйных рызык у працэсе прадпрымальніцкай дзейнасці.

Цюнэн вызначыў прыбытак прадпрымальніка як даход, які застаецца ад валавага прыбытку дзелавой аперацыі пасля выплаты працэнта на інвесціраваны капітал, платы за кіраванне і страхавой прэміі па вылічаных рызык страт. Узнагароджанне прадпрымальніка, з'яўляецца, такім чынам,

даходам за прыняцце на сябе тых рызык, якія з-за іх непрадказальнасці не пакрые ні адна страхавая кампанія. Гэтая выснова ўпершыню азначыла адрозненні паміж умовамі, верагоднасць, якіх можа быць разлічана і умовамі, верагоднасць якіх непрадказальная.

У 20 стагоддзі паняцце "рызыка" было прызнана ў якасці неад'емнай складніку любой прадпрымальніцкай дзейнасці, якая ажыццяўляецца ва ўмовах нявызначанасці. Рызыка разглядалася як вынік уздзеяння антрапагенных штучных і прыродных натуральных фактараў, што магчыма пры высокім узроўні ведаў чалавека аб навакольным свеце.

З'явілася неабходнасць сістэмнага падыходу да кіравання рызыкамі. Узніклі складаныя сістэмы ацэнкі і прагназавання, якія дазваляюць эфектыўна кіраваць рызыкамі. Пры гэтым для колькаснага вымярэння велічыні рызыкі шырока ўжываўся матэматычны апарат тэорыі верагоднасці, які выкарыстоўвае паняцце "выпадковасць".

Пэўны ўклад у развіццё інавацыйнай тэорыі рызыкі быў унесены І. Шумпетэрам. У сваёй кнізе "Тэорыі эканамічнага развіцця" (1912 г.) ён прапанаваў новы падыход да адзнакі ролі прадпрымальнікаў, якія ажыццяўляюць інавацыйную дзейнасць ва ўмовах рызыкі. Ён сцвярджаў, што толькі тэхналагічныя інавацыі могуць спарадзіць станоўчую стаўку працэнта. Адпаведна, прадпрымальнік, які ажыццяўляе інавацыйную дзейнасць ва ўмовах высокай рызыкі, з'яўляецца крыніцай усіх станоўчых дынамічных змен у эканоміцы.

Альфрэдам Маршалам і Артурам Пігу была распрацаваная так званая «неакласічная» тэорыя прадпрымальніцкай рызыкі. Сутнасць гэтай тэорыі зводзіцца да наступнага. У рынкавай эканоміцы прадпрыемства працуе ва ўмовах нявызначанасці, у сувязі з чым прыбытак з'яўляецца велічынёй выпадковай і зменнай, таму прадпрымальніка цікавіць не толькі велічыня прыбытку, але і размах яе верагодных ваганняў.

Па дадзенай тэорыі атрымліваецца, невялікі, але гарантаваны прыбытак выгодней, чым вялікі, але сумнеўны. Адгэтуль робіцца выснова аб

нявыгаднасці ўдзелу ў азартных гульнях, латарэях і таму падобных азартных мерапрыемствах.

У 1921 году Ф. Найт у кнізе «Рызыка, нявызначанасць і прыбытак» развіў выснову Й. Цюнена аб адрозненнях паміж вылічанай і невылічальнай прадпрымальніцкай рызыкай. Ён указаў на неабходнасць раздзялення паняццяў рызыкі і нявызначанасці. Вымерная нявызначанасць з'яўляецца рызыкай. Невымерная нявызначанасць з'яўляецца нявызначанасцю. Тэарэтычныя высновы Ф. Найта дазволілі ўпершыню з часоў А. Сміта выразна аддзяліць фактар рызыкі ад фактараў вытворчасці ў працэсе фарміравання прадпрымальніцкага прыбытку.

На парадак дня стала распрацоўка тэорыі выбару які ўлічвае рызыку варыянту ўкладання капіталу (інвестыцый), уліку рызыкі пры крэдытаванні, звязанага з тэхналагічнымі прычынамі (знос і паломкі абсталявання), прыроднымі катастрофамі, ваганнямі цэн і пакупніцкага попыту. Значны ўклад у вырашэнне гэтых праблем унёс Джон Мэйнард Кейнс. Ён увёў паняцце выдаткаў рызыкі, разумеючы пад імі тыя сродкі, якія прадпрымальнік павінен уключаць у выдаткі для страхоўкі на выпадак адхілення рэальнай выручкі ад запланаванай выручкі.

У выдаткі рызыкі варта ўключаць сродкі для пакрыцця магчымых падзенняў рынкавых коштаў, аварый і катастроф і заўчаснага зносу абсталявання. Прадпрымальнік павінен улічваць рызыку страты чаканай выгады ад непрадбачаных абставін; рызыка крэдытора ад магчымай страты пазыкі; рызыка ад страты рэальнага кошту грошай з цягам часу.

Прагрэс у разуменні рызыкі і нявызначанасці быў дасягнуты ў рамках тэорыі стратэгічных гульняў. У 1953 г. Нэйман разам з Оскарам Моргенштэрнам выдаў кнігу «Тэорыя гульняў і эканамічныя паводзіны». Тэорыя гульняў адкрыла прынцыпова новы падыход да разумення сутнасці нявызначанасці. Крыніцай нявызначанасці з'яўляюцца намеры іншых людзей. Для эканамічных і сацыяльных праблем гульні выконваюць – ці павінны выконваць – тую ж ролю, якую розныя геаметрычныя і

матэматычныя мадэлі з поспехам ажыццяўляюць у фізічных навуках. Адным з найважнейшых момантаў у развіцці тэорыі рызыкі стала з'яўленне паняцця "дыверсіфікацыя", прапанаванае ў 1952 г. Гары Марковіцам.

Дыверсіфікацыя дазваляе шляхам прадуманага размеркавання ўкладанняў мінімізаваць інвестыцыйную рызыку, напрыклад пры фарміраванні інвестыцыйнага партфеля. Маркавіц вызначыў паняцце "дысперсія (зменлівасць)" як меру рызыкі або нявызначанасць даходу.

Дэніэл Канеман і Эймас Цвярскі ў 60-я гады XX стагоддзя даследавалі паводзіны людзей ва ўмовах рызыкі і нявызначанасці. Яны распрацавалі тэорыю перспектывы, у якой апісалі стэрэатыпы паводзін людзей, якія не заўважаліся раней прыхільнікамі тэорыі рацыянальнага прыняцця рашэнняў.

У наш час у чыстым выглядзе класічная і неакласічная тэорыі не існуюць, паколькі зведалі пэўную трансфармацыю. Агульнараспаўсюджанай тэорыяй эканамічнай рызыкі зараз з'яўляецца неакласічная з тымі дадаткамі, якія ўнёс Дж. Кейнс. Ён упершыню даў падрабязную класіфікацыю прадпрымальніцкіх рызык, дапоўніўшы неакласічную тэорыю фактарам задавальнення. Асноўным недахопам папярэдняй неакласічнай тэорыі Кейнс лічыў недаацэнку схільнасці да рызыкі, часта сустракаемай у практыцы прадпрымальнікаў.

Далейшае развіццё неакласічнай тэорыі рызыкі прадставілі ў сваіх працах Т. Бачкаі, Д. Месена, якія сцвярджаюць, што сутнасць рызыкі – не шкода, якая наносіцца рэалізацыяй рашэння, а магчымасць адхілення ад мэты, дзеля дасягнення якой прымалася рашэнне. Гэта значыць, што разам з рызыкай панесці выдаткі існуе рызыка атрымання дадатковых даходаў (прыбытку).

Тэорыя рызык

Рызыка ў класічнай тэорыі атаясамліваецца з матэматычнымі чаканнямі страт, якія могуць быць у выніку рэалізацыі абранага рашэння. Асноўным

палажэннем класічнай тэорыі з'яўляецца вызначэнне рызыкі як верагоднасці панесці страты і страты ад абранага рашэння і стратэгіі дзейнасці.

Такое тлумачэнне рызыкі з'яўляецца аднабаковым. Яно пацягнула за сабой распрацоўку іншай тэорыі, якая была названая неакласічным. Гэтая тэорыя заснавана на наступных палажэннях: прадпрыемства (ці фірма), якое працуе ва ўмовах нявызначанасці і прыбытак якога з'яўляецца выпадковай зменнай велічынёй, павінна кіравацца ў сваёй дзейнасці двума крытэрамі: памерам чаканага прыбытку і велічынёй яе магчымых ваганняў.

Паводзіны прадпрымальніка абумоўліваецца канцэпцыяй так званай лімітавай карыснасці. Гэта азначае, што калі трэба выбраць адзін з двух варыянтаў інвеставання капіталу, які дае аднолькавую прадпрымальніцкую прыбытак, то варта выбіраць той з варыянтаў, у якім ваганні прыбытку будуць меншымі.

З гэтай тэорыі рызыкі вынікае, што дакладны прыбытак заўсёды мае большую карыснасць, чым прыбытак таго ж чаканага памеру, але злучаны з магчымымі ваганнямі. Найбольш прызнанай з'яўляецца неакласічнай тэорыя рызыкі, але з пэўнымі дапаўненнямі, унесенымі ў яе Кейнс, які:

1) упершыню сістэматызаваў існавалыя тэорыі рызыкі і даў падрабязную класіфікацыю прадпрымальніцкіх рызык;

2) дапоўніў неакласічную тэорыю фактарам «задавальнення», які складаецца ў тым, што прадпрымальнік у чаканні большага прыбытку хутчэй за ўсё пойдзе на большую рызыку.

Рызыка разглядаецца з пункту гледжання магчымага матэрыяльнага ўрону, звязанага з рэалізацыяй гаспадарчых, арганізацыйных, тэхнічных рашэнняў, з аварыямі, стыхійнымі бедствамі, банкруцтвам, памяншэннем каштоўнасці акцый і грашовай адзінкі, а таксама – з пункту гледжання прыняцця рашэнняў, звязаных. з атрыманнем прыбытку або даходу.

Па-першае, рызыка разумеецца як няўдача, небяспека матэрыяльных і фінансавых страт, якія могуць наступіць у выніку рэалізацыі абранага

рашэння. Па-другое, рызыка атаясамліваецца з меркаваным поспехам і атрыманнем прыбытку.

Упершыню найбольш агульнае вызначэнне рызыкі даў Найт. Рызыка – гэта выява дзеянняў у смутнай, нявызначанай абстаноўцы.

Рызыка – гэта сітуатыўная характарыстыка дзейнасці, якая можа мець нявызначаны зыход і неспрыяльныя наступствы ў выпадку няўдачы.

Гэтыя азначэнні ў большай меры ставяцца да паняцця рызыка ў цэлым.

Тэорыя эканамічных рызык

Аб эканамічнай рызыцы варта казаць як аб працэсе прыняцця рашэнняў ва ўмовах нявызначанасці з улікам як эканамічных, так і палітычных, маральных, псіхалагічных і іншых наступстваў, галоўным чынам неспрыяльных.

Сітуацыі рызыкі – сітуацыі, якія не маюць адназначнага зыходу або рашэнні, але абавязкова патрабуюць выбару аднаго з некалькіх варыянтаў.

Эканамічная рызыка – гэта дзейнасць суб'ектаў гаспадарчага жыцця, звязаная з пераадоленнем нявызначанасці сітуацыі непазбежнага выбару, у працэсе якой ёсць магчымасці ацаніць верагоднасці дасягнення жаданага выніку, няўдачы і адхіленняў ад іх па ўсіх разгляданых варыянтах.

У працэсе гаспадарчай дзейнасці пры прыняцці рашэнняў варта:

1) улічваць ступень верагоднасці дасягнення патрэбнага выніку і верагоднасць адхілення ад яго;

2) спрабаваць выяўляць магчымасці рэалізацыі сваіх рашэнняў, каб прадухіляць неспрыяльныя наступствы.

Адрозніваюць дзве функцыі рызыкі – стымулюючую, ахоўную. Стымулюючая функцыя мае два аспекты: канструктыўны і дэструктыўны. Першы аспект выяўляецца ў тым, што рызыка пры рашэнні эканамічных задач з'яўляецца каталізатарам, асабліва пры прыняцці інавацыйных інвестыцыйных рашэнняў. Другі аспект праяўляецца ў тым, што прыняцце і

рэалізацыя рашэнняў з неабгрунтаванай рызыкай вядуць да авантурызму. Авантура – разнавіднасць рызыкі, якая аб'ектыўна змяшчае значную верагоднасць немагчымасці ажыццяўлення задуманай мэты, хоць асобы, якія прымаюць такія рашэнні, гэтага не ўсведамляюць.

Ахоўная функцыя таксама мае два аспекты: гісторыка-генетычны і сацыяльна-прававы. Змест першага аспекту складаецца ў тым, што людзі заўсёды стыхійна шукаюць формы і сродкі абароны ад магчымых непажаданых наступстваў. На практыцы гэта выяўляецца ў стварэнні страхавых, рэзервовых фондаў, страхаванні прадпрымальніцкіх рызык. Сутнасць другога аспекту заключаецца ў неабходнасці ўкаранення ў гаспадарчае, працоўнае, крымінальнае заканадаўства катэгорый правамернасці рызыкі.

Працэс ацэнкі рызыкі ўключае ў сябе тры этапы:

1) выяўленне магчымых варыянтаў рашэння праблемы;

2) вызначэнне магчымых эканамічных, палітычных, маральных і іншых наступстваў, галоўным чынам негатыўных, якія могуць наступіць у выніку рэалізацыі рашэння;

3) інтэгральны бок рызыкі, які ў сваю чаргу складаецца з двух узаемазвязаных аспектаў – якаснага і колькаснага.

Асноўным з'яўляецца колькасны аспект адзнакі рызыкі. Прынята лічыць, што немэтазгодна ажыццяўленне рашэнняў, якія пры іх адпаведнасці колькасным параметрам адзнакі не адказваюць якасным параметрам рызыкі. Такі падыход прынята лічыць тэхнакратычным.

Існуюць тры асноўныя крытэрыі колькаснай ацэнкі рызыкі.

Сутнасць першага ў тым, што рашэнні, якія выбіраюцца ў сітуацыі рызыкі, павінны ацэньвацца з пазіцыі верагоднасці дасягнення меркаванага выніку і магчымага адхілення ад пастаўленай мэты.

З матэматычнага пункта гледжання, рызыка будзе роўны рознасці паміж чаканым вынікам дзеяння пры наяўнасці дакладных дадзеных абстаноўкі і вынікам, які можа быць дасягнуты, калі гэтыя дадзеныя не

вызначаны. Па агульным правіле лічыцца немэтазгодным прыняцце рашэнняў, рызыка якіх вымяраецца верагоднасцю 0,5-0,6 і вышэй.

З фінансавага пункту гледжання, рызыка можа быць трох ступеняў:

1) дапушчальная рызыка, звязаная са стратай прыбытку ў выпадку не рэалізацыі рашэнняў;

2) крытычная рызыка, звязаная з магчымасцю не атрымання (страты) выручкі або даходу;

3) катастрафічная рызыка, якая ўплывае на ліквідацыю пазіцый фірмы, на магчымасць яе плацежаздольнасці. Такая рызыка з'яўляецца прамой перадумовай банкруцтва фірмы.

Другі крытэрый колькаснай адзнакі рызыкі заключаецца ў тым, што лепшым будзе рашэнне, якое ў існых умовах забяспечвае дасягненне патрэбнага выніку пры меншых выдатках у параўнанні з іншымі варыянтамі.

Сутнасць трэцяга крытэрыя заключаецца ў тым, што лепшым будзе тое рашэнне, на рэалізацыю якога затрачваецца менш часу. Ступень рызыкі вызначаецца ўронам і верагоднасцю таго, што гэты ўрон адбудзецца.

Страхаванне рызык

Адна з распаўсюджаных прычын атрымання страт і, як следства, банкруцтва прадпрыемстваў, з'яўляюцца рызыкі па неаплаце за тавары, сарваныя пастаўкі (недапастаўкі) прадукцыі, невыкананне работ і паслуг.

Маёмасныя інтарэсы страхавальніка, звязаныя з рызыкай узнікнення ў яго страт у сувязі з невыкананнем (выкананнем неналежным чынам) сваіх абавязацельстваў Контрагентамі страхавальніка пры ажыццяўленні прадпрымальніцкай дзейнасці па наступных відах здзелак: купля-продаж, у тым ліку пастаўка тавараў, пастаўка тавараў для дзяржаўных патрэб, кантрактацыя, продаж нерухомасці, продаж прадпрыемства; мена; арэнда, у тым ліку пракат, арэнда транспартных сродкаў, будынкаў ці збудаванняў, прадпрыемствы, фінансавая арэнда (лізінг); запар, у тым ліку бытавы,

будаўнічы, запар на выкананне праектных і пошукавых работ, падрадныя работы для дзяржаўных патрэб.

Таксама ў спіс уваходзіць выкананне навукова-даследчых работ і доследна-канструктарскіх і тэхналагічных работ; аплатнае аказанне медыцынскіх, ветэрынарных, аўдытарскіх, кансультацыйных, інфармацыйных, рыэлтарскіх, турыстычных паслуг і паслуг сувязі; перавозка; транспартная экспедыцыя; захоўванне на таварным складзе; камісія. Прадугледжваецца выдача банкаўскіх гарантый (паручыцельства); адкрыццё акрэдытыва; пазыка; факторынг.

Страхавой рызыкай з'яўляецца фінансавая прадпрымальніцкая рызыка, звязаная з невыкананнем, неналежным выкананнем контрагентам страхавальніка (даўжніком) абавязацельстваў, прынятых на сябе па дагаворы са страхавальнікам, якія выказаліся ў: не пастаўцы, недапастаўцы тавараў, не перадачы маёмасці (тавара), невыкананні работ, неаказанні паслуг у тэрміны, устаноўленыя дагаворам; пастаўцы тавараў якасці, камплектнасці, якія не адпавядаюць умовам заключанага дагавора (толькі па здзелках куплі-продажу, пастаўкі тавараў, пастаўкі тавараў для дзяржаўных патрэб); нявыплаце грошай (неажыццяўленні плацяжоў) у тэрміны, устаноўленыя дагаворам (у тым ліку дагаворам лізінгу).

Таксама выказаліся ў незвароту грашовых сродкаў, выплачаных страхавальнікам па банкаўскай гарантыі (паручыцельству), калі гэта прадугледжана пагадненнем паміж гарантам і прынцыпалам (паручыцелем і даўжніком). Выяўленых у невяртанні грашовых сродкаў, выплачаных страхавальнікам па акрэдытыву, калі гэта прадугледжана пагадненнем паміж загадальнікам і банкам-эмітэнтам; незварот грашовых сродкаў даўжніком (крэдыторам), прадастаўленых страхавальнікам па дагаворы факторынгу; незварот грашовых сродкаў, выдадзеных страхавальнікам па дагаворы пазыкі.

Пры надыходзе страхавога выпадку, страхавальніку неабходна паведаміць страхоўшчыка аб падзеі, якая можа быць прызнана страхавым

выпадкам на працягу трох дзён. У залежнасці ад умоў страхавання парадак і тэрміны абыходжання з заявай аб страхавым выпадку па ўстаноўленай форме ўзгадняюцца са страхоўшчыкам на падставе правілаў страхавання.

Эканамічная бяспека карпарацыі, кампаніі і прадпрыемствы

Эканамічная карпаратыўная бяспека з'яўляецца вызначанай характарыстыкай стану кампаніі і прадпрыемствы, якую пажадана вымяраць колькасна альбо як скалярную, альбо як вектарную велічыню. Эканамічная бяспека прадпрымальніцкай структуры прадугледжвае абароненасць яе жыццёва важных інтарэсаў ад унутраных і знешніх пагроз.

Гэта абарона прадпрымальніцкай структуры, яе кадравага і інтэлектуальнага патэнцыялу, інфармацыі, тэхналогій, капіталу і прыбытку, якая забяспечваецца сістэмай мер спецыяльнага прававога, эканамічнага, арганізацыйнага, інфармацыйна-тэхнічнага і сацыяльнага характару.

Вызначэнне бяспекі павінна быць заснавана не толькі на інтарэсах уласніка, але і ўлічваць інтарэсы іншых зацікаўленых бакоў. У сілу гэтых абставін больш абгрунтаваным з'яўляецца падыход да вызначэння эканамічнай бяспекі прадпрыемства з пазіцый дасягнення мэт, якія праследуюцца прадпрыемствам, якія апасродкавана ўлічваюць інтарэсы бакоў, зацікаўленых у яго дзейнасці.

Эканамічная бяспека прадпрыемства як эканамічнага аб'екта вызначаецца станам архітэктуры, дынамікай функцыянавання, захаваннем жыццёва важных інтарэсаў, забеспячэннем патрэб і трэндам развіцця. Гэтая характарыстыка схільная ўздзеянню, якое негатыўна ўплывае на функцыянаванне прадпрыемства. Гэтае ўздзеянне разглядаецца як пагроза, якая прыводзіць да пагаршэння вынікаў дзейнасці.

Мяркуецца наяўнасць у прадпрыемства нейкай асноўнай характарыстыкі, якая можа быць схільная да непажаданага ўздзеяння. Калі

гэтая характарыстыка абаронена ад непажаданага ўздзеяння (пагроз), то тым самым забяспечана эканамічная бяспека прадпрыемства. Крытэрый ацэнкі бяспекі ці адсутнічае, ці ацэньваецца прыбыткам. Для прадпрыемства як эканамічнага аб'ект заўсёды вызначана яго місія, якая вызначае мэты і вынікі яго дзейнасці.

Ажыццяўляючы сваю дзейнасць у навакольным асяроддзі, прадпрыемства мае архітэктуру, якая і дазваляе яму функцыянаваць з аднаго боку, а з другога – дазваляе знаходзіцца ў раўнаважкім, устойлівым стане, якое можна назваць бяспечным.

Гэта азначае, што менеджмент прадпрыемства забяспечвае яго паспяховае функцыянаванне і дасягненне пастаўленых мэт, нягледзячы на негатыўнае ўздзеянне навакольнага асяроддзя. І калі змяненне знешніх умоў выходзіць за пэўныя межы, то менеджмент не можа забяспечыць эфектыўнае функцыянаванне прадпрыемства і дасягненне ім сваіх мэт з-за канечнасці яго рэсурсаў і абмежаванняў, якія накладаюцца архітэктурай.

Тэрмін "эканамічная бяспека" вызначаецца праз паняцці "пагроза", "небяспека", "непажаданыя змены", "непрадбачаныя абставіны". Для практычнай дзейнасці мэтазгодна прадбачыць узнікненне пагроз, каб дзеянні па планаванні забеспячэння эканамічнай бяспекі сапраўды былі б эфектыўнымі і дзейснымі.

Аднак з гэтага не вынікае, што эканамічная бяспека другасная ў адносінах да паняцця пагрозы. Такім чынам, эканамічная бяспека прадпрыемства – гэта характарыстыка стану прадпрыемства незалежна ад існавання тых ці іншых пагроз. Гэтая характарыстыка павінна малаважна змяняцца пры абмежаваных ваганнях навакольнага асяроддзя.

Уласніку, адпаведна і мэнэджменту прадпрыемства, заўсёды важна, каб прадпрыемства дасягнула жаданых эканамічных вынікаў. Гэта залежыць, па-першае, у якім стане знаходзіцца прадпрыемства, па-другое, якія рашэнні будуць прыняты і рэалізаваны, па-трэцяе, якія магчымасці мае прадпрыемства для рэалізацыі прынятых рашэнняў. Гэтыя аспекты тычыліся

ў асноўным унутранага асяроддзя прадпрыемства, што, вядома, адбіваецца на эканамічнай бяспецы прадпрыемства. Але і навакольнае асяроддзе непасрэдна ўплывае на атрыманне запланаваных вынікаў, што прадугледжвае і тут правядзенне мерапрыемстваў па эканамічнай бяспецы прадпрыемства.

Такім чынам, калі будзе забяспечана нармальнае функцыянаванне прадпрыемства (унутранае асяроддзе), а змена вонкавых умоў не будзе моцна адрозніваццa ад меркаваных, тое прадпрыемства дасягне сваіх мэт і вынікаў. Пад нармальным функцыянаваннем прадпрыемства разумеецца атрыманне ад яго дзейнасці прыбытку, які адпавядае ўяўленням уласніка. Эканамічная бяспека прадпрыемства – гэта такая характарыстыка стану прадпрыемства, пры якім яно здольна дасягнуць сваіх мэт і вынікаў пры абмежаваных зменах знешняга і ўнутранага асяроддзя.

Абмежаванасць змен двух асяроддзяў кажа толькі аб тым, што абсалютнай эканамічнай бяспекі не існуе. Яе можна забяспечыць толькі пры пэўных умовах. Напрыклад, пры скачкападобнай змене цэн на прадукцыю, сыравіну, энергарэсурсы, раптоўным павышэнні заработнай платы, нечаканым увядзенні новага заканадаўства, непрадбачаных санкцыях іншых дзяржаў забяспечыць эканамічную бяспеку прадпрыемства не ўяўляецца магчымым, калі згаданыя дзеянні прыводзяць да рэзкага памяншэння прыбытку.

Для прадпрыемства характэрна наяўнасць унутранага асяроддзя, якая вызначае яго стан, і навакольнага асяроддзя, якая аказвае ўздзеянне на вынікі яго дзейнасці. Такім чынам, існуюць пэўныя ўмовы гаспадарання, на частку якіх яно можа ўплываць, а на астатнія істотна паўплываць не ў сілах.

Напрыклад, эканамічная бяспека прадпрыемства не можа быць забяспечана пры надыходзе форс-мажорных абставін, такіх як стыхійныя бедствы, тэхнагенныя катастрофы, войны, забастоўкі, рэвалюцыі.

Такім чынам, у якасці крытэрыю, які ацэньвае эканамічную бяспеку прадпрыемства, можа служыць ацэнка ступені дасягнення запланаваных

вынікаў і мэт. У сувязі з гэтым можна вылучыць два складнікі стан уласнасці і эканамічныя рашэнні па яе выкарыстанні. Для прадпрыемства яго стан вызначаецца архітэктурай і наяўнасцю неабходных для вытворчасці такіх кампанентаў.

Аналіз пунктаў гледжання на эканамічную бяспеку прадпрыемства як сыравіну, энергарэсурсы. Рэзультатыўнасць дзейнасці прадпрыемства вызначаецца тым даходам, які атрымлівае ад яго дзейнасці ўласнік у выглядзе дывідэндаў, партнёры (плацяжы за пастаўленыя матэрыялы, камплектуючыя вырабы, энергарэсурсы); кліенты (гандаль прадукцыяй прадпрыемства); персанал (узнагароджанне за працу); дзяржава (падаткі). Калі велічыня даходу дастатковая па ўяўленнях вышэйпаказаных бакоў у сучаснасці і будучыні, то можна казаць аб дастатковай эканамічнай бяспецы прадпрыемства.

Такім чынам, спосаб дасягнення стану эканамічнай бяспекі прадпрыемства вызначаецца своечасовым выкананнем абавязацельстваў у сучаснасці і будучыні пры магчымым змене ўмоў дзейнасці. Захаванне ўласнасці з'яўляецца неабходным, а эфектыўнае яе выкарыстанне дастатковай умовай эканамічнай бяспекі прадпрыемства. На гэтай падставе задаюцца запланаваныя вынікі; вызначаюцца функцыі, паўнамоцтвы і ступень адказнасці мэнэджменту; накіроўваюцца інвестыцыі і выдзяляюцца неабходныя рэсурсы; кантралююцца выдаткі.

Галоўным кантралёрам на прадпрыемстве выступае бухгалтэрыя, мэтай якой з'яўляецца захаванне цэласнасці і забеспячэнні правільнасці разлікаў з пастаўшчыкамі, кліентамі, уласнікамі, персаналам і дзяржавай. Забеспячэнне эканамічнай бяспекі прадпрыемства заключаецца ў прыняцці і рэалізацыі такіх кіраўнічых рашэнняў, якія максімізуюць даходы ўсіх зацікаўленых бакоў пры ўмове захавання ўласнасці ў сучаснасці і будучыні.

Галоўнымі ў гэтым выпадку з'яўляюцца ўсе службы, якія забяспечваюць інавацыйнае развіццё прадпрыемства. Інавацыі з'яўляюцца неабходнай умовай захавання канкурэнтаздольнасці прадпрыемства і

вызначаюць яго інвестыцыйную палітыку, мэтай якой з'яўляецца нарошчванне каштоўнасці ўласнасці.

Нарошчванне каштоўнасці прадугледжвае такую змену архітэктуры прадпрыемства, пры якой эфектыўнасць выкарыстання ўласнасці павялічваецца ці як мінімум не памяншаецца (у выпадку неспрыяльнага стану навакольнага асяроддзя).

Такім чынам, падыход, заснаваны на барацьбе з пагрозамі, па эфектыўнасці павінен быць заведама ніжэйшы, чым падыход, заснаваны на захаванні ўласнасці і эфектыўнасці яе выкарыстання.

Пагрозы эканамічнай дзейнасці

Пагроза бяспецы прадпрыемства можа заключацца ў з'яўленні такіх умоў, пры якіх абцяжарана бягучая дзейнасць у якой-небудзь галіне або нават канкрэтнага прадпрыемства. Пад тэрмінам "пагроза" разумеецца любы канфлікт мэт з навакольным асяроддзем або ўнутранай структурай і алгарытмамі функцыянавання.

Рэальна ці патэнцыйна магчымыя дзеянні ці ўмовы наўмыснага ці выпадковага (ненаўмыснага) парушэння рэжыму функцыянавання прадпрыемства шляхам нанясення матэрыяльнай (прамой ці ўскоснай) шкоды, якая прыводзіць да фінансавых страт, уключаючы і выпушчаную выгаду. Патэнцыйна магчымыя або рэальныя падзеі, працэсы, абставіны або дзеянні зламыснікаў, здольныя нанесці маральную, фізічную або матэрыяльную шкоду.

Такое развіццё падзей, дзеянне (бяздзеянне), у выніку якіх з'яўляецца магчымасць або павышаецца верагоднасць парушэння нармальнага функцыянавання прадпрыемства і недасягнення ім сваіх мэт, у прыватнасці нанясення прадпрыемству любога віду ўрону.

Першы пункт гледжання напрамую не звязвае пагрозу з нанясеннем шкоды, а толькі выяўляе супярэчнасці паміж мэтамі і магчымасцямі іх

дасягнення, з аднаго боку, і станам навакольнага асяроддзя і архітэктуры прадпрыемства – з другога.

Вынікам з'яўляецца вызначэнне дасягальных мэт, выбар адэкватных сродкаў іх рэалізацыі пры неадпаведнасці гэтым мэтам унутранай структуры, якая мае патрэбу ў пастаяннай трансфармацыі, і дынамічным навакольным асяроддзем. Таму планаванне – гэта працэс, які і накіраваны на ліквідацыю названых неадпаведнасцяў.

Рынак – гэта перманентны канфлікт, у тым ліку і паміж вытворцамі. Таму ў прадпрыемства заўсёды існуюць некаторыя абмежаванні, якія неабходна ўлічваць пры планаванні сваёй дзейнасці. Гэта не толькі абмежаванні па магчымасцях рэалізацыі, даступным рэсурсам і рынкам збыту, заканадаўчыя абмежаванні, абмежаванні, але і дыктуемыя канкурэнтнай барацьбой.

Пры планаванні дасягнення мэт сваёй дзейнасці неабходна ўлічваць рэальнасць іх дасягнення, што не заўсёды магчыма з-за суб'ектыўнага пункту гледжання на магчымасці іх рэалізацыі. Магчымасці рэалізацыі любога плана носяць імавернасны характар. Яны маюць тую ці іншую ступень рызыкі.

І з пункту гледжання ацэнкі існуючых абмежаванняў дзейнасці, і з пункту гледжання ўліку нявызначанасці будучыні заўсёды існуе рызыка панесці страты, як у выглядзе страчанай фінансавай выгады, так і рэальныя, што і разглядаецца як пагроза эканамічнай бяспецы.

Дадатным з'яўляецца канстатаванне таго факта, што архітэктура і дзеянні мэнэджменту самі па сабе могуць несці пагрозу прадпрыемству. Такім чынам, можна прыйсці да разумення таго, што кіраўніцкія рашэнні, якія прымаюцца і рэалізуюцца мэнэджментам, таксама могуць выклікаць пагрозу для прадпрыемства.

Другі пункт гледжання вызначае вынік дзеяння пагрозы, бо фіксуе яе наяўнасць толькі пасля нанясення ўрону прадпрыемству. Трэці пункт гледжання адзначае, што пагроза не абавязкова прыводзіць да наступстваў у выглядзе парушэння функцыянавання прадпрыемства і нанясення шкоды.

Чацвёрты пункт гледжання толькі дадае імавернасны характар пагрозы, не змяняючы, па сутнасці, падыходу.

Пад пагрозай прапануецца разумець магчымасць неспрыяльнага ўздзеяння на стан ці вынікі дзейнасці прадпрыемства. Будучы колькасна вымераная, пагроза можа разглядацца як рызыка. Такім чынам, рызыка з'яўляецца колькаснай ацэнкай пагрозы, у сваю чаргу, пагроза – гэта якаснае вызначэнне рызыкі.

Рызыка характарызуе нявызначанасць умоў і вынікаў дзейнасці, а пагроза – гэта магчымасць негатыўнага развіцця падзей. Трэба адрозніваць сітуацыю пагрозы і рызыкі ад іх рэалізацыі. Рэалізацыя пагрозы – гэта рызыка або загадзя вядомы сцэнар неспрыяльнага развіцця падзей, які пачаў рэалізоўвацца па непажаданым варыянце, адпаведна, які выходзіць за рамкі прадугледжанай планаваннем нявызначанасці ўмоў дзейнасці.

Эканамічная бяспека характарызуецца сістэмай абароны эканамічных інтарэсаў ад неспрыяльных макраэканамічных фактараў, дэструктыўных паводзін уласнікаў, партнёраў ці канкурэнтаў.

Эканамічная бяспека характарызуецца сістэмай метадаў абароны эканамічных інтарэсаў прадпрыемства, якія поўнасцю адпавядаюць дзеючаму заканадаўству. Эканамічная бяспека, якая забяспечваецца нелегітымнымі метадамі, характарызуецца сістэмай метадаў абароны эканамічных інтарэсаў прадпрыемства ад пагроз, якія супярэчаць дзейным прававым нормам.

Галоўным у забеспячэнні эканамічнай бяспекі прадпрыемства з'яўляецца захаванне ўласнасці. Асноўная частка даследаванняў эканамічнай бяспекі з дадзенага пункта гледжання прысвечана выяўленню і прадухіленню парушэнняў заканадаўства ў кіраванні прадпрыемствам. Пры гэтым лічыцца, што эканамічную бяспеку можа забяспечыць асобнае структурнае падраздзяленне – служба бяспекі.

Таму асноўная ўвага засяроджана на апісанні структур і функцый службаў бяспекі, сістэм бяспекі, а таксама комплексных падыходаў да

сфармуляванай такім чынам праблемы. Такі падыход валодае практычнай карыснасцю, асабліва ў той частцы, якая датычыцца метадычных рэкамендацый, якія можна рэалізаваць.

Асноўным напрамкам лічыцца таксама кіраванне прадпрыемствам. У якасці крытэрыю выкарыстоўваецца ступень дасягнення мэт. Пры не дасягненні пастаўленых мэт лічыцца, што эканамічная бяспека прадпрыемства не забяспечваецца. Стан эканамічнай бяспекі прадпрыемства ацэньваецца з пазіцыяў яго канкурэнтаздольнасці; стратэгічнай устойлівасці; фінансавай устойлівасці.

Дзеянні службы бяспекі не могуць яе забяспечыць. Гэта выцякае з таго факта, што гэтая служба падпарадкавана першай асобе прадпрыемства (дырэктару). А гэта служба бяспекі прадухіліць не можа.

Асноўныя функцыі, якія нясе дадзеная служба, датычыцца кантролю дзеянняў персаналу з пункту гледжання выканання заканадаўства, рэжыму работы прадпрыемства, аховы матэрыяльна-тэхнічных каштоўнасцей, інтэлектуальнай уласнасці, нематэрыяльных актываў. Але гэтага відавочна недастаткова, каб гарантаваць эканамічную бяспеку прадпрыемства ў шырокім разуменні.

Межы прадпрыемства і юрыдычнай асобы на практыцы могуць не супадаць. З пункту гледжання ўласніка і мэнэджара, пад фінансава-гаспадарчай дзейнасцю прадпрыемства разумеецца дзейнасць прадпрыемства, яго падраздзяленняў і супрацоўнікаў ва ўзаемаадносінах з навакольным асяроддзем і паміж сабой, якая прыводзіць або патэнцыйна здольная прывесці да змены актываў і пасіваў прадпрыемства, т. е. уласнасці. У працэсе дзейнасці прадпрыемства ўвесь час захоўваюцца эканамічныя адносіны з уласнікам, персаналам, дзяржавай, партнёрамі і кліентамі.

Небяспекі ценявой эканомікі

Прававое рэгуляванне працэсаў эканамічнай бяспекі ўключае сістэму замацаваных нормамі права ўмоў, якія ўстанаўліваюць парадак дзеянняў

суб'ектаў гаспадарання і эканамічных адносін паміж імі, накіраваных на дасягненне пастаўленых мэт.

Па сваёй сутнасці эканамічная бяспека з'яўляецца адной з форм праяўлення ўсеагульнага імкнення суб'ектаў гаспадарання да стабільнасці і надзейнасці на прынцыпах свабоды, вызначанай адпаведнымі законамі, у якіх канцэнтруюцца інтарэсы асобы, калектыву, дзяржавы.

Гэтыя два бакі прававога забеспячэння эканамічнай бяспекі цесна ўзаемазвязаны адзін з адным, таму што змест любога закона заключаецца ў вызначэнні правоў і абавязкаў фізічных і юрыдычных асоб на ўмовах прымусу, які суправаджаецца асаблівасцямі, якія выходзяць з эканамічных інтарэсаў дзяржавы і грамадства на аснове прынцыпаў права.

Прынцыпы права па забеспячэнні эканамічнай бяспекі адлюстроўваюцца ў яго нормах і з'яўляюцца асновай прававога забеспячэння арганізацыі і дзейнасці суб'ектаў гаспадарання. Да прынцыпаў юрыдычнага характару, якія непасрэдна адносяцца да праблемы забеспячэння эканамічнай бяспекі, можна аднесці:

− агульнаабавязковасць выканання ўсім насельніцтвам дзяржавы норм права;

− адсутнасць супярэчлівасці ў нормах права, якія складаюць сістэму па забеспячэнні эканамічнай бяспекі;

− адпаведнасць аб'ектыўных норм права суб'ектыўным, а таксама норм права прававым адносінам;

− падзел на заканадаўчым узроўні права на яго віды (публічны і прыватны);

− роўнасць перад законам і судом усіх без выключэння асоб;

− адказнасць і абумоўленасць паводзін фізічных і юрыдычных асоб у рамках, вызначаных законамі;

− справядлівасць, выяўленая ў роўнай юрыдычнай адказнасці і суразмернасці дапушчаным правапарушэнням;

− гуманнасць пакарання, якое садзейнічае выпраўленню асуджаных.

Хаця эканамічная бяспека набыла новае значэнне ў сусветнай эканоміцы, яна непарыўна звязана з такімі паказчыкамі, як эканамічны рост, стабільнасць сацыяльна-эканамічнай сістэмы, дзяржаўныя даходы, падатковая база, дзяржаўны доўг і інфляцыя, а таксама беспрацоўе.

Эканамічны рост не можа быць устойлівым без дынамічнага развіцця эканомік іншых краін. Пакуль эканоміка не будзе развівацца, не будзе адэкватнага адказу на вонкавыя і ўнутраныя пагрозы. Здольнасць эканомікі выжыць у складаных сітуацыях застанецца абстрактнай.

Сістэма паказчыкаў для ацэнкі ўзроўню эканамічнай бяспекі і вызначэння іх нарматыўных значэнняў важна ў дзяржаўнай эканамічнай палітыцы. Паказчыкі ўзроўню эканамічнай бяспекі краіны і іх парогавыя значэнні зацвярджаюцца на ўрадавым узроўні.

Стан эканамічнай бяспекі ацэньваецца сістэмай аб'ектыўных крытэрыяў і паказчыкаў, якія вызначаюць гранічныя памеры функцыянавання эканамічнай сістэмы. Калі гэтыя памеры перавышаюцца, сістэма страчвае здольнасць дынамічна развівацца, становіцца неканкурэнтаздольнай на знешніх і ўнутраных рынках, становіцца аб'ектам экспансіі транснацыянальных карпарацый, нацыянальнае багацце краіны разрабуецца як унутры краіны, так і за яе межамі, і яна пакутуе ад карупцыі.

На эканамічную бяспеку дзяржавы ўплывае аб'ём ценявой эканомікі. Ценявую эканоміку можна характарызаваць па маштабах і яе дэструктыўнай ролі. Рост ценявой эканомікі вядзе да скарачэння дзяржаўных даходаў за кошт змяншэння падатковай базы. Гэта, у сваю чаргу, прыводзіць да зніжэння якасці сацыяльна-эканамічных умоў у цэлым.

Ценявая эканоміка – гэта пэўная эканамічная дзейнасць, якая ажыццяўляецца на тэрыторыі дзяржавы з мэтай ухілення ад выплаты падаткаў і афіцыйна не ўлічваецца. Таму яе развіццё мае негатыўнае ўздзеянне на сацыяльна-эканамічнае становішча. Вывучэнне прычын узнікнення і развіцця ценявой эканомікі ў грамадстве пачалося яшчэ з

мінулага стагоддзя. Таму што доля ценявой эканомікі ў вытворчасці тавараў і паслугах у гэтым перыядзе ўзрасла.

Практыка даказала, што існуюць два ўзаемазвязаныя прыватныя аспекты ценявой эканомікі:

– здзяйсняць супрацьпраўныя дзеянні з мэтай атрымання некантралюемага асабістага даходу;

– хаваць ад кантролю ўсе ці частку даходаў, атрыманых у выніку дзейнасці, з мэтай атрымання дадатковага асабістага даходу.

Незалежна ад ступені развіцця эканомікі, існаванне такіх сітуацый выклікае павелічэнне колькасці негатыўных сацыяльна-эканамічных наступстваў у грамадстве.

Сёння як ніколі вялікае значэнне набываюць празрыстасць і легальнасць аперацый у нацыянальных фінансавых сістэмах. З гэтай прычыны вельмі важна стварыць дзейсныя механізмы супрацьдзеяння ценявой эканоміцы і карупцыі, каб не толькі абараніць працаздольнасць фінансавай сістэмы краіны, але і забяспечыць належнае выкарыстанне дзяржаўных сродкаў.

У дадзеным кантэксце ставяцца задачы пашырыць выкарыстанне іншых дадзеных і вялікіх дадзеных (Big Data) для выяўлення незарэгістраваных падаткаплацельшчыкаў і транзакцый.

Для павышэння эфектыўнасці падатковага кантролю стварыць бескантактавыя цэнтры па абмене інфармацыяй паміж падатковымі органам, грамадзянамі і бізнесам. Пашырыць магчымасці цэнтраў апрацоўкі даных у падатковых і мытных органах у атрыманні інфармацыі аб транзакцыях.

Лічбавая эканоміка

Уведзены Д. Тапскоттам тэрмін «лічбавая эканоміка» і распаўсюджаны дзякуючы навуковым пошукам Н. Неграпонтэ ў цяперашні час атрымаў

шырокае распаўсюджванне, у тым ліку за кошт яго практычнага ўкаранення ў дзелавую прастору кампаній Deloitte і IBM.

Лічбавая эканоміка з пазіцый эканамічнай навукі можа быць прадстаўлена як пэўны від эканамічных адносін, якія ўзнікаюць у працэсе вытворчасці, размеркавання, абмену або спажывання, якія набываюць тэхналагічны характар дзякуючы выкарыстанню інфармацыйна-камунікацыйных і інтэрнэт – тэхналогій, якія садзейнічаюць стварэнню віртуальнага асяроддзя, якое дапаўняе рэальнасць.

У сярэдзіне XX стагоддзі, пад лічбавымі тэхналогіямі разумеліся тэхналогіі, у якіх інфармацыя пераўтворыцца ў перарывісты дыскрэтны набор дадзеных, які складаецца з 0 (няма сігналу) і 1 (ёсць сігнал).

Іх супрацьпастаўлялі аналагавым тэхналогіям, дзе дадзеныя – гэта бесперапынны струмень электрычных рытмаў рознай амплітуды з неабмежаваным лікам значэнняў.

Пазней на змену гэтаму прыйшло іншае азначэнне. Лічбавыя тэхналогіі – гэта тэхналогіі, дзе інфармацыя прадстаўляецца ва ўніверсальным лічбавым выглядзе. Іншы варыянт – гэта ўсё тэхналогіі, якія дазваляюць ствараць, захоўваць і распаўсюджваць дадзеныя.

У аналагавых тэхналогіях інфармацыя не уніфікавана. Яна захоўваецца і перадаецца ў розных фарматах, пад кожны тып носьбіта. Да прыкладу, стацыянарны тэлефон – гэта аналагавая тэхналогія, а смартфон з інтэрнэтам – ужо лічбавая. Да лічбавых тэхналогій адносяць усё тое, што звязана з электроннымі вылічэннямі і пераўтварэннем даных: гаджэты, электронныя прылады, тэхналогіі, праграмы.

У параўнанні з аналагавымі тэхналогіямі, лічбавыя тэхналогіі лепш падыходзяць для захоўвання і перадачы вялікіх масіваў дадзеных. Яны забяспечваюць высокую скорасць вылічэнняў. Пры гэтым інфармацыя перадаецца максімальна дакладна, без скажэнняў. Сярод галоўных недахопаў – высокая энергаёмістасць і негатыўнае ўздзеянне на клімат.

На долю дата – цэнтраў прыпадае каля 0,3 працэнта сусветных выкідаў вугляроду. Яны спажываюць каля 200 ТВтч у год – гэта больш, чым гадавое спажыванне энергіі ў краінах, што развіваюцца. Да 2030 года гэты паказчык можа вырасці да 20 працэнтаў ад усяго сусветнага попыту, што прывядзе да істотнага павелічэння выкідаў.

Лічбавыя тэхналогіі часта блытаюць з інфармацыйнымі тэхналогіямі. Да інфармацыйных тэхналогій адносяцца тэхналогіі, звязаныя з абменам інфармацыяй з дапамогай аналагавых прылад.

Практычна ў любым бізнэсе выкарыстоўваюць CRM, анлайн-сэрвісы для выдаленай працы, захоўванні і працы з кліенцкай базай, кіравання бухгалтэрыяй і таварнага ўліку. Усё больш кампаній выкарыстоўваюць вялікія дадзеныя і аналітыку, заснаваную на іх, каб развіваць бізнэс і нарошчваць кліенцкую базу.

У адукацыі выкарыстоўваюцца гаджэты і праграмы для дыстанцыйнага навучання, падрыхтоўкі і выканання дамашніх заданняў, складання прэзентацый, праграміравання і творчых задач. Віртуальная і дапоўненая рэальнасць дапамагаюць лепш успрымаць матэрыял і робяць навучанне больш інтэрактыўным. ІІ-алгарытмы дапамагаюць з прафарыентацыяй і навучальным працэсам.

У медыцыне лічбавыя тэхналогіі дапамагаюць хутчэй знаходзіць новыя лекі і вакцыны, дакладней ставіць дыягназ нават на ранніх стадыях, збіраць аналітыку для прагназавання захворванняў, праводзіць анлайн-кансультацыі і нават аперацыі з ужываннем AR і робатаў.

У рэтэйле лічбавыя тэхналогіі спрашчаюць працэс пошуку і замовы тавараў, кіравання складам і дастаўкай. Аналіз паводзінаў пакупнікоў і даныя аб перамяшчэнні па гандлёвых залах дапамагаюць аптымізаваць прастору магазіна. Галасавыя памочнікі і чат-боты апрацоўваюць запыты з максімальнай хуткасцю, а афлайнавыя крамы ўжо пачынаюць працаваць без кас і прадаўцоў - пры дапамозе камер і алгарытмаў распазнання асоб.

У сегменце забаў лічбавыя тэхналогіі адкрываюць неабмежаваныя магчымасці для гульняў, пакупкі і чытанні кніг, праслухоўвання музыкі і прагляду Full HD відэа онлайн, на стрымінгавых сэрвісах. Нейронныя сеткі ўдзельнічаюць у стварэнні музыкі, жывапісу і кніг, а віртуальныя акцёры і музыканты замяняюць сапраўдных акцёраў.

На вытворчасці з дапамогай тэхналогій аўтаматызуюць асобныя лініі і цэлыя заводы, распрацоўваюць новыя мадэлі і матэрыялы, сочаць за бяспекай і экалогіяй, прагназуюць адмовы абсталявання, прадухіляюць шлюб і траўмы, аптымізуюць працоўны час і рэсурсы.

Лічбавыя тэхналогіі ўдзельнічаюць у зборы і размеркаванні заказаў, падрыхтоўцы страў, кантролі за колькасцю і тэрмінамі захоўвання прадуктаў і нават дапамагаюць знаходзіць новыя кропкі з максімальным трафікам.

У ліку найбольш значных лічбавых тэхналогій вылучаюць глыбокае навучанне, згортачныя нейронавыя сеткі, камп'ютэрны зрок, навучанне з падмацаваннем, апрацоўку натуральнай мовы, рэкурэнтныя нейронавыя сеткі, трансфернае навучанне, генератыўныя спаборныя сеткі, сістэмы падтрымкі прыняцця рашэнняў, смарт-кантракты і распазнанне прамовы.

Большасць тэхналогій мае дачыненне да штучнага інтэлекту, нейронавых сетак і машыннага навучання.

Смартфоны аб'ядналі ў сабе персанальны кампутар і тэлефон, стаўшы ёмішчам для дзясяткаў лічбавых тэхналогій. Інтэрнэт рэчаў – гэта тэхналогія, якая дазваляе аб'ядноўваць сэнсары, гаджэты, бытавую тэхніку і нават аўтамабілі ў адзіную сетку пры дапамозе бесправадной сувязі. Усімі гэтымі прыладамі можна кіраваць пры дапамозе прыкладанняў і аб'ядноўваць іх у разнастайных аўтаматычных сцэнарах – напрыклад, кіраваць завадскім абсталяваннем.

Вялікія перспектывы для IoT адкрывае новы стандарт бесправадной сувязі – 5G. З яго дапамогай дадзеныя можна перадаваць хутчэй, без збояў і з мінімальнымі затрымкамі, падлучаючы яшчэ больш прылад. 5G дае

шырокапалосную мабільную сувязь на высокай хуткасці і з мінімальнай затрымкай сігналу – усяго 1-2 мс.

Часцей за ўсё пад «штучным інтэлектам» маюць на ўвазе любыя алгарытмы, якія вырашаюць якія-небудзь задачы незалежна ад чалавека: вырабляюць складаныя вылічэнні, распазнаюць выявы і гаворка, збіраюць і апрацоўваюць масівы дадзеных. Але сапраўдны «штучны інтэлект» – той, што не толькі сам вырашае задачы, але і ставіць новыя, сам прымае рашэнні і выходзіць за рамкі сваіх першапачатковых магчымасцяў.

Каб ІІ мог дзейнічаць самастойна, ужываюць алгарытмы машыннага і глыбокага навучання, а таксама канструююць нейронавыя сеткі па аналогіі з сістэмамі нейронаў у чалавечым мозгу. ІІ знаходзіць патрэбную інфармацыю, рэкамендуе прыдатныя тавары ці відэа, будуе аналітычныя прагнозы, дапамагае лячыць пацыентаў і кіраваць беспілотнікамі.

У адукацыі віртуальнае асяроддзе дапамагае навочна вывучыць анатомію, архітэктуру ці старажытныя цывілізацыі. У медыцыне, з ужываннем дапоўненай і змешанай рэальнасцяў, праводзяць анлайн-кансіліумы і аперацыі.

З дапамогай VR можна наведваць іншыя краіны і славутасці, музеі і нават патанулыя караблі. Падчас пандэміі сталі запатрабаваны распрацоўкі, якія дазваляюць праводзіць сустрэчы ў AR і VR.

3D-друк можа замяніць большую частку вытворчых тэхналогій і матэрыялаў. На 3D-друкарках друкуюць дэталі і запчасткі, кабелі, мэблю і фурнітуру, адзенне і абутак і нават дома. У медыцыне карыстаецца папулярнасцю тэхналогія біяпрынтынгу. Калі на 3D-друкарках, са спецыяльнага біягеля друкуюць чалавечыя тканіны і органы.

Першыя прататыпы рабатызаваных прылад з'явіліся яшчэ ў XIX стагоддзі, а ў другой палове XX стагоддзі рабатызацыя выйшла на прамысловы ўзровень. Робатаў выкарыстоўваюць для зборкі машын і электронікі, лагістыкі, кур'ерскай дастаўкі, прыгатавання страў і нават хірургічных аперацый.

Хмарныя тэхналогіі заснаваны на размеркаваным сеткавым доступе да IT-інфраструктуры, каб захоўваць і апрацоўваць дадзеныя любога аб'ёму. Як правіла, гэта выдаленыя серверы ці IT-сэрвісы, якія можна арандаваць па меры неабходнасці.

Такі падыход дазваляе кампаніям хутка нарошчваць вылічальныя магутнасці, запускаць або маштабаваць анлайн-праекты, якія патрабуюць вельмі вялікіх рэсурсаў. Ёсць тры віды хмарных сэрвісаў: IaaS, infrastructure as a service – інфраструктура як паслуга.

Калі карыстачы арандуюць серверы, працэсары і іншыя прылады для захоўвання і апрацоўкі дадзеных, могуць усталёўваць на іх свае АС і ПА для апрацоўкі дадзеных.

Правайдэр падае АС, на якой карыстачы могуць усталёўваць свае прыкладанні і запускаць новыя сэрвісы. Карыстальнік атрымлівае доступ да ўсіх прыкладанняў правайдэра для захоўвання, апрацоўкі і перадачы дадзеных.

Блокчейн – гэта тэхналогія, пры якой дадзеныя аб усіх здзяйсняных транзакцыях захоўваюцца ў адзінай сістэме ў выглядзе асобных блокаў і засведчваюцца лічбавым подпісам, якая абараняе ад узлому. База дадзеных у сістэме – размеркаваная паміж усімі ўдзельнікамі, гэта значыць без якога-небудзь цэнтралізаванага кіравання і кантролю. Гэта робіць яе, па меркаванні стваральнікаў, найболей незалежнай, бяспечнай і ўстойлівай да карупцыі.

У блокчейне выкарыстоўваюцца токены – неўзаемазаменныя, унікальныя сутнасці, – а таксама смарт-кантракты – алгарытмы для фарміравання, кантролю і прадастаўлення інфармацыі аб валоданні чым-небудзь (напрыклад, криптовалютой). Першы блок быў згенераваны ў 2009 годзе. Існуе больш за 2 тыс. розных сістэм блокчейна.

Адна з апошніх мадыфікацый – тэхналогія NFT, якую ўжываюць для продажу твораў мастацтва, музычных трэкаў і іншых відаў інтэлектуальнай уласнасці. Кожнаму малюнку, відэа ці аўдыё прысвойваецца унікальны лічбавы сертыфікат, які можна купіць, каб стаць уладальнікам твора. NFT

можна перапрадаваць, зарабляючы на гэтым як на фізічных прадметах мастацтва.

Крыптавалюта – цалкам лічбавая валюта, створаная па тэхналогіі блокчейна, якая выкарыстоўваецца для віртуальнага абмену і плацяжоў. Яна не залежыць ад банкаў ці іншых фінансавых структур. Для яе абароны, абмену і кантролю аперацый ужываюць адмысловыя метады шыфравання.

Тэхналогіі блокчейна ў найбліжэйшай будучыні могуць прывесці да з'яўлення поўнасцю аўтаномнай фінансавай сістэмы, якая не будзе залежаць ад дзяржаўных і міжнародных фінансавых інстытутаў. Магчыма, узнікне нават нешта накшталт лічбавай дзяржавы або віртуальнага сусвету, са сваімі ўнутранымі рынкамі і законамі.

Бліжэйшыя гады – пераломны перыяд лічбавай трансфармацыі, калі digital-тэхналогіі ахопяць нават тыя сферы, дзе заўсёды панавалі аналагавыя тэхналогіі. Дзяржаўныя, фінансавыя, медыцынскія паслугі пераходзяць у анлайн-фармат, з'яўляюцца першыя прататыпы электронных пашпартоў і лічбавыя плацежныя сістэмы без прывязкі да фізічных валют і банкаў.

Сінэргія лічбавых тэхналогій дапаможа аб'яднаць афлайн і анлайн, робячы ўсе прылады і сэрвісы ўзаемазлучанымі паміж сабой. Штучны інтэлект і вялікія дадзеныя дапамагаюць прымаць больш абгрунтаваныя рашэнні, а VR і AR – праводзіць складаныя аперацыі, падарожнічаць і вучыцца ў любым пункце.

Ацэньваючы маштабы цыфравізацыі, даследнікі прыходзяць да высновы, што лічбавую эканоміку можна разглядаць як які развіваецца хуткімі тэмпамі сегмент гаспадарчай сістэмы, у якім традыцыйныя эканамічныя сувязі і мадэлі кіравання бізнэс-працэсамі замяняюцца і дапаўняюцца новымі электроннымі тэхналогіямі вытворчасці, абмену і спажыванні.

Тэхніка-тэхналагічнае, лічбавае і сацыяльна-эканамічнае развіццё грамадства генеруе новыя пагрозы і рыскі. Таму пытанні забеспячэння

эканамічнай бяспекі становяцца больш вострымі і жыццёва важнымі, якія патрабуюць пільнага вывучэння з навуковых пазіцый.

Метадалогія эканамічнай бяспекі дазваляе ідэнтыфікаваць рызыкі з адрозненнямі ў іх дапушчальных узроўнях у залежнасці ад кіравальнасці і прагназуемасці, а таксама магчымых наступстваў іх наступлення. Гэта дазваляе разглядаць катэгорыю "эканамічная бяспека" як кіраваную рызыку для тых суб'ектаў, якія прымаюць рашэнні.

Ва ўмовах інтэнсіўнага развіцця інфармацыйных сістэм і тэхналагічных рашэнняў неразвітыя інстытуты могуць стаць істотным фактарам стрымлівання тэмпаў лічбавага развіцця і стварыць умовы для ўзнікнення новых рызык эканамічнай бяспекі.

Аснову лічбавай эканомікі як новай сістэмы эканамічных адносін складаюць інструменты цыфравізацыі гаспадарчай дзейнасці, інфармацыйна-камунікацыйныя сэрвісы і тэхналогіі, скразныя лічбавыя інструменты, тэхналогіі фізічнай і дапоўненай рэальнасці, сеткі P2P, а таксама віртуальныя механізмы фінансавай сферы.

Дзеянне паказаных інструментаў і тэхналогій уплывае на традыцыйныя эканамічныя цыклы, змяняючы паслядоўнасць і характар праходжання вытворчых працэсаў і фармуючы ўмовы для стварэння дадатковага кошту праз генерацыю лічбавых эканамічных выгод.

Інстытуцыйная інфраструктура лічбавай эканомікі

Д. Норт звярнуў увагу на тое, што новыя інстытуты ўзнікаюць у тым выпадку, калі грамадства адчувае патрэбнасць у павелічэнні даходаў, аднак існуючая інстытуцыйная сістэма аказваецца не здольнай гэта забяспечыць. Любая інстытуцыйная змена накладвае на кожнага ўдзельніка адносін новыя абмежаванні. Узнікла новая праблематыка інстытуцыйнага асяроддзя і новыя ўзнікаючыя абмежаванні ва ўмовах цыфравізацыі. Гэта:

1) стаўленне да манапалістычных эфектаў платформаў і іерархій: неэфектыўнасць барацьбы рэгулятара з усталяваннем манапольнай улады платформаў, неабходнасць яе пераарыентацыі на ўхіленне якія ўзнікаюць правалаў рынка.

2) змяненне правілаў рэгулявання лічбавых кампаній у напрамку замены ліцэнзій на рэгуляванне ex post або самарэгуляванне;

3) з прычыны негатыўнага ўплыву сістэмы дзяржаўнай стандартызацыі на колькасць патэнтаў абумоўліваецца неабходнасць пабудовы новай сістэмы стандартызацыі з улікам меркаванняў незалежных гульцоў на рынку і самарэгулявальных арганізацый. У сваю чаргу, змена абмежаванняў выклікае трансфармацыю прыярытэтаў і перагляд каштоўнасці ажыццяўлення той ці іншай дзейнасці.

Напрыклад, у звычайнай мадэлі кантрактаў Уільямсана – Макнейла выдзелены класічныя (здзелкі), неакласічныя (кааперацыя з пасярэднікам) і адносіны кантракты (фірмы). Пры гэтым характар актываў выступае галоўным фактарам выбару кшталту кантрактаў.

Нараўне з гэтым ва ўмовах цыфравізацыі ўзнікаюць новыя выгляды кантрактаў, такія як: кантракт жыццёвага цыклу прадукта на аснове sharing, smart-кантракты з выключэннем арбітра, кантракты глабалізаванага аўтсорсінгу для «самазанятых».

Менавіта таму прыярытэты суб'ектаў гаспадарання будуць перамяшчацца ў бок заключэння новых відаў кантрактаў і росту попыту на новыя віды абароны кантрактаў (напрыклад, абарона інтэлектуальнай уласнасці ў сувязі з лічбавым пірацтвам, абарона асабістай інфармацыі).

Такім чынам, ва ўмовах станаўлення лічбавай эканомікі адэкватнасць і адаптыўнасць фармальных і нефармальных інстытутаў будзе вызначаць узнікненне станоўчых або адмоўных эфектаў цыфравізацыі. Дадатныя эфекты цыфравізацыі можна ўмоўна падзяліць на тэхналагічныя, эканамічныя і сацыяльныя эфекты.

Гэта можа быць новая мадэль лічбавага бізнесу, якая дзякуючы выкарыстанню інфармацыйных тэхналогій здольна маштабавацца ў глабальных маштабах і ахопліваць індывідаў, гаспадарчых суб'ектаў і прадметы іх узаемадзеяння (тавары і паслугі) праз эфектыўнае персанальнае абслугоўванне.

Да станоўчых эканамічных эфектаў цыфравізацыі адносяць: пашырэнне гандлёвых рынкаў і аперацый; рост прадукцыйнасці працы шляхам скарачэння выдаткаў у розных сферах эканомікі; развіццё канкурэнцыі; павелічэнне колькасці працоўных месцаў у сумежных галінах; павышэнне якасці паслуг.

Развіццё лічбавай эканомікі пры наяўнасці спрыяльнага інстытуцыйнага асяроддзя стымулюе эканамічны рост і стварае ўмовы для паскарэння яго тэмпаў. Прылады, якімі аперуе лічбавая эканоміка, дазваляюць кампаніям гнутка рэагаваць на змену рынкавай кан'юнктуры, якасней і хутчэй задавальняць якія ўзнікаюць запатрабаванні спажыўцоў.

Развіццё сістэм электронных плацяжоў садзейнічае шматразоваму паскарэнню руху фінансавых патокаў, з'яўляецца крыніцай стымулявання міжнароднага тавараабмену. Традыцыйныя кампаніі пераходзяць у фармат анлайн-работы, а таксама ўсё часцей ужываюць інструменты электроннага гандлю, тым самым забяспечваючы паскарэнне эканамічнага развіцця.

Відавочныя і станоўчыя сацыяльныя эфекты цыфравізацыі: павышэнне інклюзіўнасці і зніжэнне ўзроўню беднасці; павышэнне даступнасці і рост якасці медыцынскага абслугоўвання; зніжэнне кошту і павышэнне даступнасці масавай адукацыі; паляпшэнне экалагічнай сітуацыі; павышэнне даступнасці фінансавых сэрвісаў; скарачэнне ўзроўню злачыннасці; скарачэнне працоўнага часу і павелічэнне часу вольнага часу работнікаў.

Работнікі ў 10 найбольш канкурэнтаздольных эканоміках GCI 4.0 працуюць у сярэднім на 361 гадзіну менш за год, чым у 10 краінах з самым нізкім рэйтынгам, для якіх існуюць дадзеныя аб працоўным часе.

Сэнс лічбавай трансфармацыі – у радыкальным зніжэнні ўзроўню трансакцыйных выдаткаў і змене іх структуры. Менавіта гэты факт забяспечвае поспех шматлікіх лічбавых кампаній і праектаў ад кампаній у сектары sharing economy да прыватных блокчейн-ланцугоў.

Гэта звязана са значным зніжэннем затрат на збор і апрацоўку інфармацыі. Аднак кардынальнае зніжэнне трансакцыйных выдаткаў спрыяе пашырэнню варыянтаў абмену і выклікае з'яўленне новых дыскрэтных інстытуцыйных альтэрнатыў. У выніку гэтага фармуецца "эфект накладання": адначасовае нарастанне магчымасцяў і з'яўленне канфліктнасці развіцця.

Запускаецца рост выдаткаў кожнай групы суб'ектаў з прычыны залішняй інстытуцыйнай нагрузкі, а таксама ўзнікае рэгулятыўны арбітраж, гэта значыць рэгуляванне падобных відаў эканамічнай дзейнасці з рознай ступенню інтэнсіўнасці. Названыя заканамернасці прыводзяць да ператоку бізнес-структур у сферы эканамічнай дзейнасці з больш нізкай рэгулятыўнай нагрузкай. Такая сітуацыя можа ўзнікнуць ва ўмовах інстытуцыйнай няспеласці на рынку крэдытавання паміж банкаўскімі структурамі і мікра крэдытнымі арганізацыямі.

Гэта выклікае скарачэнне маштабаў інстытуцыяналізаванага рынку, падзенне плацежаздольнага попыту, зніжэнне аб'ёму выручкі, масавы сыход з рынку "гульцоў" (з нявыкананымі абавязацельствамі), а таксама ўзмацненне мер нагляду і кантролю з боку рэгулятара (эфект агульнага ўзмацнення рэгулятыўнай нагрузкі). Узнікненне рэгулятыўнага арбітражу напрамую адбіваецца на спажыўцу, аслабляе яго абароненасць і прымушае яго пераглядаць прыярытэты рызык і метады абароны і кіраванні імі.

Кібернетычная злачыннасць і сацыяльная інжынерыя

Адным з адмоўных эфектаў цыфравізацыі стала інтэнсіўнае развіццё кібернетычнай злачыннасці, эканамічная шкода ад якой мае значную

дынаміку росту. Згодна са статыстыкай 2017 года, у ЗША штогод адбываецца больш за 130 буйнамаштабных мэтавых парушэнняў, і гэта колькасць расце на 27% у год. 31% арганізацый падвергліся кібернетычных нападаў на аперацыйную тэхналагічную інфраструктуру.

У 2017 годзе 100 000 гуртоў у 150 краінах і больш за 400 000 машын былі заражаныя вірусам Wannacry. Агульны кошт ад шкоды склаў каля $4 млрд. Напады, звязаныя з крыптам джэкінгам, павялічыліся на 8 500 % у 2017 г. Штодня блакуецца каля 24 000 шкоднасных мабільных прыкладанняў.

Сацыяльная інжынерыя (social engineering) або "атака на чалавека" – гэта сукупнасць псіхалагічных і сацыялагічных прыёмаў, метадаў і тэхналогій, якія дазваляюць атрымаць канфідэнцыйную інфармацыю.

Кібернетычных ашуканцаў, якія выкарыстоўваюць гэтыя прыёмы на практыцы, называюць сацыяльнымі інжынерамі. Спрабуючы знайсці доступ да сістэмы або каштоўных дадзеных, яны выкарыстоўваюць самае ўразлівае звяно – чалавека.

Самы просты прыклад – тэлефонны званок, дзе зламыснік выдае сябе за кагосьці іншага, спрабуючы даведацца ў абанента канфідэнцыйную інфармацыю, гуляючы на пачуццях чалавека, падманваючы або шантажуючы яго. Многія людзі даверліва расказваюць сацыяльным хакерам усё, што ім трэба. А ў арсенале ашуканцаў нямала тэхнік і прыёмаў.

Сацыяльная інжынерыя набыла трывалую сувязь з кібернетычнай злачыннасцю. У пачатку 70-х гадоў XX стагоддзя сталі з'яўляцца тэлефонныя хуліганы, якія парушалі спакой грамадзян проста дзеля жарту. Але хтосьці сцяміў, што так можна дастаткова лёгка атрымліваць важную інфармацыю.

І ўжо да канца 70-х былыя тэлефонныя хуліганы ператварыліся ў прафесійных сацыяльных інжынераў (іх сталі звацьсінжорамі), здольных па-майстэрску маніпуляваць людзьмі, па адной толькі інтанацыі вызначаючы іх комплексы і страхі.

Калі з'явіліся кампутары, большасць інжынераў змяніла профіль, стаўшы сацыяльнымі хакерамі, а паняцці "сацыяльная інжынерыя" і "сацыяльныя хакеры" сталі сінанімічныя.

Прыклад – крадзеж у кампаніі The Ubiquiti Networks 40 мільёнаў долараў у 2015 годзе. Ніхто не ўзломваў аперацыйныя сістэмы і не краў дадзеныя – правілы бяспекі парушылі самі супрацоўнікі. Ашуканцы даслалі электронны ліст ад імя топ-мэнэджара кампаніі і папрасілі, каб фінансісты перавялі вялікую суму грошай на ўказаны банкаўскі рахунак.

У 2007 годзе адна з самых дарагіх сістэм бяспекі ў свеце была ўзламана – без гвалту, без зброі, без электронных прылад. Зламыснік забраў з бельгійскага банка ABN AMRO алмазы на 28 мільёнаў долараў дзякуючы сваёй прывабнасці.

Ашуканец Карлас Гектар Фламенбаум, чалавек з аргенцінскім пашпартам, скрадзеным у Ізраілі, заваяваў давер супрацоўнікаў банка яшчэ за год да інцыдэнту. Ён выдаваў сябе за бізнэсмэна, рабіў падарункі. Аднойчы супрацоўнікі падалі яму доступ да сакрэтнага сховішча каштоўных камянёў, ацэненых у 120 000 каратаў.

Прыклады сацыяльнай інжынерыі сведчаць аб тым, што яна лёгка адаптуецца да любых умоў і да любога становішча. Гуляючы на асабістых якасцях чалавека або адсутнасць прафесійных (недахоп ведаў, ігнараванне інструкцый і гэтак далей), кіберзлачынцы літаральна "узломваюць" чалавека. Атака на чалавека можа адбывацца па шматлікіх сцэнарах, але існуе некалькі найболей распаўсюджаных тэхнік працы зламыснікаў.

Фішынг выкарыстоўвае няўважлівасць. На пошту ахвяры прыходзіць падроблены ліст ад нейкай вядомай арганізацыі з просьбай перайсці па спасылцы і аўтарызавацца. Каб выклікаць больш даверу, ашуканцы прыдумляюць сур'ёзныя прычыны для пераходу па спасылцы: напрыклад, просяць ахвяру абнавіць пароль або ўвесці нейкую інфармацыю (ПІБ, нумар тэлефона, банкаўскай карты і нават CVV-код!).

Тэхналогія траяна выкарыстоўвае такое пачуццё людзей як прагнасць. Вірус нездарма атрымаў сваю назву па прынцыпе працы траянскага каня са старажытнагрэцкага міфа. Толькі прынадай тут становіцца email-паведамленне, якое абяцае хуткі прыбытак і выйгрыш. У выніку чалавек атрымлівае вірус, з дапамогай якога зламыснікі крадуць ягоныя дадзеныя.

Тэхналогія "паслуга за паслугу", ад лацінскага "quid pro quo". Выкарыстоўваючы гэты метад, зламыснік уяўляецца супрацоўнікам службы тэхнічнай падтрымкі і прапануе выправіць узніклыя непаладкі ў сістэме, хоць насамрэч праблем у працы праграмнага забеспячэння не ўзнікала. Ахвяра верыць у наяўнасць няспраўнасцяў і, выконваючы ўказанні хакера, асабіста перадае яму доступ да важнай інфармацыі.

Яшчэ адзін прыём, да якога звяртаюцца кібернетычныя злачынцы, называецца прэтэкстынг. Гэта дзеянне, адпрацаванае па загадзя складзеным сцэнары. Каб завалодаць інфармацыяй, злачынец выдае сябе за вядомую ахвяру асобу, якой нібыта неабходна канфідэнцыйная інфармацыя для выканання важнай задачы.

Сацыяльныя інжынеры прадстаўляюцца супрацоўнікамі банкаў, крэдытных сэрвісаў, тэхнічнай падтрымкі, сябрам і членам сям'і. Для большай дакладнасці яны паведамляюць патэнцыйнай ахвяры якую-небудзь інфармацыю аб ёй: імя, нумар банкаўскага рахунку, рэальную праблему, з якой яна звярталася ў гэтую службу раней. Прыкладам з'яўляюцца чорныя "call-цэнтры", калі зняволеныя пад выглядам супрацоўнікаў буйных банкаў тэлефануюць грамадзянам і падманам прымушаюць перавесці грошы.

Методыка зваротнай сацыяльнай інжынерыі накіравана на тое, каб ахвяра сама звярнулася да сацыяльнага інжынера і выдала яму неабходныя звесткі. Гэта можа дасягацца праз укараненне асаблівага праграмнага забеспячэння. Спачатку праграма ці сістэма працуе спраўна, але потым адбываецца збой, які патрабуе ўмяшання адмыслоўца.

Сітуацыя падстроена такім чынам, каб тым спецыялістам, да якога звернуцца па дапамогу, аказаўся сацыяльны хакер. Наладжваючы працу

праграмнага забеспячэння, ашуканец вырабляе неабходныя для ўзлому маніпуляцыі. А калі ўзлом выяўляецца, сацыяльны інжынер застаецца па-за падазрэннем.

Зламыснікі могуць рэкламаваць свае паслугі як кампутарных майстроў ці іншых спецыялістаў. Ахвяра звяртаецца да ўзломшчыка сама, а злачынец не толькі працуе тэхнічна, але і вывуджвае інфармацыю праз зносіны са сваім кліентам. Калі вы не жадаеце стаць чарговай ахвярай сацыяльных інжынераў, рэкамендуемы выконваць наступныя правілы абароны.

Заўсёды зважайце на адпраўніка лістоў і адрас сайта, дзе збіраецеся ўвесці нейкія асабістыя дадзеныя. Калі гэта пошта на дамене буйной арганізацыі, пераканайцеся, што дамен менавіта такі і ў ім няма памылак друку. Калі ёсць сумневы – звяжыцеся з тэхпадтрымкай або прадстаўніком арганізацыі па афіцыйных каналах.

Не працуйце з важнай інфармацыяй на вачах у старонніх людзей. Ашуканцы могуць выкарыстоўваць так званы плечавы сёрфінг – від сацыяльнай інжынерыі, калі крадзеж інфармацыі адбываецца праз плячо ахвяры – подглядыванием. Не пераходзіце на падазроныя сайты і не спампоўвайце сумнеўныя файлы. Бо адзін з самых лепшых памочнікаў сацыяльнай інжынерыі – цікаўнасць.

Не выкарыстоўвайце адзін і той жа пароль для доступу да знешніх і карпаратыўных працоўных рэсурсаў. Усталюйце антывірус. Ва ўсіх буйных антывірусах ёсць убудаваная праверка на шкоднасныя рэсурсы. Азнаёмцеся з палітыкай канфідэнцыйнасці кампаніі. Усе супрацоўнікі павінны быць праінструктаваны аб тым, як паводзіць сябе з наведвальнікамі і што рабіць пры выяўленні незаконнага пранікнення.

Доксінг

Doxing – гэта скарачэнне ад ангельскіх слэнгавых слоў "drop drop dox" (скінуць дакументы), "dox" (дакументы). Як правіла, доксінг – гэта

зламыснае дзеянне, накіраванае супраць людзей, з якімі зламыснік не згодны або знаходзіцца не ў лепшых адносінах.

Доксінг – гэта раскрыццё ў сетцы ідэнтыфікавалай інфармацыі аб кім-небудзь, такі як сапраўднае імя, хатні адрас, месца працы, нумар тэлефона, фінансавая і іншая асабістая інфармацыя. У далейшым гэтая інфармацыя распаўсюджваецца без дазволу ахвяры.

Хоць раскрыццё асабістай інфармацыі без дазволу ўладальніка мела месца яшчэ да з'яўлення інтэрнэту, тэрмін доксінг упершыню з'явіўся ў хакерскай субкультуры ў 90-х гадах XX стагоддзя, дзе ананімнасць лічылася святой. Супрацьстаянне паміж канкуруючымі хакерамі часам прыводзіла да таго, што адны вырашалі "раскрыць дакументы" (drop docs) іншых, раней вядомых толькі па імені карыстальніка або псеўданіму. Слова "docs" ператварылася ў "dox", страціла прэфікс "drop" і з часам стала дзеясловам.

Цяпер выкарыстанне тэрміна "доксінг" выйшла за межы супольнасці хакераў і ўжываецца для апісання факту раскрыцця асабістай інфармацыі. Хаця гэты тэрмін усё яшчэ выкарыстоўваецца для апісання выкрыцця ананімных карыстальнікаў, гэта стала менш актуальным, паколькі большасць выкарыстоўвае свае сапраўдныя імёны ў сацыяльных сетках.

Канкуруючыя хакеры выкрываюць тых, хто прытрымліваецца супрацьлеглых поглядаў. Мэта доксінгу – перанесці канфлікт з інтэрнэту ў рэальны свет, раскрываючы інфармацыю, якая ўключае: дамашнія адрасы; дадзеныя аб месцы працы; нумары асабістых тэлефонаў; нумары сацыяльнага страхавання; інфармацыю аб банкаўскім рахунку і крэдытных картах; дэталі асабістай перапіскі; інфармацыю аб крымінальным мінулым; асабістыя фатаграфіі; якія кампраметуюць асабістыя дадзеныя.

Доксінг-напады маюць такія мадыфікацыі, як падробленая падпіска на рассылку або дастаўку піцы, да такіх як пераслед сям'і, крадзеж асабістых дадзеных, пагрозы і асабістае дамаганне.

Палітыкі і журналісты часта падвяргаюцца доксінгу. Яны пакутуюць ад анлайн-пераследаў, асцерагаючыся за ўласную бяспеку і часам нават за

жыццё. Гэтая практыка таксама распаўсюдзілася на кіраўнікоў буйных кампаній. Доксінг стаў шырока вядомы ў снежні 2011 года, калі група прафесійных хакераў

Anonymous раскрыла падрабязную інфармацыю аб 7000 супрацоўнікаў праваахоўных органаў у адказ на расследаванне хакерскіх дзеянняў. З тых часоў гурт Anonymous выкрыў сотні меркаваных чальцоў KKK (Ку-клукс-клан), а адной з іх апошніх мэт былі прыхільнікі Q-Anon.

Матывы доксінгу розныя. Асобы, якія падвергліся нападу або абразе, жадаюць адпомсціць. Напад можа быць накіраваны на асоб, якія маюць супрацьлеглы пункт гледжання. Аднак гэта, як правіла, мае месца, калі справа датычыць асабліва вострых пытанняў, а не паўсядзённых палітычных рознагалоссяў.

Наўмыснае раскрыццё асабістай інфармацыі ў інтэрнэце звычайна адбываецца з мэтай пакараць, запалохаць або прынізіць ахвяру. Пры гэтым доксеры таксама могуць разглядаць свае дзеянні як спосаб пакараць каго-небудзь за мінулыя памылкі, прыцягнуць да адказнасці на вачах у грамадскасці або раскрыць планы, якія раней не раскрываліся публічна.

Незалежна ад матывацыі, асноўная мэта доксінгу – парушыць канфідэнцыяльнасць і паставіць людзей у нязручнае становішча, часам з жудаснымі наступствамі. У інтэрнэце ёсць вялікая колькасць асабістай інфармацыі, і людзі часта маюць над ёй значна менш кантролю, чым яны мяркуюць. Гэта азначае, што любы, хто мае час, матывацыю і цікавасць, можа ператварыць гэтыя дадзеныя ў зброю.

Многія людзі выкарыстоўваюць адно і тое ж імя карыстальніка ў розных сэрвісах. Гэта дазваляе патэнцыйным доксерам скласці ўяўленне аб інтарэсах ахвяры і аб тым, як яна праводзіць час у Інтэрнеце. Інфармацыя аб кожным уладальніку даменнага імя захоўваецца ў рэестры, які часта з'яўляецца агульнадаступным пры выкарыстанні пошуку WHOIS.

Выкажам здагадку, што чалавек, які набыў даменнае імя, не схаваў асабістую інфармацыю пры куплі. У гэтым выпадку інфармацыя, якая

дазваляе ўстанавіць яго асобу (імя, адрас, нумар тэлефона, месца працы і адрас электроннай пошты), даступная ў інтэрнэце для ўсіх.

Калі хто-небудзь выкарыстоўвае неабаронены ўліковы запіс электроннай пошты, то зламыснікі могуць раскрыць канфідэнцыйныя электронныя лісты гэтага чалавека і апублікаваць іх у інтэрнэце.

Калі ўліковыя запісы ў сацыяльных сетках з'яўляюцца агульнадаступнымі, любы можа высветліць інфармацыю і пачаць кібернетычны пераслед. Можна даведацца пра месцазнаходжанне, месца працы, інфармацыю пра сяброў, атрымаць фатаграфіі, глядзець лайкі і дызлайкі, наведаныя месцы, даведацца пра імёны членаў сям'і і хатніх жывёл. Выкарыстоўваючы гэтую інфармацыю, доксеры нават змогуць знайсці адказы на сакрэтныя пытанні і ўзламаць іншыя акаўнты.

Доксеры могуць выкарыстоўваць розныя метады вызначэння IP-адрасу, звязанага з фізічным месцазнаходжаннем. Даведаўшыся IP-адрас, яны могуць прымяніць метады сацыяльнай інжынерыі да інтэрнэт-правайдэра і атрымаць аб ахвяры больш інфармацыі. Напрыклад, яны могуць падаць скаргу на ўладальніка IP-адрасы або паспрабаваць узламаць сетку.

Даведаўшыся нумар мабільнага тэлефона, зламыснікі змогуць атрымаць аб чалавеку больш інфармацыі. Напрыклад, сэрвісы пошуку па нумары тэлефона, такія як Whitepages, дазваляюць па нумары мабільнага ці любога іншага тэлефона вызначыць асобу ўладальніка гэтага нумара.

Такія сайты, як Whitepages, бясплатна падаюць толькі дадзеныя аб горадзе і штаце. За прадастаўленне дадатковай інфармацыі, звязанай з нумарам мабільнага тэлефона, яны спаганяюць аплату. За плату можна даведацца дадатковую асабістую інфармацыю аб чалавеку па нумары мабільнага тэлефона.

Тэрмін «праслухоўванне сеткі» часам выкарыстоўваецца ў сувязі з доксінгам. Яго выкарыстоўваюць у дачыненні да доксераў, якія перахапляюць дадзеныя ў інтэрнэце, якія шукаюць усё, ад пароляў, нумароў

крэдытных карт і інфармацыі аб банкаўскіх рахунках да старых паведамленняў электроннай пошты.

Доксеры падлучаюцца да сеткі, узломваюць яе абарону, а затым збіраюць уваходныя і выходныя дадзеныя сеткі. Адзін са спосабаў абароны ад праслухоўвання сеткі – выкарыстанне VPN.

Брокеры дадзеных існуюць для збору інфармацыі аб людзях і продажы гэтай інфармацыі з мэтай атрымання прыбытку. Брокеры дадзеных збіраюць інфармацыю з адкрытых крыніц, карт лаяльнасці (якія адсочваюць анлайн і афлайн пакупкі), гісторыі пошуку ў інтэрнэце (усё, што карыстачы шукалі, чыталі і загружалі) і ў іншых брокераў дадзеных. Многія брокеры дадзеных прадаюць інфармацыю рэкламадаўцам, але некаторыя сайты па пошуку людзей прапануюць вычарпальныя запісы аб людзях за адносна невялікае ўзнагароджанне. Доксера дастаткова заплаціць патрэбную суму і атрымаць неабходную інфармацыю, каб пачаць пераслед ахвяры.

Доксеры могуць стварыць карціну, якая прывядзе да раскрыцця асобы рэальнага чалавека, які хаваецца за псеўданімам: яго імя, адрас месца жыхарства, адрас электроннай пошты, нумар тэлефона і шматлікае іншае. Доксеры таксама могуць купляць і прадаваць асабістую інфармацыю ў даркнеце.

Знойдзеную інфармацыю можна выкарыстоўваць як пагрозу, напрыклад, апублікаваць у Твітары ў адказ на нязгоду апанента. Доксінг можа складацца не столькі ў раскрыцці інфармацыі, колькі ў тым, як яна выкарыстоўваецца для запалохвання або пераследу ахвяры. Напрыклад, той, у каго ёсць ваш адрас, можа знайсці вас ці вашу сям'ю.

Той, у каго ёсць нумар вашага мабільнага тэлефона ці адрас электроннай пошты, можа засыпаць вас паведамленнямі, якія перашкаджаюць вам мець зносіны са службай падтрымкі. Нарэшце, ведаючы ваша імя, дату нараджэння і нумар сацыяльнага страхавання, зламыснік можа ўзламаць вашыя ўліковыя запісы або выкарыстоўваць вашыя асабістыя дадзеныя ў сваіх мэтах.

Любы, хто мае жаданне, час, доступ у інтэрнэт і матывацыю, зможа сабраць дасье на ахвяру. І калі ахвяра доксінгу забяспечыла адносную даступнасць дадзеных аб сабе ў інтэрнэце, выкрасці іх будзе зусім не складана. Найбольш распаўсюджаныя віды доксінгу можна падзяліць на тры катэгорыі: публікацыя ў інтэрнэце персанальнай інфармацыі, якая дазваляе ўстанавіць асобу; раскрыццё ў інтэрнэце раней невядомай інфармацыі аб прыватнай асобе.

Выдаванне інфармацыі аб прыватных асобах у інтэрнэце можа нанесці шкоду іх рэпутацыі і рэпутацыі іх партнёраў. Доксінг можа разбураць жыцці, паколькі пры доксінгу і ахвяры, і члены іх сем'яў могуць падвяргацца пераследу, як у Інтэрнэце, так і ў рэальным свеце.

Доксінг не лічыцца незаконным, калі раскрываемая інфармацыя знаходзіцца ў адкрытым доступе і была атрымана законнымі метадамі. Тым не менш, у залежнасці ад юрысдыкцыі, доксінг можа супярэчыць законам, распрацаваным для барацьбы з пераследам, дамаганнем і пагрозамі.

Гэта таксама залежыць ад віду раскрываецца інфармацыі. Напрыклад, расчыненне чыйго-небудзь сапраўднага імя лічыцца не настолькі сур'ёзным, як раскрыццё хатняга адрасу або нумары тэлефона. Аднак у ЗША раскрыццё інфармацыі аб дзяржаўным служачым падпадае пад федэральныя законы аб змове і разглядаецца як федэральнае правапарушэнне. Паколькі доксінг – адносна нядаўняя з'ява, якія тычацца яго законы пастаянна мяняюцца і не заўсёды адназначныя.

Незалежна ад законаў, доксінг парушае ўмовы выкарыстання многіх вэб-сайтаў і, такім чынам, можа прывесці да блакіроўкі. Гэта звязана з тым, што доксінг звычайна лічыцца неэтычным. У большасці выпадкаў ён ажыццяўляецца са злым намерам, каб запалохваць, шантажаваць і кантраляваць іншых. Ахвяры доксінгу падвяргаюцца патэнцыйным пераследам, крадзяжу асабістых дадзеных, зневажэнням, страце працы і непрыманню з боку сям'і і сяброў.

Выкарыстанне антывірусных праграм можа прадухіліць крадзеж інфармацыі з выкарыстаннем шкоднасных дадаткаў. Рэгулярнае абнаўленне праграмнага забеспячэння дапамагае прадухіліць дзюры ў сістэме бяспекі, якія могуць прывесці да ўзлому і расчыненні інфармацыі.

Надзейны пароль звычайна складаецца з камбінацыі загалоўных і малых літар, а таксама лічбаў і сімвалаў. Пазбягайце выкарыстання аднаго і таго ж пароля для некалькіх уліковых запісаў і рэгулярна мяняйце паролі. Калі ў вас праблемы з запамінаннем пароляў, выкарыстоўвайце менеджэр пароляў. Выкарыстанне розных імёнаў карыстальнікаў для розных мэт абцяжарыць адсочванне вашых дзеянняў на розных сайтах.

Разгледзьце магчымасць выкарыстання розных уліковых запісаў электроннай пошты для розных мэт: прафесійных, асабістых і для спаму. Асабісты адрас электроннай пошты можна выкарыстоўваць для перапіскі з блізкімі сябрамі, членамі сям'і і іншымі даверанымі асобамі; пазбягайце публічнага выкарыстання гэтага адраса.

Спам-адрас электроннай пошты можна выкарыстоўваць для рэгістрацыі уліковых запісаў у розных сэрвісах і рэкламных акцыях. Працоўны адрас электроннай пошты (незалежна ад таго, ці з'яўляецеся вы фрылансерам ці супрацоўнікам кампаніі) можна пазначыць публічна.

Як і ў выпадку з агульнадаступнымі ўліковымі запісамі ў сацыяльных сетках, пазбягайце ўказваць залішнюю ідэнтыфікуючую інфармацыю ў адрасе электроннай пошты (пазбягайце адрасоў тыпу імя. прозвішча. Дата нараджэння@gmail.com).

Ацэніце налады канфідэнцыйнасці вашых профіляў у сацыяльных сетках і пераканайцеся, што вас задавальняе, якая інфармацыя пра вас даступная і каму.

Вызначыце, якія платформы вы карыстаецеся для якіх мэт. Калі вы выкарыстоўваеце платформу ў асабістых мэтах (напрыклад, дзяліцеся фатаграфіямі з сябрамі і роднымі ў Facebook або Instagram), узмацніце налады канфідэнцыяльнасці.

Калі вы выкарыстоўваеце платформу для прафесійных мэт (напрыклад, для адсочвання апошніх навін або для размяшчэння спасылак на вашу працу ў Твітары), можна пакінуць профіль агульнадаступным. У гэтым выпадку пазбягайце публікацыі канфідэнцыйнай асабістай інфармацыі і выяваў.

Вам ці каму-небудзь, які спрабуе выканаць уваход у ваш уліковы запіс, спатрэбіцца як мінімум два віды ідэнтыфікацыі: звычайна гэта пароль ад уліковага запісу і нумар тэлефона. Так зламыснікам будзе складаней атрымаць доступ да вашых прылад або уліковых запісаў, паколькі сістэма будзе патрабаваць не толькі пароль, але і дадатковы PIN-код.

Праглядзіце, на колькіх сайтах ёсць інфармацыя аб вас. Нягледзячы на тое, што такія сайты, як MySpace, ужо «вышлі з моды», профілі, створаныя больш за дзесяць гадоў таму, па-ранейшаму бачныя і даступныя. Гэта адносіцца да любога сайта, на якім вы, магчыма, праяўлялі актыўнасць раней. Па магчымасці выдаліце састарэлыя і невыкарыстоўваныя профілі.

Доксеры могуць выкарыстоўваць фішынгавыя атакі, каб даведацца хатні адрас, нумар поліса сацыяльнага страхавання ці нават паролі. Будзьце асцярожныя пры атрыманні паведамленняў з запытам асабістых дадзеных, адпраўленых нібыта банкам ці кампаніяй-эмітэнтам крэдытнай карты. Фінансавыя ўстановы ніколі не запытваюць такую інфармацыю па электроннай пошце.

WHOIS - гэта база дадзеных усіх зарэгістраваных даменных імёнаў у інтэрнэце. Гэты агульнадаступны рэестр можа выкарыстоўвацца для вызначэння асобы або арганізацыі, якім належыць дамен, іх фізічнага адраса і іншай кантактнай інфармацыі.

Калі вы плануеце кіраваць вэб-сайтам ананімна, не раскрываючы асобу, пераканайцеся, што вашыя асабістыя дадзеныя з'яўляюцца канфідэнцыйнымі і схаваныя з базы дадзеных WHOIS. Рэгістратары даменаў могуць кантраляваць параметры канфідэнцыйнасці, таму варта ўдакладніць у рэгістратара вашага дамена, як гэта зрабіць.

Калі асабістая інфармацыя з'яўляецца ў выніках пошуку Google, можна запытаць яе выдаленне з пошукавай сістэмы. У Google гэта рэалізавана як просты працэс з выкарыстаннем анлайн-формы. Многія брокеры дадзеных размяшчаюць такую інфармацыю ў інтэрнэце, звычайна для праверкі біяграфічных дадзеных або дадзеных аб злачынствах.

Можаце выдаліць сваю асабістую інфармацыю з сайтаў брокераў даных. Самастойнае выдаленне даных без матэрыяльных затрат можа аказацца працаёмкім. Калі вы абмежаваныя па часе, пачніце з трох асноўных брокераў: Epsilon, Oracle і Acxiom.

Неабходна рэгулярна правяраць гэтыя базы даных, паколькі інфармацыя можа быць апублікавана паўторна нават пасля выдалення. Можна таксама аплаціць паслугі такіх сэрвісаў як DeleteMe, PrivacyDuck ці Reputation Defender, каб яны выдалілі вашыя дадзеныя.

Анлайн-віктарыны могуць здацца бяскрыўднымі, але часта яны з'яўляюцца крыніцай асабістых дадзеных, якія карыстачы падаюць, не задумляючыся аб наступствах. Некаторыя пытанні віктарыны нават могуць аказацца кантрольнымі пытаннямі для вашых пароляў.

Многія віктарыны запытваюць дазвол на прагляд профілю ў сацыяльных сетках ці адрасы электроннай пошты, перш чым паказаць вынікі. Яны могуць звязаць вынікі апытання з вашай рэальнай асобай, не асабліва клапоцячыся аб тым, хто запускае віктарыну і чаму лепш пазбягаць захоўванні гэтых дадзеных разам.

Мабільныя прыкладанні таксама з'яўляюцца крыніцамі асабістых дадзеных. Многія прыкладанні запытваюць дазволы на доступ да дадзеных або прыладзе, якія наогул не датычацца гэтых прыкладанняў.

Напрыклад, з дадаткам для рэдагавання малюнкаў не мае сэнсу запытваць дазвол на доступ да кантактаў. Абгрунтавана, калі яно запытвае доступ да камеры або фатаграфій. Але калі прыкладанне патрабуе доступ да кантактаў, дадзеным аб месцазнаходжанні і профілі ў сацыяльных сетках, будзьце асцярожныя.

Па магчымасці, пазбягайце публічнага разгалашэння пэўнай інфармацыі, напрыклад, нумары поліса сацыяльнага страхавання, хатняга адраса, нумары правоў кіроўцы, а таксама любой інфармацыі аб банкаўскіх рахунках або нумарах крэдытных карт. Хакеры могуць перахапляць паведамленні электроннай пошты, таму не ўказвайце ў іх свае асабістыя дадзеныя.

Лепшая абарона – абцяжарыць зламыснікам атрыманне вашай асабістай інфармацыі. Можна праверыць, наколькі лёгка вы можаце падвергнуцца доксінгу, высветліўшы, якую інфармацыю пра вас можна атрымаць. Знайдзіце себы ў Google. Выканайце зваротны пошук малюнкаў. Праверце свае профілі ў сацыяльных сетках, у тым ліку параметры прыватнасці. Праверце, ці не патрапіла якая-небудзь з вашых уліковых запісаў электроннай пошты ў буйную ўцечку дадзеных, выкарыстоўваючы сайт com.

Праверце вашыя рэзюмэ і дадзеныя на асабістых вэб-сайтах, каб даведацца, якая асабістая інфармацыя маецца ў вашых прафесійных профілях. Калі ў інтэрнэце ёсць PDF-файлы з вашым рэзюмэ, абавязкова выключыце такія дадзеныя, як хатні адрас, асабісты адрас электроннай пошты і нумар мабільнага тэлефона (ці заменіце іх агульнадаступнымі версіямі такой інфармацыі).

Будзьце асцярожныя з інфармацыяй, якая публікуецца ў інтэрнэце. Ніколі не публікуйце асабістую інфармацыю на форумах, дошках аб'яваў ці ў сацыяльных сетках. Наіўна меркаваць, што інтэрнэт дае людзям свабоду размаўляць ці пісаць усё, што хочацца. Людзі лічаць, што ананімнасць дазваляе ім выказваць любыя думкі, незалежна ад таго, наколькі спрэчнымі яны з'яўляюцца, без магчымасці адсочвання. Але, як мы пераканаліся, гэта не так, таму важна з асцярожнасцю выказваць сваё меркаванне ў інтэрнэце.

Самая распаўсюджаная рэакцыя на доксінг – гэта страх ці нават адкрытая паніка. Вельмі відавочна ўзнікае адчуванне ўразлівасці. Доксінг спецыяльна распрацаваны так, каб выклікаць у ахвяры пачуццё небяспекі,

прымусіць панікаваць, вывесці з сябе. Калі вы сталі ахвярай доксінгу, можна зрабіць наступныя крокі:

Паведаміце аб нападзе ў адміністрацыю платформы, на якой была размешчана ваша асабістая інфармацыя. Ва ўмовах выкарыстання платформы або ў правілах супольнасці выканайце пошук інфармацыі аб парадку інфармавання аб нападах такога тыпу, і выконвайце гэтыя інструкцыі. Запаўняючы форму, захавайце яе на будучыню (каб не прыйшлося паўтарацца). Гэта першы крок да спынення распаўсюджвання вашых асабістых дадзеных.

Калі доксер пагражае вам асабіста, звернецеся ў мясцовае аддзяленне паліцыі. Любыя дадзеныя, якія змяшчаюць ваш хатні адрас або фінансавую інфармацыю, павінны мець вышэйшы прыярытэт пры разглядзе, асабліва калі маюцца дакладныя пацверджанні факту пагроз.

Зрабіце здымкі экрана або загрузіце старонкі, на якіх размешчана ваша асабістая інфармацыя. Паспрабуйце пераканацца, што бачныя даты і вэб-адрасы. Гэтыя доказы важныя для вас, і могуць аказацца карыснымі праваахоўным і іншым зацікаўленым органам.

Калі доксеры апублікавалі нумар вашага банкаўскага рахунку або крэдытнай карты, неадкладна паведаміце аб гэтым у адпаведныя фінансавыя ўстановы. Эмітэнт крэдытнай карты, хутчэй за ўсё, анулюе вашу карту і дашле вам новую. Таксама будзе неабходна змяніць пароль анлайн-банка і рахункаў крэдытнай карты.

Зменіце паролі, выкарыстоўвайце менеджэр пароляў, дзе магчыма, уключыце шматфактарную аўтэнтыфікацыю, узмацніце налады канфідэнцыяльнасці для кожнага выкарыстоўванага ўліковага запісу.

Доксінг можа быць эмацыйна стомным. Папрасіце каго-небудзь, каму вы давяраеце, дапамагчы вам разабрацца з гэтай праблемай, каб вам не даводзілася вырашаць яе ў адзіночку. Доксінг – сур'ёзная праблема, якая ўзнікла з-за лёгкай даступнасці асабістай інфармацыі ў інтэрнэце. Заставацца

ў бяспецы ў анлайн-свеце не заўсёды лёгка. Дапамагае выкарыстанне перадавых метадаў кібернетычнай бяспекі.

Кібернетычны буллінг

Гэта запалохванне і цкаванне з выкарыстаннем лічбавых тэхналогій. Ён можа праходзіць у сацыяльных сетках, у дадатках для абмену паведамленнямі, на гульнявых платформах і мабільных тэлефонах. Гэта паўтаральныя эпізоды, мэта якіх – напалохаць, раззлаваць ці зганьбіць тых, каго пераследуюць. Гэта:

• распаўсюджванне ілжывай інфармацыі ці размяшчэнне непрыстойных фатаграфій каго-небудзь у сацыяльных сетках;

• адпраўка абразлівых паведамленняў або пагроз праз платформы абмену паведамленнямі;

• выдача сябе за іншую асобу і адпраўка непрыстойных паведамленняў ад яго імя.

Інтэрнэт-траўля пакідае лічбавы след – запіс, які можа апынуцца карысным і стаць доказам, неабходным для спынення запалохванняў.

Часам суразмоўца можа сказаць, што ён "проста пажартаваў" ці што вам не варта ўспрымаць яго словы сур'ёзна.

Аднак калі вас зачапілі яго словы ці вам здаецца, што ён смяецца не з вамі, а над вамі, то, хутчэй за ўсё, такі жарт перайшоў межы дазволенага. Калі такія паводзіны працягваюцца нават пасля таго, як вы папрасілі чалавека перастаць, і вас па-ранейшаму крыўдзяць яго словы, то тады гэта можа расцэньвацца як цкаванне.

Калі ганенне адбываецца ў сетцы, гэта можа пацягнуць за сабой непажаданую ўвагу з боку шырокага кола людзей, у тым ліку незнаёмцаў. Дзе б такія паводзіны ні адбываліся, калі яны выклікаюць вашу незадаволенасць, не трэба трываць і ігнараваць такую сітуацыю.

Калі чалавека труцяць у сеткі, яму здаецца, што яго пераследуюць паўсюль, нават калі ён знаходзіцца ў сябе дома. У яго складваецца ўражанне, што яму няма дзе схавацца ад крыўдзіцеляў. Такія дзеянні могуць мець доўгатэрміновыя наступствы:

псіхалагічныя – чалавек сумуе, адчувае няёмкасць, здаецца самому сабе дурным ці злуецца;

эмацыйныя – чалавек пачынае саромецца сваіх захапленняў або губляе да іх цікавасць;

фізіялагічныя – стомленасць (праблемы са сном) або такія сімптомы, як болі ў жываце і галаўныя болі.

Боязь насмешак або пераследу з боку іншых людзей можа перашкодзіць ахвярам расказаць аб праблеме або паспрабаваць яе вырашыць. У крайніх выпадках інтэрнэт-траўля можа давесці чалавека да самагубства.

Траўля ў інтэрнэце ўплывае на самыя розныя аспекты жыцця. Але ўсе гэтыя праблемы можна пераадолець, і ўпэўненасць у сабе адновіцца.

Калі цкаванне адбываецца ў сацыяльных сетках, вы можаце заблакаваць праследавацеля і адправіць на яго скаргу адміністратарам сацыяльнай сеткі. Кампаніі, якім належаць сацыяльныя сеткі, абавязаны гарантаваць бяспеку сваіх карыстальнікаў.

Карысна сабраць доказы – перапіску і скрыншоты пастоў у сацыяльных сетках для таго, каб пацвердзіць тое, што адбываецца. Для таго каб спыніць інтэрнэт-траўлю, неабходна яе выявіць, а найважнейшы крок – падача скаргі. Гэта таксама пакажа пераследніку, што яго паводзіны недапушчальныя.

Калі вы знаходзіцеся ў небяспецы, вам трэба звязацца з паліцыяй. Падумайце, перш чым выкладваць штосьці ў сетку – гэтая інфармацыя можа захавацца ў інтэрнэце навечна, і потым яе хто-небудзь можа выкарыстаць вам на шкоду. Не паведамляйце такія асабістыя дэталі, як ваш адрас, нумар тэлефона ці школа, у якую вы ходзіце.

Вывучыце налады канфідэнцыйнасці ў вашых любімых сацыяльных сетках. Вы можаце вырашыць, каму дазваляецца праглядаць ваш профіль,

адпраўляць вам асабістыя паведамленні ці пакідаць каментары да вашых пастоў, змяніўшы налады канфідэнцыйнасці вашага ўліковага запісу.

Вы можаце адправіць скаргу на абразлівыя каментары, паведамленні і фатаграфіі і папрасіць іх выдаліць. Акрамя "выдалення са спісу сяброў", вы можаце цалкам заблакаваць пэўных карыстальнікаў для таго, каб яны не маглі бачыць ваш профіль або звязвацца з вамі.

Вы таксама можаце выбраць наладу, з дапамогай якой каментары пэўных карыстальнікаў будуць з'яўляцца толькі ў іх, не блакуючы іх цалкам. Вы можаце выдаляць паведамленні ў сваім профілі ці хаваць іх ад канкрэтных карыстальнікаў.

У большасці вашых любімых сацыяльных сетак карыстальнікі не атрымліваюць паведамлення аб тым, што нехта іх заблакаваў, абмежаваў ім доступ да вашага ўліковага запісу або адправіў на іх скаргу.

Людзі, якія з'яўляюцца ахвярамі любых форм гвалту, у тым ліку ганенне і запалохванне, а таксама інтэрнэт-траўлю, маюць права на правасуддзе і прыцягненне да адказнасці правапарушальніка.

У краінах, дзе дзейнічаюць спецыяльныя законы аб кібернетычным булінгу, паводзіны ў інтэрнэце, накіраваныя на выкліканне сур'ёзных эмацыйных перажыванняў, разглядаецца як злачыннае дзеянне. У некаторых з гэтых краін ахвяры інтэрнэт-траўлі могуць звяртацца за абаронай, дамагчыся забароны зносін праследавацеля з імі, часовага або пастаяннага абмежавання выкарыстання праследавацелем электронных прылад, якія выкарыстоўваюцца для здзяйснення ім інтэрнэт-траўлі.

Тролінг у інтэрнэце

Пад тэрмінам «Інтэрнэт-троль», як правіла, маюць на ўвазе анлайн-каментатара або ўдзельніка дыскусіі, мэта якога справакаваць канфлікт паміж іншымі суразмоўцамі шляхам размяшчэння спрэчных і абуральных каментароў. І хаця тролі існуюць ужо даўно, увагу большасці яны

прыцягнулі ўжо з папулярнасцю сацыяльных сетак. Неўзабаве яны з'явіліся на розных вядомых платформах.

Акрамя ігнаравання абуральных паведамленняў троляў, неабходна ведаць, як іх ідэнтыфікаваць. Варта разумець, што тролі – гэта не тыя людзі, якія маюць меркаванне, супрацьлеглае вашаму або з якім вы не згодныя.

Сустрэць троляў даволі проста, паколькі яны ўсюды – у сацыяльных сетках, на сайтах анлайн-гульняў, у раздзелах каментароў навінавых старонак і на анлайн-форумах.

Анлайн-тролі бываюць розных відаў – ад людзей, якія публікуюць наўмысна раздражняльныя або супярэчлівыя каментары, каб распаліць спрэчку для ўласнай забаўкі, да кіберзлачынцаў, якія маюць іншыя зламысныя мэты ў Інтэрнэце.

Сёння вядомым прыкладам Інтэрнэт-тролінга з'яўляецца выкарыстанне тэмы пандэміі COVID-19 анлайн-злачынцамі для распаўсюджвання спрэчных публікацый. У прыватнасці, тролі выступаюць супраць вакцынацыі, дзелячыся падробленымі хатнімі лекамі ці нават ставячы пад сумненне кампетэнтнасць медыцынскіх спецыялістаў.

Варта адзначыць, што кіберзлачынцы таксама выкарыстоўваюць Інтэрнэт-тролінг, напрыклад, размяшчаюць кантэнт спрэчнага характару. Аднак іх каментары, як правіла, суправаджаюцца спасылкамі, замаскіраванымі пад крыніцу інфармацыі, са шкоднасным праграмным забеспячэннем.

Спачатку Інтэрнэт-тролінг можа здацца нявінным, але часта сітуацыя можа пагоршыцца і перарасці ў кібербулінг або кіберпераслед. Не карміце троляў – гэта асноўнае правіла, якога варта прытрымлівацца, сутыкаючыся з гэтымі злачынцамі ў Інтэрнэце. У адваротным выпадку, вы можаце толькі пагоршыць сітуацыю, даўшы тролям тое, чаго яны хочуць – увага.

Хоць вам і жадаецца прыняць удзел у дыскусіі, будзьце гатовыя да таго, што вашы аргументы застануцца без увагі. Паколькі мэта такіх людзей не абмеркаванне, а рэакцыя – у асноўным злосная або трывожная.

Тым не менш, існуюць метады для абароны ад анлайн-троляў. Сацсеткі Facebook, Twitter і Instagram прапануюць інструменты для абвесткі аб тролях, якія наўмысна запалохваюць іншых карыстальнікаў, публікуюць чужую асабістую інфармацыю на ўсеагульны агляд, выкарыстоўваюць «мова варожасці» або парушаюць іншыя агульнапрынятыя прынцыпы.

Сайты не ўхваляюць такія паводзіны, таму ў залежнасці ад сур'ёзнасці парушэння мадэратары могуць прымяняць пакаранне – ад папярэджанняў і часовых забарон да блакіроўкі акаўнтаў паўторных парушальнікаў.

Калі Інтэрнэт-тролінг адбываецца на іншых форумах, перш за ўсё вы павінны звязацца з адміністратарамі службы, у якіх ёсць прылады для барацьбы з парушальнікамі. Навінавыя сайты маюць выразную палітыку ў стаўленні абразлівых паводзін, якую тролі часта парушаюць, што прыводзіць да іх часавага ці сталага блакавання. У выпадку ператварэння Інтэрнэт-тролінга ў кіберпераслед, кібербулінг, дамаганні інтымнага характару, абразы ці іншыя дзеянні, якія могуць супярэчыць розным законам, вы можаце звярнуцца ў праваахоўныя органы.

Інтэрнэт-тролінг часта можа быць адносна бясшкодным заняткам, якім некаторыя людзі займаюцца для прыцягнення ўвагі іншых з мэтай забаўкі. Хаця ў некаторых выпадках такія людзі пераходзяць мяжу на шкоду іншым карыстальнікам. У такіх выпадках памятаеце пра адмысловыя прылады, створаных для пакарання анлайн-троляў.

У любым выпадку злачынцы двойчы падумаюць, перш чым паўтарыць гэта зноў, паколькі Інтэрнэт-ананімнасць не ўсё якая ахоплівае, і рана ці позна пра ўсё станавіцца вядома.

Лічбавыя сляды

Кожны карыстач сеткі пакідае сляды дзеянняў і прысутнасці, нават калі яны носяць правамерны характар. Гэтыя сляды называюцца лічбавымі. Злачынствы, якія здзяйсняюцца з выкарыстаннем кампутарных і сеткавых

кампутарных тэхналогій, паказваюць неверагодны рост, што з'яўляецца вялікай пагрозай для радавых грамадзян

Крыміналістычныя магчымасці развіваюцца прапарцыйна развіццю ІТ-сферы, таму ў крыміналістычнай тэорыі назіраецца тэндэнцыя вывучэння тэматыкі лічбавых слядоў злачыннай дзейнасці ў наступных асноўных кірунках: гэта папярэджанне, раскрыццё і расследаванне злачынстваў у сферы камп'ютэрнай інфармацыі.

Неправамерны доступ да камп'ютарнай інфармацыі. Стварэнне, выкарыстанне і распаўсюджванне шкоднасных камп'ютэрных праграм. Якія ў большасці выпадкаў з'яўляюцца прэдыкатнымі для ўчынення (або ўтойвання) іншых злачынстваў (крадзяжоў, распаўсюджвання экстрэмісцкіх матэрыялаў), фальсіфікацыі вынікаў галасавання.

У шырокім напрамку – гэта процідзеянне ўчыненні злачынстваў з выкарыстаннем ІТ-тэхналогій. Сярод гэтых злачынстваў:

– давядзенне да самагубства з выкарыстаннем сеткі Інтэрнэт або схіленне да самагубства;

– дыстанцыйныя крадзяжы ў сферы фінансаў;

– заклікі да ажыццяўлення тэрарыстычнай, экстрэмісцкай дзейнасці, масавых беспарадкаў;

– абарот наркотыкаў і зброі, парнаграфічных матэрыялаў;

– арганізацыя азартных гульняў;

– злачынствы супраць палавой недатыкальнасці непаўналетніх, фішынг, крадзеж асабістых дадзеных, інфармацыйная блакада, шпіянаж і шантаж.

Лічбавыя сляды ў крыміналістыцы варта разглядаць значна шырэй. Яны актуальныя пры правядзенні працэсуальных праверак і расследаванні любых злачынстваў незалежна ад аб'екта і спосабу замаху, катэгорыі або формы віны, дасведчанасці або недасведчанасці асобы аб іх пакіданні, а таксама прыналежнасці таму ці іншаму ўдзельніку крымінальнага працэсу (падазронаму, пацярпеламу або сведку).

Цікавасць уяўляюць лічбавыя спосабы даказвання злачыннай дзейнасці, выкарыстанне высокатэхналагічнай крыміналістычнай тэхнікі і спецыялізаваных праграм для атрымання крыміналістычна значнай інфармацыі пры аглядзе або правядзенні экспертных даследаванняў гаджэтаў карыстальнікаў і вялікага аб'ёму білінгавай інфармацыі.

Спецыфіку набываюць і неардынарныя спосабы даказвання такіх злачынстваў, аб'ектыўны бок якіх выяўляецца ў распаўсюджванні якой-небудзь інфармацыі або ў публічных закліках да супрацьпраўнай дзейнасці. Сюды ўваходзяць:

– агляды сацыяльных сетак карыстальнікаў, іх электронных прылад;

– скрыншоты старонак, на якіх адлюстроўваецца ўся актыўнасць дадзеных карыстальнікаў (перапіскі, адпраўленыя і атрыманыя выявы, відэазапісы, дакументы, пакінутыя «лайкі» і каментары).

Суды і прысяжныя засядацелі станоўча ўспрымаюць такую практыку, бо яна дакладная і надзейная.

Пад лічбавым следам варта разумець набор унікальных дзеянняў, які робіцца ў інфармацыйным асяроддзі, уключаючы інфармацыю, пакінутую ў выніку ўзаемадзеяння з рознымі сеткавымі і тэлекамунікацыйнымі рэсурсамі. Лічбавы след можа быць пакінуты як фізічнай, так і юрыдычнай асобай.

Таксама лічбавы след можна вызначыць, як любую крыміналістычна значную кампутарную інфармацыю. Гэта звесткі (паведамленні, даныя), якія знаходзяцца ў электронна-лічбавай форме, зафіксаваную на матэрыяльным носьбіце з дапамогай электрамагнітных узаемадзеянняў або перадаецца па каналах сувязі з дапамогай электрамагнітных сігналаў.

Асабістыя дадзеныя застаюцца ў лічбавай прасторы навечна, і пазбавіцца ад іх практычна немагчыма, у той час, як пакінуць іх не ўяўляе ні найменшага працы. Сцвярджэнне "Інтэрнэт памятае ўсё" з'яўляецца таму пацвярджэннем. Лічбавыя сляды – гэта:

– відэа фіксацыя (як самімі злачынцамі, так і зробленая апроч іх волі) падрыхтоўкі, здзяйснення, утойвання злачынстваў;

– білінгавая інфармацыя аб злучэннях паміж абанентамі (абаненцкімі прыладамі);

– інфармацыя, якая змяшчаецца ў памяці (хмарным сховішчы) смартфона, тэлефона ўдзельніка крымінальнага судаводства;

– крыміналістычна значная інфармацыя, якая знаходзіцца ў памяці кампутара;

– метададзеныя і лічбавая інфармацыя розных гаджэтаў, якая дазваляе вызначыць месцазнаходжанне гаджэта і яго ўладальніка; сацыяльныя сеткі як крыніца крыміналістычна значнай інфармацыі;

– дадзеныя гісторыі браўзэра карыстальніка;

– дыстанцыйнага зандавання паверхні Зямлі.

Больш за канкрэтным выразам электронна-лічбавых слядоў з'яўляюцца файлы аперацыйнай сістэмы і прыкладнога праграмнага забеспячэння, файлы сістэмнага рэестра, часопісы, канфігурацыйныя файлы, налады, тэкставыя дакументы, табліцы, базы дадзеных, фота-, аўдыё- і відэафайлы, логі праграм, печыва і іншыя файлы, якія змяшчаюцца ў сістэме і кампанентах самага сістэмнага блока кампутара. Да асаблівасцяў электронных слядоў трэба аднесці тое, што яны:

– з'яўляюцца адной з аб'ектыўных форм існавання камп'ютарнай інфармацыі;

– заўсёды апасродкаваны праз штучна створаны прадмет матэрыяльнага свету – электронны носьбіт інфармацыі, па-за якім фізічна не могуць існаваць;

– дыстанцыйны доступ да іх могуць адначасова мець шмат фізічных асоб;

капіруюцца на розныя віды электронных носьбітаў інфармацыі; выяўляюцца, капіююцца (дубліруюцца), даследуюцца і выкарыстоўваюцца ў мэтах крымінальнага судаводства толькі з дапамогай адмысловых навукова-тэхнічных сродкаў – сродкаў пошуку, збору, захоўванні, апрацоўкі, перадачы і паданні кампутарнай інфармацыі.

У лічбавага следа адсутнічае прасторавая форма, маюцца асаблівасці ўнутранай будовы і спосабы пераўтварэння, і ён недаступны для непасрэднага ўспрымання. Выманне лічбавых слядоў, а таксама іх замацаванне аналіз і даследаванне ў якасці крыміналістычна значнай для расследавання інфармацыі патрабуе асоб, якія валодаюць спецыяльнымі ведамі ў гэтай сферы, для правядзення кансультавання, дапамогі ў адабранні, правядзення судовай экспертызы або допыту ў якасці эксперта.

Адной з ключавых пераваг лічбавых слядоў злачынстваў з'яўляецца тое, што яны забяспечваюць аб'ектыўны і даступны запіс дзейнасці злачынцы. Гэта асабліва важна ў выпадках, калі доказы цяжка атрымаць традыцыйнымі метадамі, напрыклад, у выпадках кібернетычнай злачыннасці. У гэтых выпадках лічбавыя сляды злачынства могуць падаць каштоўную інфармацыю аб асобе злачынца, яго месцазнаходжанні і дзеяннях, а таксама аб часе і даце здзяйснення злачынства.

Іншым важным аспектам лічбавых слядоў злачынства з'яўляецца тое, што іх можна выкарыстоўваць для складання храналогіі падзей, злучаных са злачынствам. Гэта можа быць асабліва карысна ў складаных выпадках, калі патрабуецца апрацаваць вялікі аб'ём інфармацыі і мноства патэнцыйных падазраваных. Аналізуючы лічбавыя сляды, следчыя могуць лепей зразумець парадак падзей і іх удзельнікаў.

Лічбавыя сляды злачынства не заўсёды надзейныя. Напрыклад, злачынец можа паспрабаваць схаваць свае сляды, выдаліўшы сваю гісторыю наведвання Інтэрнэту, выкарыстоўваючы іншую прыладу для здзяйснення злачынства, падмяніўшы свой ip-адрас, сцершы метададзеныя і гэта толькі найпростыя спосабы з усіх існых.

Лічбавыя сляды могуць быць падроблены або зменены, што робіць іх менш надзейнымі ў якасці доказаў. Гэта падкрэслівае неабходнасць іх належнага адабрання, захоўвання, аналізу і апрацоўкі, каб забяспечыць надзейнасць, зручнасць і адпаведнасці крымінальнаму закону пры выкарыстанні ў якасці доказаў у крымінальных расследаваннях.

Важна разумець этычныя наступствы выкарыстання лічбавых слядоў у якасці доказаў. Напрыклад, выкарыстанне лічбавых слядоў можа выклікаць праблемы з канфідэнцыяльнасцю, паколькі асобныя асобы могуць не ведаць, што іх дзеянні адсочваюцца ці запісваюцца.

Існуюць законы і нарматыўныя акты аб недатыкальнасці прыватнага жыцця, якія рэгулююць збор, захоўванне і выкарыстанне лічбавых слядоў, і для праваахоўных органаў вельмі важна быць дасведчанымі аб гэтых законах, каб гарантаваць дапушчальнасць сабраных імі доказаў у судзе.

У будучыні выкарыстанне лічбавых слядоў злачынстваў, верагодна, стане яшчэ больш распаўсюджаным і важным, паколькі тэхналогіі працягваюць развівацца і становяцца ўсё больш інтэграванымі ў нашае паўсядзённае жыццё. Для таго каб эфектыўна выкарыстоўваць лічбавыя сляды злачынстваў у якасці доказаў, важна, каб крыміналісты і праваахоўныя органы працавалі разам.

Крыміналісты могуць падаць неабходныя веды і досвед аб прыродзе і выкарыстанні лічбавых слядоў у крымінальных расследаваннях, у той час як праваахоўныя органы могуць падаць неабходныя рэсурсы для збору, захоўванні, аналізу і апрацоўкі лічбавых слядоў. Важна прызнаць, што лічбавыя сляды злачынства не з`яўляюцца заменай традыцыйным формам доказаў. Хутчэй, яны з'яўляюцца дадатковым інструментам, які можа даць каштоўную інфармацыю і дапамагчы ў расследаваннях.

Найбольш эфектыўным спосабам расследавання з'яўляецца камбінацыя традыцыйных і лічбавых доказаў, для атрымання поўнай карціны злачынства і пабудовы пераканаўчай доказнай базы. "Віртуальныя сляды" і прыёмы працы з імі дапоўняць крыміналістычную тэхніку, і крымінальны закон зведае неабходныя змены, якія забяспечаць механізм выканання ўсяго комплексу дзеянняў з віртуальнымі слядамі.

Бяспека бізнес мадэляў

Лічбавая эканоміка пераходзіць на платформы і лічбавыя экасістэмы. Разнастайнасць лічбавых экасістэм ужо вялікая, і большасць вядомых экасістэм ахопліваюць мноства галін і ўключаюць у сябе розныя сектары прамысловасці, партнёраў, канкурэнтаў, кліентаў і бізнэс.

Гэта кідае выклік і традыцыйным настроях думак у галіне. Шляхі кліентаў могуць быць узаемазвязаны, і экасістэма можа падтрымліваць розныя віды дзейнасці, уключаючы электронную камерцыю, сацыяльныя сеткі, праграмныя рашэнні, апаратныя прапановы і лічбавыя забаўкі.

Галоўная мэта экасістэм прапанаваць заказчыкам адзіную і простую ў выкарыстанні сістэму, якая забяспечвае каштоўнасць за кошт разнастайных паслуг, прадуктаў і ведаў. Гэта таксама дазваляе платформам расці ў геаметрычнай прагрэсіі і апярэджваць звычайны рынак, выкарыстоўваючы некалькі задзейнічаных механізмаў.

Гэта таксама азначае, што пры маштабаванні экасістэмы магчымы розныя бізнэс-мадэлі. Ад прамых продажаў прадуктаў і паслуг да рэкламы, падпіскі і шмат чаго іншага.

Дзякуючы лепшаму разуменню кліента і перабудове прадуктовай прапановы можна павялічваць колькасць прапанаваных паслуг і прадуктаў з улікам колькасці інфармацыі, атрыманай ад кліентаў. Гэта робіць лічбавыя экасістэмы настолькі магутнымі, а таксама настолькі прыбытковымі, што спіс самых каштоўных кампаній у свеце ўзначальваюць кампаніі, якія выкарыстоўваюць магчымасці лічбавых экасістэм.

Тут вы знойдзеце Apple, Google, Facebook, Microsoft і многія іншыя кампаніі, якія выкарыстоўваюць сваю кліенцкую базу і экасістэмны падыход для росту даходаў і прапановы лепшых прадуктаў і паслуг сваім кліентам.

З 2000 гады Amazon увесь час будуе сваю лічбавую экасістэму. Спачатку раздробнаму гіганту неабходна было пабудаваць гіганцкую серверную інфраструктуру па ўсім свеце, каб мець магчымасць абслугоўваць

кліентаў на сваёй платформе электроннай камерцыі. Але неўзабаве Amazon пачала здаваць магутнасці серверaў у арэнду іншым прадпрыемствам. Гэты крок прывёў да з'яўлення Amazon Web Services (AWS) і стаў важнай вяхой для кампаніі ў стварэнні гэтай вялізнай экасістэмы, якая ў іх цяпер ёсць.

Amazon выкарыстоўваў уласную інфраструктуру AWS не толькі для забеспячэння іншых кампаній інфраструктурнымі паслугамі, але і ў якасці стартавай пляцоўкі для ўсіх іншых сэрвісаў, такіх як Amazon Prime Videos, Prime Music, Studio.

Гэта прывяло да хуткага стварэння сэрвісаў у сусвеце Амазонкі, а таксама да блакіроўкі для многіх карыстальнікаў. Перавагамі гэтых сэрвісаў было тое, што яны былі асноўнымі карыстачамі і хутчэй атрымлівалі пакеты, мелі доступ да музыкі amazon і нават маглі глядзець серыялы і фільмы з асноўнай бібліятэкі.

Пазней Amazon прыцягнула да ўдзелу ў экасістэме мноства іншых кампаній. Гэтак жа, як і ў выпадку з электроннай камерцыяй, кампанія Amazon першай адкрыла і дазволіла нават канкурэнтам выкарыстоўваць гэтую інфраструктуру паслуг і прылад, прапанаваных кампаніяй. Гэта прынесла ім вялізны поспех.

Паспяховыя лічбавыя экасістэмы маюць арыентацыю на стварэнне кошту. Часам у гэтых экасістэмах нават не было мадэлі манетызацыі ў пачатку, паколькі яны былі арыентаваны на кліента і разумелі яго яшчэ да таго, як яны пачнуць усталёўваць кошт на паслугі ці прапановы.

Характэрна арыентаванасць не толькі на абслугоўванне кліентаў і персаналізаваную рэкламу прапаноў кампаніі. Гэта азначае цэласную аперацыйную дзейнасць і супрацоўніцтва паміж аддзеламі і паміж паслугамі, каб як мага лепш інтэграваць падарожжа кліента.

Адной з асноўных пераваг выкарыстання лічбавай экасістэмы з'яўляецца магчымасць збору дадатковай інфармацыі аб працэсах, кліентах і здзелках. Гэта робіць дадзеныя адным з ключавых фактараў для кожнай лічбавай экасістэмы. Чым больш вы можаце даведацца аб кліенце, тым лепш

вы можаце прапанаваць паслугі, праграмнае забеспячэнне, тэхналогіі і інструменты для паляпшэння працы кліента.

Дзякуючы вялікаму разуменню, якое лічбавыя экасістэмы атрымліваюць ад кліентаў, пастаўшчыкоў і трэціх бакоў, можна таксама зрабіць гэтае разуменне дзейсным. Аўтаматызацыя з'яўляецца адным з ключавых элементаў зніжэння цаны, павышэння задаволенасці кліентаў, а таксама прапановы новых паслуг для павелічэння патоку каштоўнасці.

Лічбавыя экасістэмы існуюць для маштабавання, і, абмяжоўваючы іх галоўным чынам краінамі ці рэгіёнамі, вы ніколі не атрымаеце выгаду ад выкарыстання платформы і экасістэмы. Гэта азначае, што лічбавыя экасістэмы таксама павінны быць пабудаваны, каб зрабіць магчымым супрацоўніцтва паміж краінамі, рэгіёнамі і нават мовамі. Часам неабходна ўхіліць нават культурныя бар'еры.

У сувязі з маштабамі лічбавых экасістэм таксама трэба адзначыць, што менталітэт павінен быць вельмі дынамічным. Экасістэмы павінны хутка адаптавацца і хутка рэагаваць на зменлівую дынаміку рынку, у адваротным выпадку карыстацкая база будзе рухацца наперад і перамыкаць платформу. Бізнэс-інтэлект, хуткае прыняцце рашэнняў, а таксама выкарыстанне новых тэхналогій і бізнес-мадэляў павінны быць у цэнтры кожнага рашэння.

Перш чым вы пачнеце ўяўляць сябе будаўніком экасістэмы, вам неабходна глыбока пагрузіцца ў вашу кампанію і і вашыя прапановы. Гэта таксама азначае, што вам неабходна вызначыць, якія экасістэмы важныя для вас, і якую ролю вы будзеце гуляць у экасістэме.

Існуюць тры розныя ролі, якія ваша кампанія можа гуляць у экасістэме. Арганізатары экасістэмы бяруць на сябе рызыку, складанасць, а таксама праблемы пабудовы лічбавай экасістэмы. Гэта такія кампаніі, як Amazon, Alibaba і Ping, якія дазваляюць іншым удзельнічаць у экасістэме і прадаваць тавары і паслугі праз гэтую сістэму.

Модульныя вытворцы ўносяць свой уклад у экасістэму і манетызуе кошт у розных экасістэмах. Адным з самых вядомых вытворцаў модуляў

можа быць PayPal. З дапамогай сваіх паслуг яны прапануюць розныя платформы і экасістэмы паслугі, каб мець адзіны плацежны шлюз, каб кліенты маглі лёгка плаціць. Вытворца модуляў можа дадаць асноўныя паслугі да экасістэм, якія адказваюць патрэбнасцям спажыўцоў, бізнесу, а таксама пакупнікоў і прадаўцоў у пэўным сэнсе.

Кліентам можа быць чалавек ці прадпрыемства, якое атрымлівае выгаду з экасістэмы. Забраніраваўшы Airbnb, вы становіцеся кліентам экасістэмы, якую стварыў і арганізаваў Airbnb.

Часам межы бываюць зменлівымі. Так, напрыклад, карыстач Facebook з'яўляецца адначасова стваральнікам (кантэнт) і спажыўцом (рэклама). Акрамя таго, кампаніі могуць часам выкарыстоўваць, часам арганізоўваць, а часам дадаваць паслугі ў некалькі лічбавых экасістэм.

Існуюць тры тыпы лічбавых экасістэм. Функцыянальная лічбавая экасістэма звычайна будуецца вакол існуючага прадукта або прапановы кампаніі. У ёй удзельнічае абмежаваную колькасць кампаній і партнёраў (магчыма, 10-100). Яна засяроджана на ўнутраным аспекце.

Дзякуючы прастаце і лёгкасці інтэграцыі, гэта найболей шырока выкарыстоўваная экасістэма. Але і тут ёсць свае абмежаванні, паколькі збор даных і далейшая інтэграцыя абцяжараны, бо ў большасці выпадкаў гэта закрытая экасістэма.

Прыклады такіх функцыянальных экасістэм можна знайсці ў аўтамабільнай прамысловасці, дзе платформы падлучаюцца да лічбавых сэрвісаў партнёраў, ствараючы арыентаваную на прадукт экасістэму разумнага і падлучанага аўтамабіля з абмежаванай колькасцю прадуктаў.

Больш прасунутымі экасістэмамі з'яўляюцца экасістэмы лічбавых платформ. Яны могуць уключаць мільёны партнёраў, а таксама ўключаць мноства лічбавых прапаноў. Гэтыя лічбавыя экасістэмы заснаваныя на падыходзе "дадзеныя вышэй за ўсё", які дазваляе выкарыстоўваць інфармацыю аб кліенце для далейшага павышэння продажаў або распрацоўкі новых прапаноў на аснове атрыманых дадзеных.

Але самым вялікім адрозненнем з'яўляецца агульная платформа, на якой усе партнёры ўдзельнічаюць і ствараюць сваю каштоўнасць. Арганізатар экасістэмы прапануе агульную платформу, на якой усе падключаныя бакі працуюць разам.

Google дае агульную платформу, на якой распрацоўшчыкі, вытворцы і інжынеры могуць працаваць разам над стварэннем бытавой тэхнікі, якая выкарыстоўвае платформу Google Home, каб стаць падключанай і разумнай. Google сам распрацоўвае такія прылады, як хатні дынамік, але і партнёры могуць выкарыстоўваць экасістэму платформы, каб прапанаваць свае прадукты і паслугі.

Супер платформенныя экасістэмы звычайна складаюцца з мноства розных галін, розных паслуг і спрабуюць як мага лепш звязаць увесь шлях карыстача з экасістэмай. Большасць экасістэм супер платформаў знаходзяцца ва ўласнасці Apple, Google, Amazon і Tencent. WeChat дэманструе кітайскае супер дадатак.

Прыкладанні ахоплівае ўсе важныя аспекты жыцця карыстальніка. У рамках адзінай платформы яно прапануе тысячы паслуг і функцый, уключаючы паўсядзённыя банкаўскія аперацыі, сацыяльныя сеткі, пакупкі, зносіны і многае іншае. З кожнай новай прапановай WeChat усё больш інтэгруецца ў паўсядзённае жыццё, што дазваляе лепш збіраць дадзеныя, якія могуць прывесці да новых прапаноў і блакаванні.

Выклікі і рызыкі лічбавых экасістэм

Хоць лічбавыя экасістэмы валодаюць велізарным патэнцыялам для стварэння кошту і росты, яны таксама нясуць з сабой унікальны набор праблем і рызык з-за свайго памеру і складанасці.

Адным з галоўных пытанняў з'яўляецца канфідэнцыяльнасць і бяспека даных. Улічваючы вялікую колькасць дадзеных, якія адсочваюцца, перадаюцца і апрацоўваюцца ўнутры экасістэмы, існуе значная рызыка

ўцечкі дадзеных, няправільнага выкарыстання і кібернетычных нападаў, якія жадаюць займець гэтыя дадзеныя. Акрамя таго, залежнасць ад аднаго або некалькіх пастаўшчыкоў платформаў можа прывесці да манапольнага кантролю, што ў доўгатэрміновай перспектыве абмяжоўвае канкурэнцыю і інавацыі, а існуючыя плыні таксама спрабуюць прадухіліць гэта нарматыўна-прававым шляхам.

Для правайдэраў у экасістэме (модульных вытворцаў) таксама існуе рызыка стаць занадта залежнымі ад экасістэмы ў плане свайго бізнэсу, што робіць іх уразлівымі, калі экасістэма выйдзе са строю або істотна зменіцца. Падобныя праблемы для супольнасцяў і кампаній дэманстравалі прыклады Twitter і Reddit.

Для арганізатара экасістэмы сур'ёзнай праблемай і рызыкай, з'яўляецца сумяшчальнасць розных тэхналогій і сістэм унутры экасістэмы. Неадпаведныя ці несумяшчальныя тэхналагічныя стандарты могуць аказаць моцны ўплыў, таму Google і Facebook усталёўваюць свае ўласныя тэхналагічныя стандарты і распрацоўваюць іх самастойна.

У залежнасці ад бізнэс-мадэлі, нарматыўныя патрабаванні таксама з'яўляюцца праблемай. Паколькі лічбавыя экасістэмы складаныя і глабальныя, а нарматыўныя акты, якія датычацца абароны даных, адпаведнасці, антыманапольнага заканадаўства і іншых адпаведных палітык, неабходна пастаянна адсочваць і выконваць. Краіны часта не дапускаюцца да розных сэрвісаў.

Для стварэння экасістэмы неабходна шырокая кліенцкая база, паслядоўнае стварэнне кошту, дакладнае ўзгадненне розных партнёраў, кліентаў і тэхналогій, а таксама вельмі гнуткае мысленне.

Праца ў інтэрнэце спалучана з выкарыстаннем незлічоных пароляў і асобных лагінаў, рэгулярнымі запытамі адной і той жа інфармацыі пры стварэнні уліковых запісаў лічбавых сэрвісаў. Павінен быць больш бяспечны і эфектыўны спосаб абароны ад махлярства.

Неабходна ўдасканаліць метад лічбавай ідэнтыфікацыі і забяспечыць яе бяспеку такім чынам, каб дабіцца шырокага прымянення гэтага метаду. Улічваючы шэраг ініцыятыў у сферы лічбавай ідэнтыфікацыі, якія рэалізуюцца на сённяшні дзень, мінулыя няўдачы, а таксама праблемы канфідэнцыйнасці, з якімі трэба сутыкнуцца, нядзіўна, што іншы назіральнік разам з натхненнем праяўляе асцярожнасць і стрыманасць.

Банкі паспяхова ўвялі агульную лічбавую ідэнтыфікацыйную карту, якой карыстаюцца тры чвэрці насельніцтва краіны. Пры гэтым некаторыя праграмы пацярпелі няўдачу, сутыкнуўшыся з нязвыклымі нюансамі асваення новых тэхналогій і ўзаемадзеяння з рэгулятарнымі органамі і грамадскасцю. Шырокае распаўсюджванне лічбавых прылад з функцыяй ідэнтыфікацыі азначала б значнае паляпшэнне стану спраў.

Папяровыя дакументы пры адсутнасці надзейных метадаў аўтэнтыфікацыі вельмі ўразлівыя для крадзяжу і махлярства. Нават стандартныя меры бяспекі, уключаныя ў існыя лічбавыя сэрвісы, часта залежаць ад базавых метадаў аўтэнтыфікацыі (напрыклад, ад уразлівасці пароляў). Калі ўлічыць, што на сённяшні дзень 87% выпадкаў махлярства з выкарыстаннем персанальных дадзеных у Вялікабрытаніі адбываецца па лічбавых каналах, становіцца зразумела, што метады забеспячэння бяспекі павінны мяняцца па меры ўкаранення лічбавай эканомікі.

Тэстуюцца творчыя падыходы да прымянення дэцэнтралізаваных метадаў, каб не залежаць ад буйной цэнтралізаванай мадэлі базы даных, а таксама больш эфектыўна кіраваць гэтымі рызыкамі і зводзіць іх да мінімуму. Рызыкі можна паменшыць з дапамогай архітэктурных рашэнняў, якія дазваляюць звесці да мінімуму аб'ём дадзеных аб транзакцыях, якія збіраюцца падчас праверкі ідэнтыфікацыйных дадзеных.

Загадзя ўсталяваўшы выразныя прынцыпы канфідэнцыйнасці, і ўлучыўшы іх у аснову праектавання, можна ўбудаваць у гэтыя сістэмы неабходныя сродкі абароны. Такі падыход таксама дапаможа павысіць давер канчатковых карыстальнікаў да лічбавых тэхналогій і забяспечыць іх

шырокае прымяненне дзякуючы шматлікім перавагам лічбавай трансфармацыі. Праблемы ўкаранення лічбавай ідэнтыфікацыі не з'яўляюцца непераадольнымі.

Штучны інтэлект і лічбавая ідэнтычнасць фінансавых дадзеных

Гандлёвы працэс эвалюцыянаваў да стану, калі трэйдары выкарыстоўваюць складаныя параметры і камбінацыі фактараў, каб прыйсці да рашэння. Ад адзнак сацыяльных настрояў, праз тэхнічныя індыкатары да фундаментальнай інфармацыі – інвеставанне сёння складаней, чым калі-небудзь. Машыннае навучанне можа аблегчыць увесь працэс, аналізуючы вялікія кавалкі дадзеных, выяўляючы істотныя заканамернасці і генеруючы адзіную інфармацыю, якая накіроўвае трэйдараў да пэўнага рашэння, заснаванаму на прагназуемых цэнах актываў.

Фінансавыя рынкі, як правіла, непрадказальныя і нават нелагічныя. У сілу гэтых асаблівасцяў фінансавыя дадзеныя павінны разглядацца як якія маюць даволі хаатычную структуру, што часта абцяжарвае пошук устойлівых мадэляў. Для рашэння гэтай задачы алгарытм павінен быць забяспечаны як мага вялікай колькасцю аб'ектыўнай інфармацыі.

Мадэляванне хаатычных структур патрабуе алгарытмаў машыннага навучання, здольных знаходзіць утоеныя законы ў структуры дадзеных і прадказваць, як яны паўплываюць на яе ў будучыні. Найбольш эфектыўнай метадалогіяй для дасягнення гэтай мэты з'яўляецца глыбокае навучанне.

Павінна весціся праца над сферай ідэнтыфікацыі, аўтэнтыфікацыі і кіраванні лічбавай ідэнтычнасцю. Напрыклад, у банкаўскай сферы – забеспячэнне дыстанцыйнага доступу да паслуг банкаў, уключаючы ўкараненне адзіных падыходаў да праверкі звестак, якія забяспечваюцца банкам пры абслугоўванні кліентаў, у электроннай форме.

У выніку трэба прагназаваць павышэнне фінансавай уцягнутасці насельніцтва і павелічэнне спектра фінансавых паслуг. Кампетэнцыяй лічбавай эканомікі на дзяржаўным узроўні павінна быць узаемасувязь хуткіх працэсаў укаранення фінансавых інавацый (менш за тры месяцы) і адносна павольных працэдур змянення рэгулятыўнага асяроддзя (не менш за год), размыванне ўстояных межаў фінансавага рынку, павелічэнне складанасці і фрагментацыі прылады фінансавага рынку. Гэтыя праблемы ствараюць рызыкі ў стабільнасці функцыянавання фінансавай сістэмы.

У фінансавай сферы пачынаюць выкарыстоўвацца блокчэйн-тэхналогіі. Блокчейн – адзін з вызначальных трэндаў у фінтэх-галіны. Тэхналогія размеркаванага рэестра раней асацыявалася выключна з крыпта валютамі. Сёння блокчейн спрабуюць укараніць ва ўсе сферы, дзе неабходны кантроль над празрыстасцю і бяспекай здзелак. Тэхналогія размеркаванага рэестра, забяспечвае адмену пасярэдніцтва; павелічэнне хуткасці правядзення транзакцый; верыфікацыю здзелак.

Адным з варыянтаў выкарыстання блокчейна на крэдытным рынку можа стаць вызначэнне крэдытнага рэйтынгу фізічнай асобы для адабрэння або адмовы ў крэдыце.

Крэдытны скоринг з'яўляецца папулярным інструментам для вызначэння фінансавай здольнасці фізічнай асобы пагасіць суму доўгу за пэўны перыяд часу. Ацэнка звычайна вызначаецца кампаніямі крэдытнага саюза (некаторай колькасцю крэдытных арганізацый), якія, як правіла, аналізуюць кожны тып фінансавай аперацыі, якую зрабіў чалавек, якая з'яўляецца альбо крэдытам увогуле, альбо вядзеннем гісторыі тэрмінаў плацяжоў па розных крэдытных лініях канкрэтнага чалавека. Гэты агульны метад лічыцца дастаткова эфектыўным і з'яўляецца звычайнай крыніцай атрымання інфармацыі аб узроўні крэдытаздольнасці чалавека.

Але ёсць пэўныя фактары, якімі грэбуюць пры разліку крэдытнага рэйтынгу асобнага чалавека класічным спосабам. Напрыклад, гэта інфармацыя аб разліковых рахунках індывіда ў розных банках. Механізм

крэдытнага скоринга на аснове блокчейн-фрэймворка мае патэнцыял стаць больш эфектыўным. Дадзены механізм, заснаваны на блокчейн-фрэймворку, аналізуе мноства аспектаў крэдытнай і даходнай гісторый асобы з пункту гледжання фінансавай стабільнасці для эфектыўнага і дакладнага аналізу. Ён дазволіць аналізаваць не толькі стан рахункаў, але і паступленні адтоку, звязаныя з імі. Так, лічыцца, што сума крэдыту выводзіцца з банка на ўсе мэты фізічнай асобы.

Банк непасрэдна ўзаемадзейнічае з кліентам пры прадастаўленні неабходнага крэдыту. У гэтым выпадку дадзеныя кліента адносна інфармацыі аб некалькіх дэбетавых або крэдытных картах, страхоўцы, паступленнях заработнай платы загружаюцца стэйкхолдэрамі ў блокчейн-фрэймворк, створаны пад адзіную фізічную асобу. Дадзеныя, якія былі загружаныя ў блокчейн, правяраюцца ўсімі зацікаўленымі бакамі блокчейна бо зыходны код з'яўляецца адчыненым для праверкі дакладнасці і дакладнасці дадзеных.

Зацікаўленыя бакі ў дадзенай сетцы з'яўляюцца асноўнымі рэспандэнтамі пры загрузцы дадзеных аб транзакцыях, якія тычацца канкрэтнага кліента, у блокчэйн-сетку на аснове ідэнтыфікацыі кліента, якая ў далейшым будзе выкарыстоўвацца для кумулятыўнай ідэнтыфікацыі магчымасцяў або скоринга кліента. У выпадку, калі ў рэальным часе кліент звяртаецца да філіялу банка з заяўкай на пэўную суму крэдыту, банк на аснове працэсу ідэнтыфікацыі ініцыюе смарт-кантракт. Ен атрымлівае дадзеныя транзакцыі з блокчейна на аснове канкрэтнага кода ідэнтыфікацыі, які змяшчае поўныя дадзеныя транзакцыі кліента.

Дадзеныя перадаюцца агенту. Агент у сваю чаргу вылічае некалькі неабходных інфармацыйных аб'ектаў з інфармацыі, якая перадаецца ў мадэль машыннага навучання, якая з'яўляецца бінарнай класіфікацыйнай мадэллю, якая забяспечвае верагоднасць таго, ці зможа кліент пасля пагасіць патрабаваную суму ці не за пэўную колькасць часу. Прагнозы з мадэлі

машыннага навучання далей прымаюцца да ўвагі банкам, каб вырашыць, ці варта ўхваляць запыт на крэдыт ці не.

Крэдытны рынак актыўна прымяняе фінансавыя тэхналогіі. Напрыклад, вызначэнне крэдытнага рэйтынгу фізічнай асобы для адабрэння або адмовы ў крэдыце можа стаць больш эфектыўным дзякуючы тэхналогіі прымянення размеркаванага рэестра.

Лічбавая бяспека энергетычных кампаній

Кампаніі энергетыкі з'яўляюцца асноўнай мішэнню для кібератак з боку дзяржаў і кіберзлачынцаў, якія імкнуцца выкарыстоўваць гэты сектар у сваіх палітычных ці эканамічных мэтах. Энергетычная прамысловасць зведала хуткую цыфравізацыю, падаўшы новыя магчымасці кібернетычным злачынцам. Напады справакаваны высокім коштам актываў дадзеных энергетычнай галіны, а таксама аўтаматызаванымі і слаба абароненымі працэсамі і сеткамі. Асноўныя ўразлівасці энергетычнай галіны:

- састарэлае праграмнае забеспячэнне;
- адсутнасць бяспечнага выдаленага доступу;
- адсутнасць рэгулярнага кантролю канфігурацый і праграмнага забеспячэння;
- адсутнасць размежавання правоў доступу;
- адсутнасць рашэнняў па кантролі запуску прыкладанняў;
- адсутнасць сродкаў рэгістрацыі падзей інфармацыйнай бяспекі.

Задачы інфармацыйнай бяспекі ў энергетыцы:

- абарона тэхналагічных участкаў генерацыі электраэнергіі і дастаўкі канчатковым карыстальнікам;
- забеспячэнне бяспекі карпаратыўных рэсурсаў (інфармацыйная інфраструктура, вэб-рэсурсы);
- абарона канчатковых прылад;
- абарона адчувальнай інфармацыі і персанальных дадзеных;

− адпаведнасць патрабаванням рэгулятараў; прадухіленне ўцечак інфармацыі;

− выяўленне ўнутраных злоўжыванняў і нелаяльных супрацоўнікаў.

Эфектыўнае навучанне пытанням кібернетычнай бяспекі – яшчэ адна важная мера забеспячэння бяспекі арганізацый. Важна навучыць супрацоўнікаў выяўляць пагрозы фішынгу, сацыяльнай інжынерыі, каб гарантаваць бяспеку інфармацыі і ўліковых запісаў, тым самым знізіўшы рызыку ўзлому.

Атрымліваючы інфармацыю аб найноўшых пагрозах бяспекі, усталёўваючы сучасныя сродкі абароны інфармацыі, захоўваючы бачнасць сваёй і іншай IT-інфраструктуры, а таксама падтрымліваючы проактивную бяспеку і моцную культуру дасведчанасці аб рызыках, арганізацыі ў энергетычнай галіне могуць прадухіліць магчымыя напады на свае рэсурсы.

Рашэнні кібернетычнай бяспекі для энергетыкі:

− рэгулярныя трэнінгі для павышэння дасведчанасці персаналу ў пытаннях інфармацыйнай бяспекі;

− аўдыт інфармацыйнай бяспекі і прылады сканавання сеткі для выяўлення і прадухіленні эксплуатацыі ўразлівасцяў, своечасовага патчынгу;

− карэктная сегментацыя сеткі для лепшага кантролю сеткавага трафіку і падвышэнні эфектыўнасці сістэм кібернетычнай бяспекі;

− сістэмы аховы для падтрымання бесперапыннасці тэхналагічнага працэсу;

− Network Traffic Analysis для выяўленне анамалій у трафіку і выяўленне кібернетычных нападаў на ранніх этапах;

− міжсеткавыя экраны і сістэмы выяўлення і прадухіленні ўварванняў (IDS/IPS) для абарона перыметра сеткі, блакіроўка несанкцыянаванага доступу і выяўленні патэнцыйна шкоднаснага трафіку;

− WAF (Web Application Firewall) для абароны вэб-рэсурсаў з дапамогай міжсеткавых экранаў прыкладанняў ад такіх нападаў, як міжсайтавая

падробка запыту (CSRF), міжсайтавы скрыптынг (XSS), SQL-ін'екцыя і іншых пагроз;

− абарона канчатковых кропак для зніжэння рызыкі заражэння праграмамі і вірусамі, шыфравання інфармацыі, захавання адпаведнасці палітыкам; арганізацыя бяспечнага выдаленага доступу да сеткі і стварэння зашыфраванага канала сувязі з дапамогай сродкаў крыптаграфічнай абароны інфармацыі рэгулятараў;

− DLP сістэмы для прадухілення ўцечкі канфідэнцыйных матэрыялаў, а менавіта аналізу і блакіроўкі дадзеных, якія перадаюцца з дапамогай электроннай пошты, месэнджараў, інтэрнэт-рэсурсаў і іншых крыніц;

− сістэмы кіравання доступам (IDM, PIM) для кантролю жыццёвага цыкла уліковых запісаў і размежаванні правоў доступу да сегментаў сеткі;

− рашэнні для кіравання сеткавым доступам (NAC) для інвентарызацыі прылад, забеспячэнні бачнасці і кантролю падлучэнняў да карпаратыўнай сеткі;

− сістэмы класіфікацыі даных для павышэння бяспекі канфідэнцыйнай інфармацыі шляхам класіфікацыі, вызначэння карыстальнікаў, якія ўзаемадзейнічалі з дакументамі, спрашчэння доступу, пошуку і адсочвання даных, а таксама ўстаранення дубліравання; выкарыстанне інтэрактыўных пастак для эфектыўнага выяўлення APT-нападаў;

− SIEM сістэмы для цэнтралізаванага маніторынгу інфармацыйнай бяспекі, збору і аналізу дадзеных ад інструментаў кібернетычнай бяспекі.

Бяспека экасістэмы IoT

Пастаўшчыкі паслуг і прылад рынку IoT парушаюць прынцып скразной інфармацыйнай бяспекі, які рэкамендаваны для ўсіх прадуктаў і паслуг. Згодна з гэтым прынцыпам, інфармацыйная бяспека павінна закладвацца на пачатковай стадыі праектавання прадукта або паслугі і падтрымлівацца аж да завяршэння іх жыццёвага цыклу.

Паколькі не ўсе прыборы маюць убудаваныя сродкі абароны, уладальнікам таксама варта паклапаціцца аб усталёўцы вонкавай абароны, прызначанай для хатняга выкарыстання, з тым каб інтэрнэт-прылады не сталі адчыненымі шлюзамі ў хатнюю сетку ці прамымі прыладамі прычынення шкоды. Бяспечнай экасістэмы IoT на сённяшні дзень не існуе.

Адмысловую небяспеку рэчы Інтэрнэту ўтойваюць у сабе ў кантэксце распаўсюджвання мэтавых нападаў. Варта толькі зламыснікам праявіць цікавасць і гаджэты ператвараюцца ў здраднікаў, якія адкрываюць доступ у свет сваіх уладальнікаў. Слабыя месцы IoT:

- пераход на электронную валюту;
- харчаванне датчыкаў;
- стандартызацыя архітэктуры і пратаколаў, сертыфікацыя прылад;
- інфармацыйная бяспека; стандартныя ўліковыя запісы ад вытворцы, слабая аўтэнтыфікацыя;
- адсутнасць падтрымкі з боку вытворцы для ўхілення ўразлівасцяў;
- выкарыстанне тэкставых пратаколаў і непатрэбных адчыненых партоў;
- выкарыстанне неабароненых мабільных тэхналогій; выкарыстанне неабароненай хмарнай інфраструктуры;
- выкарыстанне ня бяспечнага праграмнага забеспячэння.

Бяспека метасусветаў

Нягледзячы на тое, што канцэпцыя метасусвету застаецца расплывістай, яе папулярнасць імкліва расце. У сувязі з гэтым узніклі асцярогі наконт бяспекі новага метаміру. Кібернетычныя атакі знойдуць свой шлях у метасусвет, што падкрэслівае неабходнасць паклапаціцца аб бяспецы імерсіўных светаў. Выпадак з карыстальніцай, якая падверглася лічбаваму харассменту, заахвоціў Meta увесці сістэму «асабістых меж». На сапраўдны

момант агульнапрынятых законаў і спадарожных мер пакарання ў метасусвету не існуе.

Іншае пытанне, які цікавіць спецыялістаў па бяспецы, – гэта канфідэнцыяльнасць карыстальнікаў. Мае месца мноства ўзломаў і фальсіфікацыі розных гульнявых акаўнтаў, таму справядліва выказаць здагадку, што новы сусвет з велізарнай колькасцю забаўляльных сэрвісаў сутыкнецца з падобнай праблемай.

Адным з ключавых элементаў, якія маюць патрэбу ў абароне, з'яўляецца лічбавая ідэнтыфікацыя кожнага карыстальніка. Бо профіль будзе змяшчаць значна больш асабістай інфармацыі, чым уліковы запіс Google або Facebook. Метасусвет ўвасобіць усё лічбавае жыццё, з банкаўскім рахункам і іншымі канфідэнцыйнымі дадзенымі, дзе абарона ад крадзяжу будзе вырашальным фактарам.

Не менш важнай будзе і гарантыя таго, што карыстачы не змогуць падрабіць чужую асобу. Механізм пацверджання асобы важны. Аднак да гэтага часу незразумела, як можна прадухіліць спуфінг ў метасусвету.

Спуфінг – гэта тып махлярства, пры якім злачынец маскіруе адрас электроннай пошты, якое адлюстроўваецца імя, нумар тэлефона або URL-адрас сайта, каб пераканаць ахвяру ў тым, што яна ўзаемадзейнічаюць з даверанай крыніцай.

Зламыснік зможа атрымаць доступ нават да такой інфармацыі, як частата сардэчных скарачэнняў, рух вачэй і пальцаў. Біяметрычныя дадзеныя карыстальнікаў з'яўляюцца асабліва адчувальнай інфармацыяй, якую, у адрозненне ад нумара банкаўскай карты і пароля ад уліковага запісу, змяніць немагчыма.

Без належнай увагі да абароны дадзеных метасвет стане яшчэ адной прасторай, дзе напады на карыстальнікаў будуць рабіцца для атрымання выгады. Улічваючы тое, як цяжка абараніць інтэлектуальную ўласнасць у фізічным свеце, зразумела, што забяспечыць абарону аўтарскіх правоў у метасусвеце будзе яшчэ складаней.

Якімі б складанымі ні былі прыёмы абыходу мер бяспекі, бізнэсу неабходна быць на крок наперадзе кібернетычных злачынцаў. Існуюць праблемы бяспекі, характэрныя менавіта для метасусвету і такіх тэхналогій, як блокчейн, криптовалюты і NFT.

Non-fungible token, у перакладзе з англ. – «неўзаемазаменны токен» – гэта спосаб валодання лічбавым мастацтвам у форме музыкі, выявы, анімацыі. Значная рызыка NFT звязаны з магчымай купляй падробленых неўзаемазаменных токенаў. Зламыснікі могуць выдаваць сябе за вядомых аўтараў і прадаваць падробленыя пасведчанні аб праве ўласнасці.

У цяперашні час не існуе даступнай сістэмы бяспекі для абароны метасусвету ад шкоднасных праграм. Асабліва востра стаіць пытанне распрацоўкі вялікай колькасці стандартаў бяспекі: зрабіць гэта неабходна ў максімальна кароткія тэрміны.

Імерсіўны віртуальны свет сёння існуе без законаў. Таму немагчыма скласці спіс рэкамендацый па абароне асобы ў лічбавым свеце. Можна толькі паспрабаваць прадказаць некаторыя праблемы.

Метасусвет закладзе новыя патэрны паводзін, атакавалы будзе больш прывілеяваны і будзе імкнуцца ўзламаць сістэму, а не людзей. Яшчэ больш актуальнымі стануць пытанні, злучаныя з ідэнтыфікацыяй і аўтарызацыяй карыстачоў. Улічваючы дадатковы ўзровень абстракцыі, выкарыстанне чужых асоб (Identity Theft) пры здзяйсненні пэўных дзеянняў (афармлення ўласнасці, плацяжоў, пакупак і інш.) стане нормай гэтай новай "рэальнасці". На жаль, нягледзячы на паўсюднае ўкараненне passwordless тэхналогій і MFA, вырашыць гэтую праблему ў рэальным свеце да гэтага часу не ўдаецца, а канцэпцыя метасусветаў яшчэ больш ускладніць яе рашэнне.

Лічбавы харассмент

На фоне развіцця метасусветаў у сетцы пачалі з'яўляцца паведамленні аб дамаганнях, з якімі сутыкаюцца карыстачы віртуальных міроў. Пры гэтым

часта лічбавы харрасмент прыводзіць да такой жа псіхалагічнай шкоды, як і звычайныя дамаганні, аднак значна горш рэгулюецца заканадаўствам.

У канцы 2021 г. Ніна Джэйн Патель з Брытаніі стварыла ўласны аватар у метасусвету Horizon Venues. У гульнявой прасторы на яе персанажа напалі трое іншых аватараў, як мяркуецца, мужчынскага полу. Аватар жанчыны падвергся пераследу і нападу адразу пасля з'яўлення ў гульнявой прасторы Horizon Venues. Банда з трох аватараў-мужчын наблізілася да створанага Джэйн персанажа, яе ўдзельнікі пачалі агрэсіўна абмацваць яго.

Таксама яны адпускалі сэксуальныя каментарыі ў адрас жанчыны і рабілі скрыншоты. Каб уцячы ад гвалтаўнікоў Ніне Джэйн Патель прыйшлося адключыцца ад сеткі. Жанчына пасля лічбавага дамагання пачала пакутаваць ад трывожнасці. Узнікла праблема бяспекі жанчын у віртуальным асяроддзі.

Харасмэнт з'яўляецца актуальнай і вельмі небяспечнай формай сэксуальных дамаганняў, прымусам да іх здзяйснення. Па сваёй прававой прыродзе такія дзеянні з'яўляюцца самым грубым умяшаннем у прыватнае жыццё грамадзяніна.

Да харассмента могуць ставіцца, такія дзеянні як: перыядычныя непрыемныя жарты, недарэчны і агрэсіўны флірт, настойлівая ўвага, а таксама намёкі і запалохванні сэксуальнага падтэксту, у тым ліку і непасрэдна фізічныя кантакты з аб'ектам харассмента. У рэальным жыцці харассмент падпадае пад заканадаўчае рэгуляванне, хоць і такога рэгулявання аказваецца недастаткова.

З лічбавым харассментам у віртуальным асяроддзі справы сітуацыя горшая. Пакуль выпадкі лічбавага харрасмента расследуюць толькі кампаніі, якія прадстаўляюць доступ да платформы. Знаходжанне ў віртуальнай рэальнасці рэгулюецца карыстацкай дамовай, якое падпісваюць людзі для доступу да прыкладанняў.

Адпаведна, у кампаній-праваўладальнікаў і распрацоўшчыкаў ёсць поўны "карт-бланш" для вырашэння ўзнікаюць у віртуальным асяроддзі праблем (у тым ліку і ў пытанні харассмента).

Кампанія Microsoft выдаліла такія сацыяльныя цэнтры як Campfire, News і Entertainment Commons на VR-платформе AltspaceVR, якія дапамагалі людзям сустракацца і мець зносіны ў лічбавым асяроддзі. Радыкальнае рашэнне было прынята ў сувязі з частымі выпадкамі дамаганняў у віртуальнай рэальнасці.

Таксама кампанія па змаўчанні замацавала за кожным з карыстачоў віртуальнай сусвету функцыю "бурбалка бяспекі". Опцыя дапамагае ствараць фізічныя бар'еры паміж карыстальнікамі, якія кантактуюць, і не дазваляе парушаць асабістую прастору кожнага з іх.

Дадаткова кампанія ўзмацніла кантроль уваходу ў платформу новых карыстальнікаў. Зараз для выкарыстання сэрвісаў віртуальнай сусвету неабходны ўліковы запіс Microsoft. Кампанія прыняла рашэнне зрабіць тэхнічную сінхранізацыю акаўнтаў з дадаткам Microsoft Family Safety. Рашэнне дазволіць кантраляваць допуску дзяцей да прыкладанняў VR.

Небяспекі віртуальнай рэальнасці

Тэхналогіі віртуальнай рэальнасці маюць адмысловую гарнітуру шлемаў. Пачнем з філасофскай шкоды ад віртуальнай рэальнасці – эскапізму. Эскапізмам завуць сыход (уцёкі) ад цяжкасцяў, нуды жыцця ў выдуманы свет. Практычна ўсіх геймераў і аматараў віртуальнага свету можна аднесці да эскапістаў. Эскапізм не лічыцца хваробай. Эскапістамі былі такія знакамітыя людзі, як пісьменнік Леў Талстой, музыка Сід Барэт.

Джон Рональд Руэл Толкін, лічыў эскапізм неабходнай складнікам творчага развіцця асобы. Яго сцвярджэнне пацвярджаецца тым, што маса заўсёднікаў віртуальнай рэальнасці піша кнігі. У сувязі з гэтым зьявіўся новы, асобны жанр.

Існуюць 2 віды эскапізму – добраахвотны і вымушаны эскапізмы. Істотнае адрозненне паміж добраахвотным эскапізмам і змушаным складаецца ў тым, што пры добраахвотным эскапізме чалавек сам выбірае выяву жыцця пустэльніка, адмаўляючыся ад "мірскай мітусні". У якасці прыкладу можна правесці паралель з тэорыяй псіхааналітыка Карэн Хорн аб пустэльніцтве, як неўратычнай рэакцыі на жыццё.

Пры змушаным эскапізме геймера засмоктвае ў віртуальную рэальнасць супраць яго волі. Паралель: п'янства, курэнне, наркаманія. Карыстальнік не ўсведамляе выдуманасць навакольнага свету. У момант вяртання з VR, змірыцца з рэальнасцю не дазваляюць якія ўзніклі на фоне яе злоўжывання захворванні, такія як дэперсаналізацыя і дэзадаптацыя.

Адбываецца страта ўласнай асобы і арыентацыі ў рэальным свеце, знікаюць побытавыя навыкі. Абвыкшы з лёгкасцю «забіваць цвікі» у гульні, чалавек не можа забіць сапраўдны цвік. Ідзе падмена рэакцый на падзеі, абясцэньванне сацыяльных установак. Віртуальная рэальнасць даводзіць да неўратычных захворванняў і поўнага догляду ў VR, што прыводзіць да псіхічных захворванняў.

Абвыкшы лёгка забіваць у гульні, карыстач з лёгкасцю можа стаць забойцам і ў рэальным свеце. У сувязі з гэтым, гульні, якія змяшчаюць сцэны жорсткасці, неабходна забараніць. Але сярод карыстальнікаў VR працэнт гвалту ніжэйшы, чым у іншых катэгорыях грамадзян.

У віртуальным свеце гулец губляецца. Яго меркаванне аб сабе фармуецца па водгуках іншых гульцоў, якія ў сваю чаргу засноўваюцца на выкананні ім выдуманых заданняў.

Абвыкаючы да таго, што сілу, здароўе і маладосць можна з лёгкасцю атрымаць ці папоўніць, паспяхова выканаўшы шэраг заданняў, а пры няўдалым зыходзе пачаць гуляць (жыць) нанова, геймер перастае зважаць на рэальны стан свайго фізічнага здароўя.

Для памяншэння ўплыву на фізічнае здароўе, для «якія завісаюць» працяглы час у віртуальнай рэальнасці геймераў, вядуцца распрацоўкі па

вынаходстве «капсул поўнага апускання» – з масажам і трэніроўкай фізічных функцый. Датуль, пакуль такія капсулы не ідуць у камплекце да VR шлема ці ачкам, гулец можа забыцца пра гігіену, а гэтак жа прапусціць развіццё сур'ёзнага захворвання.

Віртуальная рэальнасць адмоўна ўплывае на шматлікія псіхалагічныя працэсы, якія праходзяць у арганізме чалавека. Да мінусаў віртуальнай рэальнасці можна аднесці пагаршэнне доўгачасовай памяці. Пагаршэнне памяці ўплывае не толькі выкарыстанне VR. Дадзеная заканамернасць назіраецца ва ўсіх актыўных карыстальнікаў Інтэрнета. Напрыклад яшчэ некалькі гадоў таму, для таго, каб даведацца аб чым-небудзь патрабавалася наведаць бібліятэку, адшукаць патрэбную кнігу, знайсці ў ёй неабходную інфармацыю і запісаць яе. У выніку ведаў становіцца больш, але ў нас яны не затрымоўваюцца, бо дастаюцца занадта лёгка.

Віртуальная рэальнасць спрыяе развіццю ўвагі, але некалькі аднабакова. VR найбольш згубна ўздзейнічае на мысленне карыстальніка. Адбываецца падмена паняццяў, рэакцый на выдуманую падзею. Напрыклад чалавек, які навучыўся ў віртуальнай рэальнасці скакаць з парашутам, у рэальным свеце не ўсведамляе, што яго гульнявыя навыкі ў гэтай справе яму не дапамогуць.

На гэтае моцнае ўздзеянне звярнулі ўвагу фірмы-вытворцы шлемаў VR трэнажораў (Varjo, VR-2 Pro, StarVR). Напрыклад пажарныя, пры выкарыстанні VR трэнажораў, дэманстравалі выдатны вынік па выніковым тэставанні ў VR. Аднак у жыцці, сутыкнуўшыся з рэальным пажарам, яны губляліся.

VR трэнажоры адно з важных напрамкаў выкарыстання віртуальнай рэальнасці. Таму вытворцы шукаюць выйсце з сітуацыі, якая склалася. Шлемы забяспечваюцца дадатковымі трэкерамі, бегавымі дарожкамі, трэнажорамі (для адчувальнасці цяжар вогнетушыцеля), кантролерамі. Вырашэнне гэтай праблемы яшчэ не знойдзена, але на яе пошукі

выдзяляецца вялізнае фінансаванне і верагодна, у хуткім будучым, яна будзе вырашана.

Яшчэ адзін мінус віртуальнай рэальнасці складаецца ў тым, што сцэнары для гульняў пішуць людзі. Звычайныя, наёмныя сцэнарысты са сваімі комплексамі ў галаве. Сцэнары да віртуальных гульняў могуць выкарыстоўвацца ў якасці прапаганды, навязвання меркавання ці думак.

Над імі ажыццяўляецца пільны кантроль, сцэнары для гульняў праходзячы масу праверак, перад тым як паступіць у продаж. Нягледзячы на гэта на тую ці іншую гульню ўзнікае мноства скаргаў.

Напрыклад людзі скардзяцца на тое, што зласлівыя людаеды-оркі амаль усе пагалоўна маюць рускія імёны. Увесь час гуляючы ў гэтую гульню рускія імёны для карыстача пачнуць трывала асацыявацца са злосцю і людаедствам.

У гульнях юзэр часта блукае па калена ў крыві, бачыць пацярпелых з цяжкімі траўмамі. У наступстве пры аўтакатастрофе ці іншага віду здарэння, натуральнай чалавечай рэакцыяй стала б аказанне першай дапамогі. Аднак геймер, убачыўшы такую карціну, не надасць ёй вялізнага значэння. У яго галаве можа нават не ўзнікнуць думкі аб дапамозе пацярпелым, узамен гэтага ён дастане свой смартфон і стане здымаць усё на відэа.

Варта адзначыць, што такія паводзіны, адносіцца да тых карыстальнікаў, якія "жывуць у VR", а не карыстаюцца ёй час ад часу.

Дадзеныя паводзіны з'яўляецца вялізным мінусаў ўплыву віртуальнай рэальнасці. Выйсця з гэтай сітуацыі пакуль не прыдумалі. Распрацоўнікі VR гульняў папярэджваюць аб тым, што не трэба імі марнатравіць. Гульцу неабходна валодаць крытычным мысленнем, цвяроза ўсведамляць свае дзеянні, то дзе ты знаходзішся, пазбягаць прывыканні. Аднак пры гэтым, вытворцы ўвесь час удасканальваюць VR гульні, каб людзі былі цалкам у іх уцягнутыя.

Фізічная шкода ад віртуальнай рэальнасці аспрэчваецца аўтарытэтнымі адвакатамі, найманымі кампаніямі-вытворцамі ці іх рэкламнымі агентамі. Таму заклікаць іх да адказнасці практычна немагчыма.

Даўно ўсталяваны факт таго, што VR выклікае ўкалыхванне, галавакружэнне і млоснасць – асабліва падчас першага яе выкарыстання. Чыннікам гэтага з'яўляецца неадпаведнасць нагрузкі, якую наш мозг можа ўспрыняць. Дзеянні адбываюцца віртуальнай рэальнасці супярэчаць фізічнаму стану геймера ў гэты момант. Напрыклад, паводле гульні, карыстач скача ў прорву, мозг гэта візуальна ўсведамляе, а ў рэальнасці карыстач варта на месцы.

У пазбяганне пабочных эфектаў ад выкарыстання віртуальнай рэальнасці ў VR-шлемах увесь час удасканальваецца частата «кадра» (абнаўленні экрана) і трэкінг. Гэтак жа вытворцы папярэджваюць, што пры першых выпадках млоснасці ці галавакружэння, трэба тэрмінова зрабіць перапынак ці зусім адмовіцца ад далейшай гульні.

На фоне апускання ў віртуальную рэальнасць у геймера можа ўзнікнуць астыгматызм. Чыннікам гэтага служыць тое, што вочы карыстача абвыкаюць глядзець у VR на адну пэўную адлегласць (экран знаходзіцца ў адным і тым жа месцы). Пры зняцці VR шлема карыстальнік гледзячы на рэальныя аб'екты выяўляе, што яны знаходзяцца на розных адлегласцях, у выніку чаго вочы даводзіцца напружваць.

Як бы не ўдасканальваліся экраны, колькі б пікселяў не ўкладвалі ў карцінку, малюнак VR ачкоў і VR шлемаў даюць мігаценне. Гэта спрыяе развіццю эпілепсіі. Варта адзначыць, што вытворцы ўкладваюць вялікую колькасць грошай, накіраваных на павышэнне бяспекі выкарыстання прылад віртуальнай рэальнасці, але рызыка будзе прысутнічаць заўсёды.

Не варта марнатравіць віртуальнай рэальнасцю. Пры дрэнным самаадчуванні ці прыёме медыкаментаў варта адмовіцца ад паводзін вечара за каханай гульнёй. Можна нанесці фізічную шкоду сабе і сваім блізкім.

Небяспекі імерсіўнага асяроддзя

Іммерсіўнае асяроддзе стварае эфект прысутнасці. За кошт гэтых уласцівасцей можна разглядаць імерсіўны тэатр як спектакль, у якім гледачы

дзейнічаюць у спектаклі нароўні з акцёрамі, а не толькі назіраюць за тым, што адбываецца на сцэне. Становяцца не спажыўцамі відовішча, а саўдзельнікамі дзеяння. Такі фармат дае гледачу роўныя правы і абавязкі, якія раней належалі толькі акцёру. Гэта гісторыі пра межы этыкі. Досвед можа валодаць не толькі дадатнымі характарыстыкамі.

Базавая небяспека ўзнікае на розніцы паміж успрыманнем класічнага тэатра і імерсіўнага. І вось чаму – існуе сакрэтная, але ўсімі інтуітыўна прыманая і падзяляная канвенцыя. Яе апісвае Эрфін Гофман: Дзеянне, пастаўленае ў тэатры, уяўляе ўмоўную, прыдуманую ілюзію, пра што ўсё выдатна ведаюць. У адрозненне ад звычайнага жыцця, нічога рэальнага ці сапраўднага не можа здарыцца з прэзентамі, якія прадстаўляюцца на сцэне. Імерсіўныя фарматы яе парушаюць. Састарэлая сакрэтная канцэпцыя спараджае ілюзію бяспекі.

У бяспечнай прасторы ўжо ёсць некаторыя рызыкі. На хорар квэсты вы паспяхова пагрузіліся ў атмасферу жаху, пабеглі ад маньяка, спатыкнуліся, рассеклі скуру на твары або проста выцяліся. Задавальнення мала. Гэта прыклад, калі ўдзельнік наносіць сабе шкоду сам.

У класічным тэатры такая небяспека не існуе. Ёсць і іншы бок. Вядомыя выпадкі на хорар квэстах, калі ўдзельнікі рэфлекторна білі акцёраў. Больш небяспечны псіхалагічны страх – не сінхранізавацца з іншымі ўдзельнікамі, выпасці са спектакля ці сапсаваць яго частку для астатніх. У выпадку з класічным тэатрам, гэтай рызыкі не існавала б.

Некаторыя эвенты мяркуюць высокі ўзровень шчырасці. Прычым шчырасці не персанажа, а выканаўцы. Удзельнік атрымлівае права, а ў некаторых выпадках і абавязак выказаць сваё меркаванне. І як у выпадку з любым публічным выказваннем меркавання – з правам прыходзіць і адказнасць за словы. І гэтая адказнасць можа дагнаць удзельніка самым розным чынам. Людзі цалкам могуць змяніць меркаванне аб гэтым чалавеку. Магчыма, гэта раней якое хаваецца, але публічна задэкларованае меркаванне адаб'ецца на яго рэпутацыі на працы, у сям'і і сярод сяброў.

Гледачы давяраюць акцёрам і рэжысёру, калі яны просяць зрабіць нейкае дзеянне. Але трэба разумець, што гэтыя дзеянні – накіраваныя на дасягненні нейкай ім, а не нам вядомай мэты. Хутчэй за ўсё гэтая мэта эстэтычная, а задача аўтара – рэалізацыя яго задумы. І ёсць ненулявая верагоднасць, што, выкарыстоўваючы для ўцягвання гледача ў спектакль інструменты з ролевых гульняў і псіхатэрапіі, аўтары толькі аб задуме і думаюць. А аб адказнасці або наступствах – не.

Пры гэтым прылады могуць быць даволі магутнымі, і без наступнага суправаджэння ў індывідуальных выпадках могуць выклікаць рэтраўматызацыю ўдзельніка. Таксама не трэба забываць, што адной з мэт любой мастацкай праявы можа быць эпатаж, а ў гэтым выпадку аўтар ці наўрад схільны задумвацца аб камфорце або бяспецы ўдзельніка.

У скандынаўскай практыцы ролевых гульняў (у норгаў вельмі магутная школа, якая датуецца на дзяржаўным узроўні, а ў некаторых выпадках выкарыстоўваная як прылада прапаганды) існуе такі тэрмін як "bleeding" – праходжанне, перанос эмоцый і матывацый з персанажа ва ўдзельніка. Калі ўдзельнік пачынае адчуваць тое ж, што і персанаж.

З аднаго боку, ці гэта не мэта імерсіўнага спектакля – максімальна глыбокае апусканне? З іншага боку, гэта прамы шлях да рэтраўматызацыі ці сама меней сапсаванаму настрою.

Уваходзячы ў тэатр глядач падпісвае негалосную канвенцыю даверу, давяраючы сваё жыццё рэжысёру. Можна паглядзець, як гэта выглядала на прыкладзе "Груз 300", дзе аўтары зрабілі роўна тыя ж умовы што і Зімбарда, толькі выкруцілі налады на хард – таксама дзеля мастацкай задумы.

Як зараз вырашаецца пытанне бяспекі? Ды практычна ніяк. З квэстаў-перформансаў можна сысці, памахаўшы ў камеру назіральніку. Але гэта ўвогуле не перакрывае астатнія, пералічаныя вышэй рызыкі.

Тэатры ўводзяць падпісныя формы згоды. Але яны абараняюць не гледача. Яны абараняюць аўтараў ад юрыдычнага пераследу і акцёраў ад непажаданага фізічнага кантакту. І наадварот, даюць права аўтару на

парушэнне вашай бяспекі. На некаторых эвентах, у прыватнасці на "Грузе 300", абазначана наяўнасць псіхалагічнай падтрымкі пры неабходнасці пасля спектакля. Бяспека ў імерсіўных тэатрах зараз не ажыццяўляецца.

Але можна пачаць з нарматыўнай метадалогіі. Не прасіць удзельнікаў рабіць нешта, што крымінальны кодэкс разглядае як парушэньне. І самім не рабіць гэтага з гледачамі. Патрэбна двухбаковая канвенцыя. Не толькі інфармаваная згода, але і сапраўды апісаны ўзровень узаемадзеяння на дадзеным эвенце.

Што можна рабіць і што нельга – правілы паводзін і ўдзелы. Папярэджанне аб фізічных небяспеках, якія могуць быць закладзены ў эвент. Калі будуць гучна "страляць" – пішыце, што будуць гучныя, палохалыя гукі. Калі выкарыстоўваеце страбаскоп – пішыце, што эпілептыкам наведванне эвенту можа апынуцца не занадта карысным. Калі мяркуецца глядзельная дэпрывацыя (штучнае абмежаванне зроку) – папярэдзіце пра гэта.

Патрэбна празрыстасць правілаў. Правілы ўдзелу і паводзін павінны быць вядомыя цалкам і загадзя, каб рашэнне аб тым, ісці на спектакль ці не, можна было прыняць на іх падставе да. А не калі цябе завуць шаўкай і малююць на лбе фалас. Не павінна пакутаваць і падвяргацца зневажэнням асоба ўдзельніка. Чалавек не павінен аказвацца ў зневажальным становішчы. Пытанне этыкі павінна спыніць аўтара і выразна паказаць яму мяжу.

Калі вы гуляеце сябе, вы несяце не толькі рызыка рэпутацыі, але і спрашчаеце спрацоўванне ўсіх псіхалагічных трыгераў, якія могуць супасці з вашым папярэднім, часам траўматычным досведам. Нават нягледзячы на тое, што непрафесіянал не прывучаны адштукаваць сваё Я ад свайго персанажа, наяўнасць ролі ўсё роўна гуляе ролю буфера. І лепш такі буфер, чым ніякага, асабліва калі прастора эвенту змяшчае ў сабе дадатковыя механізмы, якія дазваляюць аддзяліць сябе ад персанажа.

Хёйзінга Ё. ў "Чалавеку гуляючым" уводзіць такі тэрмін, як "Магічнае кола". Гэта асаблівая прастора і час, дзе правілы рэальнага свету саступаюць

месца правілам гульні. Чалавек, які аказваецца ў ім, цалкам можа адмовіцца ўспрымаць рэальнасць, якая існуе за межамі гэтай прасторы.

Многім знаёма вельмі глыбокае апусканне ў кампутарныя гульні або крайнюю ступень засяроджанасці на партыі ў настольныя протаваргеймы тыпу шахмат або Го, калі навакольнае рэальнасць перастае існаваць. Праца з Магічным кругам мае на ўвазе дэманстрацыю вельмі выразнай мяжы – пераступіўшы гэты парог, ты апыняешся ў прасторы, дзе дзейнічаюць іншыя, чым у рэальным жыцці правілы. Цяпер ты абавязаны выконваць іх увесь час пакуль ты знаходзішся ў гэтых межах.

І яшчэ вельмі важная рэч у Магічным крузе і яго арганізацыі – гэта вельмі выразная дэманстрацыя таго, што эвент – скончаны. Усё, фініш, выйшаўшы з круга, ты пакінуў свайго персанажа ўнутры і зараз павінен разглядаць тое, што адбылося, не яго вачыма, а сваімі ўласнымі.

Павінна быць права на дапамогу. Дамоўленасць аб тым, як чалавек можа папрасіць аб дапамозе або зніжэнні нагрузкі не патрабуючы для гэтага перапынення эвенту. Апусканне можа апынуцца занадта глыбокім, настолькі, што становіцца некамфортным.

Пры гэтым удзельнік у далейшым можа вярнуцца і не выпадаць з дзеяння цалкам. Акцёр таксама можа карыстацца правам прыпыніць самавыяўленне ўдзельніка, які пагрузіўся настолькі, што выходзіць за межы правілаў. У правілах заўсёды павінна быць дакладна прапісана права на выхад з эвенту. Гэта дапамагае ўдзельніку не адчуваць сябе закладнікам тэатра, абавязаным прытрымлівацца ўсяго, што з ім там робяць.

Ніводнае з прапанаваных рашэнняў не прыбірае небяспеку. Але ёсць спосаб пазмагацца і з гэтым – выкарыстоўваць на першым такце мерапрыемства практыкаванне на разняволенне. Можа аказацца важным не пакідаць удзельніка сам-насам з атрыманым вопытам, а дапамагчы яму падзяліць і вопыт і эмоцыі паміж іншымі ўдзельнікамі.

Па-першае гэта дапаможа прысвоіць вынік эвенту, а па-другое згладзіць перажыванні ці непрыемную частку досведу, падзяліўшыся ёю з

іншымі. Не выкідваць чалавека на вуліцу, а дапамагчы ператварыць усё што ён набыў унутры дзеянні – у калі не пазітыўны, то ў канструктыўны досвед.

Уважліва чытайце канвенцыю. Яна можа быць выказана ў выглядзе правілаў удзелу, "інфармаваную згоду". Зразумейце, на што вы падпісваецеся і скарэктуйце сваё ўяўленне аб бяспецы прасторы, у якую вы ідзяце за новым досведам. Калі канвенцыі ўвогуле няма – гэта ўжо не вельмі добры знак.

Калі вы прачыталі канвенцыю і нешта не зразумелі – задайце пытанні перад пачаткам. Але прыміце з разуменнем, калі аўтары адмовяцца расчыніць мастацкую задуму цалкам. Эфект чакання і нечаканасці – важны інструмент для тэатра, аўтар не будзе раскрываць гледачу ўсю інтрыгу, пазбаўляючы яго задавальнення.

Калі вы прачыталі канвенцыю і не знайшлі ў правілах дазволу ў любы момант пакінуць спектакль – абгаварыце гэта перад пачаткам. Вы не закладнік тэатра. Выйсці з мерапрыемства – не значыць сарваць яго, асабліва, калі гэта адзначана ў правілах.

Сарваць мерапрыемства – гэта дзейнічаць супраць правіл, наўмысна парушаючы іх. Варта пашукаць у канвенцыі спосаб, якім вы можаце паказаць арганізатарам, што вы больш не пачуваецеся ў бяспецы, але не жадаеце сарваць спектакль і, магчыма, працягнеце ўдзел, калі гэтая небяспека знікне. Калі яго няма, але вам здаецца, што варта падстрахавацца – абгаварыце гэта з аўтарамі.

Калі аўтары жорстка адмаўляюць папрасіць аб дапамозе, сігналізаваць аб небяспецы ці пакінуць мерапрыемства – гэта цалкам можа казаць пра тое, што мастацкая задума для іх больш каштоўная, чым вы. Калі вам прапануюць гуляць сябе, то ўсе псіхалагічныя трыгеры будуць біць менавіта ў вас.

Калі ёсць роля, то роля нават для непадрыхтаванага чалавека – гэта ўсё ж буфер, абарона. Асабліва калі ў падзеі закладзены рэфлексіўныя такты, якія дапамагаюць падзяліць зробленае выканаўцам і яго персанажам.

Бяспека прамысловага інтэрнэту

У рамках праекту будучыні індустрыі 4.0 адбываецца ўсё больш актыўнае аб'яднанне вытворчасці і IT. Гэта цягне за сабой узмацненне жорсткасці патрабаванняў да забеспячэння бяспекі. Як правіла, хакеры знаходзяць шчыліны ў карпаратыўную сетку праз інтэрфейс паміж офіснай IT сеткай і вытворчай сеткай.

Праведзенае ў 2017 годзе "Лабараторыяй Касперскага" даследаванне паказала, што амаль кожная трэцяя кібератака накіравана на прамысловыя сістэмы кантролю і такім чынам супраць якія вырабляюць кампаній. З кожным годам расце колькасць шкоднасных праграм, а разам з ім і звязаны з імі ўрон для прамысловых сістэм. Нядаўні выпадак кібератакі на аўтаматызаваную сістэму (SIS) шкоднаснай праграмай Triton даказвае, што такі сцэнар абсалютна рэальны.

Ва ўмовах, калі арыентаваныя на функцыянальную бяспеку сістэмы аўтаматызацыі становяцца мэтай хакерскіх нападаў, патрабуецца ўзаемная інтэграцыя сфер функцыянальнай і інфармацыйнай бяспекі. Дзеля гэтага трэба выпрацаваць агульную стратэгію на будучыню.

Прамысловыя сістэмы кіравання ў цяперашні час схільныя мноству пагроз, да якіх, у прыватнасці, адносяцца:

- заражэнне шкоднаснымі праграмамі праз інтэрнэт і ўнутраныя сеткі;
- укараненне шкоднасных праграм праз зменныя носьбіты дадзеных і іншыя вонкавыя апаратныя сродкі;
- сацыяльны інжынірынг, т. е. уздзеянне на людзей з мэтай скланення да вызначаных дзеянняў;
- чалавечыя памылкі і сабатаж;
- пранікненне ў сістэму з дапамогай сродкаў дыстанцыйнага абслугоўвання;
- выкарыстанне кампанентаў кіравання, якія злучаюцца па інтэрнэце з дапамогай IP-пратакола;

− тэхнічныя збоі і форс-мажорныя акалічнасці;

− ўзлом смартфонаў, якія знаходзяцца ў вытворчай асяроддзі, а таксама кампанентаў экстранета і хмарных рашэнняў.

Функцыянальная бяспека – гэта надзейнае функцыянаванне звязаных з бяспекай сістэм (кіравання) і іншыя сродкі зніжэння рызыкі. У выпадку ўзнікнення крытычнай памылкі сістэма кіравання пераводзіць абсталяванне ў бяспечны стан. Патрабаванні да характарыстык звязаных з бяспекай элементаў сістэм кіравання выкладзены ў стандарце групы B EN ISO 13849, а таксама ў серыі МЭК 61508/МЭК 61511/МЭК 62061.

У залежнасці ад ступені рызыкі адпаведныя меры абароны падпадзяляюцца на розныя ўзроўні: узроўні эфектыўнасці (PL) ўзроўні паўнаты бяспекі.

У сваю чаргу, задачай кібернетычнай бяспекі з'яўляецца абарона ад нападаў, накіраваных на абмежаванне гатоўнасці, цэласнасці і канфідэнцыяльнасці дадзеных. Задача рэалізуецца з дапамогай прафілактычных ці актыўных тэхнічных, а таксама арганізацыйных мер. Недаацэнка аспектаў інфармацыйнай бяспекі пры арганізацыі функцыянальнай бяспекі можа мець прамыя наступствы для вытворчага абсталявання. Таксама магчымы ўскосны ўплыў на вытворчы працэс і, тым самым, на канчатковы прадукт.

У якасці прыкладу можа служыць фармацэўтычная прадукцыя ці кампаненты сістэм бяспекі для аўтамабільнай прамысловасці. Тут змены могуць мець значныя негатыўныя наступствы для спажыўцоў. Таму стандарт МЭК 61511-1 патрабуе адзнаку IT-рызыкаў у сістэмах бяспекі перапрацоўчай прамысловасці. Карыстальнік павінен правесці адзнаку IT рызык у па метадзе NA паводле рэкамендацый NAMUR і рэалізаваць вызначаныя такім чынам меры. Карыстальнік можа прааналізаваць сістэму бяспекі АСКВ у адпаведнасці з сучасным узроўнем тэхнікі і выканаць свае абавязацельствы ў частцы добрасумленнасці выканання патрабаванняў.

У частцы як функцыянальнай бяспекі, так і бяспекі доступу спачатку выконваецца аналіз патэнцыйнай рызыкі ў рамках адзнакі рызык, ці больш дакладна адзнакі IT пагроз. Прасочваецца істотнае адрозненне ў падыходзе. У рамках адзнакі рызык канструктары павінны прымаць да ўвагі хутчэй статычныя рыскі паводле дырэктывы па машынным абсталяванні, напрыклад, механічныя ці электрычныя крыніцы падвышанай небяспекі.

У сваю чаргу, эксперт у галіне бяспекі IT дзейнічае ва ўмовах стала якое змяняецца асяроддзя. Зламыснікі з ужываннем усё новых метадаў актыўна шукаюць слабыя месцы ў сістэмах абароны, якія разглядаюцца ў вобласці функцыянальнай бяспекі як сістэматычныя збоі.

Яшчэ адзін важны аспект – чалавечы фактар. У вобласці бяспекі машын існуе такое паняцце, як "разумна прадбачанае злоўжыванне", калі, напрыклад, персанал свядома блакуе працу ахоўных прылад. У выпадку маштабных кібернетычных нападаў на прамысловыя ўстаноўкі гаворка ідзе, хутчэй за ўсё, пра мэтанакіраваны крымінальны намер.

Бяспека аперацыйнай сістэмы лічбавых экасістэм

Праблема абароны ад несанкцыянаваных дзеянняў пры ўзаемадзеянні са знешнімі сеткамі можа быць паспяхова вырашана толькі на аснове комплекснай абароны карпаратыўных інфармацыйных сістэм. Абароненыя аперацыйныя сістэмы ставяцца да базавых сродкаў шматузроўневай комплекснай абароны. Большасць праграмных сродкаў аховы інфармацыі з'яўляюцца прыкладнымі праграмамі. Для іх выканання патрабуецца падтрымка аперацыйнай сістэмы.

Асяроддзе, у якім функцыянуе аперацыйная сістэма, завецца даверанай вылічальнай базай. Яна ўключае ў сябе поўны набор элементаў, якія забяспечваюць інфармацыйную бяспеку: аперацыйную сістэму, праграмы, сеткавае абсталяванне, сродкі фізічнай абароны і нават арганізацыйныя працэдуры. Краевугольным каменем гэтай піраміды з'яўляецца абароненая

аперацыйная сістэма. Без яе даверaная вылічальная база аказваецца пабудаванай на пяску.

Арганізацыя эфектыўнай і склонавай абароны аперацыйнай сістэмы немагчыма без папярэдняга аналізу магчымых пагроз яе бяспецы. Пагрозы бяспекі аперацыйнай сістэмы істотна залежаць ад умоў эксплуатацыі сістэмы, ад таго, якая інфармацыя захоўваецца і апрацоўваецца ў сістэме.

Напрыклад, калі аперацыйная сістэма выкарыстоўваецца для арганізацыі электроннага дакументазвароту, найболей небяспечныя пагрозы, звязаныя з несанкцыянаваным доступам да файлаў. Калі ж аперацыйная сістэма выкарыстоўваецца як платформа правайдэра інтэрнэт-паслуг, вельмі небяспечныя напады на сеткавае праграмнае забеспячэнне.

Пагрозы бяспецы аперацыйнай сістэмы можна класіфікаваць па розных аспектах іх рэалізацыі. Класіфікацыя пагроз па цэлі атакі: несанкцыянаванае чытанне інфармацыі; несанкцыянаванае змяненне інфармацыі; несанкцыянаванае знішчэнне інфармацыі; поўнае ці частковае разбурэнне аперацыйнай сістэмы.

Класіфікацыя пагроз па прынцыпе ўздзеяння на аперацыйную сістэму:

выкарыстанне вядомых (легальных) каналаў атрымання інфармацыі, напрыклад пагроза несанкцыянаванага чытання файла, доступ карыстальнікаў да якога вызначаны некарэктна і згодна з палітыкай бяспекі доступ павінен быць забаронены;

выкарыстанне ўтоеных каналаў атрымання інфармацыі, напрыклад пагроза выкарыстання зламыснікам недакументаваных магчымасцяў аперацыйнай сістэмы;

стварэнне новых каналаў атрымання інфармацыі з дапамогай праграмных закладак.

Класіфікацыя пагроз па тыпе выкарыстоўванай зламыснікам уразлівасці абароны:

неадэкватная палітыка бяспекі, у тым ліку і памылкі адміністратара сістэмы;

памылкі і недакументаваныя магчымасці праграмнага забеспячэння аперацыйнай сістэмы, у тым ліку і так званыя люкі - выпадкова ці наўмысна убудаваныя ў сістэму "службовыя ўваходы", якія дазваляюць абыходзіць сістэму абароны;

раней укаранёная праграмная закладка.

Класіфікацыя пагроз па характары ўздзеяння на аперацыйную сістэму:

актыўнае ўздзеянне – несанкцыянаваныя дзеянні зламысніка ў сістэме;

пасіўнае ўздзеянне – несанкцыянаванае назіранне зламысніка за працэсамі, якія адбываюцца ў сістэме.

Аперацыйную сістэму завуць абароненай, калі яна прадугледжвае сродкі абароны ад асноўных класаў пагроз. Абароненая аперацыйная сістэма абавязкова павінна змяшчаць сродкі размежавання доступу карыстальнікаў да сваіх рэсурсаў, а таксама сродкі праверкі сапраўднасці карыстальніка, які пачынае працу з аперацыйнай сістэмай. Акрамя таго, абароненая аперацыйная сістэма павінна змяшчаць сродкі процідзеяння выпадковаму або наўмыснаму вываду аперацыйнай сістэмы з ладу.

Калі аперацыйная сістэма прадугледжвае абарону не ад усіх асноўных класаў пагроз, а толькі ад некаторых, яе завуць часткова абароненай.

Існуе дна асноўных падыходу да стварэння абароненых аперацыйных сістэм - фрагментарны і комплексны падыходы.

Пры фрагментарным падыходзе спачатку арганізуецца абарона ад адной пагрозы, затым ад іншай і т. д. Прыкладам фрагментарнага падыходу можа служыць сітуацыя, калі за аснову бярэцца неабароненая аперацыйная сістэма (напрыклад, Windows 98), на яе ўсталёўваюць антывірусны пакет, сістэму шыфравання, сістэму рэгістрацыі дзеянняў карыстальнікаў.

Пры комплексным падыходзе ахоўныя функцыі ўносяцца ў аперацыйную сістэму на этапе праектавання архітэктуры аперацыйнай сістэмы і з'яўляюцца яе неад'емнай часткай. Асобныя элементы падсістэмы абароны, створанай на аснове комплекснага падыходу, цесна ўзаемадзейнічаюць сябар з сябрам пры рашэнні розных задач, злучаных з

арганізацыяй абароны інфармацыі, таму канфлікты паміж яе асобнымі кампанентамі практычна немагчымыя.

Падсістэма абароны, створаная на аснове комплекснага падыходу, можа быць уладкована так, што пры фатальных збоях у функцыянаванні яе ключавых элементаў яна выклікае крах аперацыйнай сістэмы, што не дазваляе зламысніку адключаць ахоўныя функцыі сістэмы. Пры фрагментарным падыходзе такая арганізацыя падсістэмы абароны немагчымая.

Падсістэму абароны аперацыйнай сістэмы, створаную на аснове комплекснага падыходу, праектуюць так, каб асобныя яе элементы былі заменныя. Адпаведныя праграмныя модулі могуць быць заменены іншымі модулямі.

Ніводны карыстач не можа пачаць працу з аперацыйнай сістэмай, не ідэнтыфікаваўшы сябе і не падаўшы сістэме аўтэнтыфікуючую інфармацыю, якая пацвярджае, што карыстач сапраўды з'яўляецца тым, кім ён сябе заяўляе. Кожны карыстач сістэмы мае доступ толькі да тых аб'ектаў аперацыйнай сістэмы, да якіх яму прадстаўлены доступ у адпаведнасці з бягучай палітыкай бяспекі.

Аперацыйная сістэма рэгіструе ў спецыяльным часопісе падзеі, патэнцыйна небяспечныя для падтрымання бяспекі сістэмы.

Палітыка бяспекі павінна стала падтрымлівацца ў адэкватным стане, гэта значыць павінна гнутка рэагаваць на змены ўмоў функцыянавання аперацыйнай сістэмы. Упраўленне палітыкай бяспекі ажыццяўляецца адміністратарамі сістэмы з выкарыстаннем адпаведных сродкаў, убудаваных у аперацыйную сістэму.

Абарона інфармацыі неймаверная без выкарыстання крыптаграфічных сродкаў абароны. Шыфраванне выкарыстоўваецца пры захоўванні і перадачы па каналах сувязі пароляў карыстачоў і некаторых іншых дадзеных, крытычных для бяспекі сістэмы. Аперацыйныя сістэмы працуюць не ізалявана, а ў складзе лакальных і глабальных камп'ютарных сетак.

Аперацыйныя сістэмы кампутараў, якія ўваходзяць у адну сетку, узаемадзейнічаюць паміж сабой для рашэння розных задач, у тым ліку мелых прамое стаўленне да абароны інфармацыі.

Кожная з функцый падсістэмы абароны вырашаецца адным ці некалькімі праграмнымі модулямі. Некаторыя функцыі ўбудоўваюцца непасрэдна ў ядро аперацыйнай сістэмы. Паміж рознымі модулямі падсістэмы абароны павінен існаваць выразна вызначаны інтэрфейс, які выкарыстоўваецца пры ўзаемадзеянні модуляў для рашэння агульных задач.

Аперацыйная сістэма. якая задавальняе стандарту абароненасці, павінна ўтрымоўваць падсістэму абароны, якая выконвае ўсе вышэйпералічаныя функцыі. Звычайна падсістэма абароны дапушчае пашырэнне дадатковымі праграмнымі модулямі.

Людзі і кампаніі ўсё больш належаць на лічбавае ўзаемадзеянне, перавага аддаецца выгодзе, а не бяспецы і прыватнасці. Рэспандэнты стварылі ў сярэднім 15 новых анлайн-акаўнтаў падчас пандэміі, што адпавядае мільярдам новых уліковых запісаў, створаных па ўсім свеце.

Каля 44% паведамілі, што яны не плануюць выдаляць або дэактываваць гэтыя новыя ўліковыя запісы, што прывядзе да павелічэння лічбавага следа на бліжэйшыя гады, што значна пашырыць паверхню атакі для кібернетычных злачынцаў.

Аналагічную сітуацыю можна назіраць з Industrial IoT (IIoT): расстаўляючы датчыкі па заводзе, суб'ект вытворчасці стварае крыніцы вялізнага патоку дадзеных, якія трэба захоўваць, апрацоўваць у рэжыме рэальнага часу, маніторыць стан і бяспеку і кіраваць доступам да гэтых дадзеных.

Лічбавыя экасістэмы становяцца ўсё больш функцыянальнымі і дазваляюць зачыняць большую колькасць задач бізнэсу ці задавальняць усё больш карыстацкіх запытаў. Мінус у тым, што ўсе гэтыя падсістэмы трэба бараніць. І пытанне не ў тым, што нам трэба ўкараняць усё больш ИБ-сістэм,

каб абараніць дадзеныя. Трэба, каб укараняемыя сродкі бяспекі былі здольныя яшчэ і апрацаваць гэты аб'ём дадзеных у рэжыме рэальнага часу».

Такія патрабаванні прад'яўляюцца ўжо не IT-дэпартаментамі кампаній, а кіраўніком, які сёння не жадае чакаць на працягу двух гадзін, пакуль дадзеныя ў волкім выглядзе выгрузяцца ў Excel, а патрабуе, каб яны адлюстроўваліся ў рэальным часе на дашбордзе ў мабільным тэлефоне.

Адно гэтае патрабаванне выклікае адразу некалькі пытанняў: як апрацоўваць такі аб'ём дадзеных у рэжыме «тут і цяпер»? Як забяспечыць бяспеку гэтай базы дадзеных, як кантраляваць інтэграцыйныя пласты, доступ карыстальнікаў, у тым ліку, прывілеяваных карыстальнікаў? Як звязаць мабільнае прыкладанне кіраўніка з гэтай базай дадзеных так, каб не праніклі зламыснікі? У выніку ўзнікае вялікая колькасць пытанняў да службаў інфармацыйнай бяспекі.

Экасістэмы растуць не толькі ў звычайных карыстальнікаў або бізнес-заказчыкаў, яны сапраўды гэтак жа растуць у зламыснікаў. Існуюць форумы ў даркнеце, хмарныя сэрвісы для хакераў – размеркаваная сеткавая інфраструктура падбірае паролі ці ўзломвае хэшкоды па аналогіі з тым, як майне крыптавалюта. Калі казаць аб размеркаванай майнінгавай ферме, то яна ўзламае пятнаццацізначны пароль на працягу сутак, і гэтыя факты немагчыма ігнараваць.

Хутка ў кампаній будуць фармавацца прадстаўніцтвы ў мета-сусветаў гэтак жа, як сёння ў кожнай кампутара свой сайт. У гэтых прадстаўніцтвах будуць збіраць карыстацкія дадзеныя і канфідэнцыйная інфармацыя, якую таксама трэба будзе абараняць.

Аб'ём росту экасістэм, якія абараняюцца, паскараецца, і сродкі для іх абароны патрабуюцца магутныя, рознанакіраваныя, якія прывабліваюць разнастайную экспертызу. Каманда павінна не проста ўмець устанавіць антывірус, але разумець, у якіх рэаліях жыве бізнес, у якіх напрамках яго, у першую чаргу, варта абараняць.

Да прыкладу, у анлайн-краме можа здарыцца простай сістэмы аплаты, які інтэграваны праз аўтарызацыю ў сацыяльнай сетцы.

У кожнай падсістэме хакеры могуць запусціць вірус (праз хмарную платформу, у тым ліку). Дробны бізнэс, не кажучы ўжо пра звычайнага чалавека, проста не можа ўсачыць за ўсімі рызыкамі, альбо ў яго няма бюджэту на тое, каб абараніцца. Узровень недаступнасці паўнавартаснага сэрвісу кібернетычнай надзейнасці для большасці гульцоў рынка становіцца занадта высокім.

У гэтых умовах бізнэс усё часцей звяртаецца да кампаній, якія аказваюць аўтсорсінгавыя паслугі. Рызыкі ў галіне інфармацыйнай бяспекі павінны закладвацца ў кожны інвестыцыйны праект

Тэхналагічная сінгулярнасць – гэта тэарэтычны момант, у якім чалавек страціць кантроль над тэхнічным прагрэсам, а той, у сваю чаргу, стане незваротным. Кажучы простай мовай, у найбліжэйшай будучыні тэхналогіі могуць настолькі развіцца, што чалавецтва проста перастане паспяваць за імі і разумець іх.

Адзін з прыкладаў тэхналагічнай сінгулярнасці – гэта NFT, папулярная сістэма перадачы правоў карыстання на лічбавыя аб'екты. Чым далей, тым больш падобных тэхналогій будзе ўзнікаць: людзі або іх не разумеюць, або яны ім не цікавыя.

Узнікае ўмова нераўнамернага размеркавання будучыні: хтосьці ўжо жыве ў будучыні, дзе ідзе дужанне за абарону высокаэфектыўных лічбавых актываў, а хтосьці карыстаецца базавымі падручнымі сродкамі і своечасова не раскідвае патч-корды для роўтара. Найпросты сканар можа прасканаваць сетку "наіўнага" карыстача на працягу хвіліны і выявіць дзюры ў сістэме абароны. Пятнаццаць секунд і вірус з вамі назаўжды.

Менавіта таму інфармацыйная бяспека павінна ўлічвацца ў бізнес-плане IT-праекта на этапе яго першаснай абароны перад інвестарам, да разліку PNL (Profit and Loss Statement – справаздача аб прыбытках і стратах).

Чым пазней выяўляецца недахоп ИБ-сэрвісаў, тым даражэй каштуе іх укараненне і абарона існага сэрвісу.

Яшчэ адна праблема – гэта нізкая якасць камунікацыі паміж бізнесам і ИБ. Часта спецыялісты фізічнай бяспекі бліжэй да бізнэсу, чым спецыялісты бяспекі інфармацыйнай. Як правільна павінен паводзіць сябе ўладальнік з пункту гледжання забеспячэння ИБ?

вылучаць дастатковую колькасць сродкаў на пабудову і падтрыманне сістэмы ІБ;

надзяляць высокаўзроўневымі паўнамоцтвамі спецыялістаў ІБ-каманды, садзейнічаць іх дыялогу з асобамі, якія прымаюць рашэнні;

ўсведамляць прыярытэт інфармацыйнай бяспекі ва ўсіх унутраных праектах кампаніі.

З ростам колькасці дадзеных узнікаюць цікавыя сцэнары ў працы розных сістэм, напрыклад, у рабоце сістэмы абароны кампаніі ад уцечкі даных (DLP). Гэтая сістэма здольная не толькі кантраляваць доступ да дадзеных, але і ствараць ценявыя копіі дакументаў, якія праходзяць праз сістэму, аналізуючы іх: хто звяртаўся да таго ці іншага дакумента, капіраваў, мяняў і гэтак далей.

У выніку ў сістэмы DLP узнікае сістэма захоўвання, у якой ляжаць копіі самых "цікавых" дакументаў кампаніі. Сотні тысяч контрагентаў ствараюць сотні тысяч дакументаў у дзень, такім чынам гэтая сістэма захоўвання сама па сабе становіцца аб'ектам Big Data, які, у сваю чаргу, гэтак жа мае патрэбу ў абароне.

Гарантуючы бяспеку Big Data, трэба выкарыстоўваць адпаведныя сродкі, якія здольныя працаваць з такім аб'ёмам інфармацыі.

Правіла дакранаецца і машыннага навучання: адзін з вектараў кібернетычнага нападу – падробка сістэмы візуальнага распазнання. Гэта наглядна ілюструе кейс аб тым, як у 2019 годзе каманда Tencent паказала, што можа падманам прымусіць аўтапілот Tesla перасекчы раздзяляльную паласу, дадаўшы невялікія бяскрыўдныя палоскі стужкі на паверхню дарогі.

Нельга ўкараніць сістэму, якая на аснове машыннага навучання распазнае патэрн паводзін чалавека і, такім чынам, прымае рашэнне аб тым, хто знаходзіцца за кансоллю.

У аснове тэхналогіі – сістэма біяметрычнай ідэнтыфікацыі, у тым ліку, распазнанне па рухах мышкі, па камеры, адбітак пальцаў і гэтак далей. Зламыснікі ж у адказ створаць сістэму, якая засноўваецца на той жа тэхналогіі machine learning і вучыцца падрабляць паводніцкую мадэль іншага карыстача, каб сістэма распазнавала зламысніка, як свайго.

Пясочніцы прадстауляюць сістэмы віртуальных машын. Для віруса ці для зламысніка яны выглядаюць як частка карпаратыўнай сістэмы, напрыклад, бухгалтэрыя з сотняй сапраўдных працоўных месцаў. Зламыснік, трапляючы ў гэтую пастку, бачыць шмат IP-адрасоў, падсетак, машын, у іх адкрыты парты, працуюць прыкладанні, і буксуе, вывучаючы гэтую "інфраструктуру". Спецыялісту па інфармацыйнай бяспецы гэта дае часовую перавагу, каб выявіць дзеянні зламысніка.

Стварэнне пясочніц становіцца ўсё больш складанай, паколькі прыходзіцца сімуляваць усё больш і больш падсістэм, каб выглядаць праўдападобна для хакера. Даводзіцца ствараць выдуманы метасвет для хакераў, у якой яны павінны заблудзіцца. Гэта патрабуе вялізных магутнасцяў. Сярэднестатыстычная кампанія не можа дазволіць сабе такія выдаткі, і выйсцем становяцца хмарныя правайдэры бяспекі.

Важная задача інфармацыйнай бяспекі заключаецца ў пабудове сістэмы прыярытэтаў для бізнесу па абароне ключавых сегментаў кампаніі. Любы бізнэс можна падзяліць на блокі, прыярытэт працы якіх вышэйшы, чым у іншых. Кошт прастою пралічыць даволі лёгка: колькі за год зарабляе кампанія? Напрыклад, мільярд рублёў, з іх пяцьсот мільёнаў зарабляецца на базе аднаго блока, дзвесце пяцьдзесят на базе іншага і гэтак далей.

Што будзе, калі спыніць на суткі той ці іншы блок? Трэба падзяліць на 365 суму даходу, які прыносіцца блокам. Так разлічваюцца і патэнцыйныя

страты пры надыходзе інцыдэнту інфармацыйнай бяспекі, якія затым ранжыруюцца па ступені крытычнасці і верагоднасці рэалізацыі.

Можна пабудаваць карту рызык у грашовым выражэнні для любой кампаніі. Такая прылада дазваляе кіраўніку хутка прыняць рашэнне аб тым, якія рыскі ён дапушчае, а якія ні ў якім разе, і, зыходзячы з гэтага, набыць патрабаванае рашэнне, якое нівелюе ўзнікненне дарагіх інцыдэнтаў.

Унутраны аўдыт дапамагае аптымізаваць выдаткі і павысіць эфектыўнасць. У выніку інфармацыйная бяспека ўскосна дапамагае бізнэсу, нават на этапе адзнакі.

Можна пабудаваць таксама карту тэхнічнай адпаведнасці заканадаўству ў разрэзе краіны, галіны і лакальных нарматыўных актаў. Любы заканадаўчы акт можна выказаць у канчатковым спісе патрабаванняў.

Бяспека праграмных сродкаў

Асноўная ўвага ў тэорыі і практыцы забеспячэння бяспекі інфармацыйных сістэм засяроджана на абароне ад зламысных разбурэнняў, скажэнняў, крадзяжоў і выкарыстанні праграмных сродкаў і інфармацыі баз дадзеных. Для гэтага распрацаваны і актыўна развіваюцца праблемна-арыентаваныя метады і сродкі аховы ад несанкцыянаванага доступу, ад розных тыпаў вірусаў і закладак, ад уцечкі інфармацыі па каналах электрамагнітнага выпраменьвання.

Пры гэтым маецца на ўвазе наяўнасць асоб, зацікаўленых у несанкцыянаваным доступе да інфармацыі ў сістэмах, з мэтай яе незаконнага выкарыстання. Для вырашэння праблемы створаны і актыўна развіваюцца метады, сродкі і стандарты абароны праграм і даных.

Разглядаюцца небяспечныя сітуацыі, якія прыводзяць да страты працаздольнасці сістэм, да аварый і катастроф. Пры такіх сітуацыях знешняя функцыянальная працаздольнасць сістэм можа разбурацца не поўнасцю. Аднак немагчыма паўнавартаснае выкананне функцый і патрабаванняў да

якасці інфармацыі. У разгляданых сістэмах бяспека іх функцыянавання вызначаецца праявамі дэстабілізуючых фактараў, якія прыносяць шкоду:

тэхнічнымі адмовамі апаратуры і скажэннямі інфармацыі ад аб'ектаў асяроддзя і сістэм;

збоямі і фізічнымі разбурэннямі элементаў і кампанентаў апаратных сродкаў вылічальных комплексаў і сродкаў тэлекамунікацыі;

дэфектамі і памылкамі ў комплексах праграм апрацоўкі інфармацыі і ў дадзеных;

прабеламі і недахопамі ў сродках выяўлення небяспечных адмоў і аператыўнага аднаўлення працаздольнага стану сістэм, праграм і даных.

Магчымы катастрафічныя наступствы і адмовы функцыянавання з вялікай шкодай пры адсутнасці варожых асоб, зацікаўленых у падобных парушэннях працаздольнасці сістэм і праграмных сродкаў. Яны маюць сваю прыроду, асаблівасці і характарыстыкі.

Таму яны патрабуюць самастойнага вывучэння і адэкватных метадаў і сродкаў забеспячэння бяспекі. У некаторых сістэмах адмовы, якія адбіваюцца на бяспецы, могуць быць наўмысным разбурэннем або скажэннем інфармацыі ў базах дадзеных.

Дбайнае спецыфікаванне і ацэньванне бяспекі сістэм, праграмнага прадукта і інфармацыі адлюстроувае фактар забеспячэння іх эфектыўнага і адэкватнага прымянення. Гэта можа быць дасягнута на аснове вылучэння, вызначэння і забеспячэнні падыходных характарыстык з улікам выкарыстання і функцыянальных задач праграмных сродкаў і сістэм.

Выдзяляюць два класы сістэм і іх праграмных сродкаў. Першы клас складаюць сістэмы, якія маюць убудаваныя комплексы праграм жорсткага рэгламенту рэальнага часу. Час рэакцыі на няштатныя сітуацыі такіх сістэм звычайна вылічаецца секундамі ці дзелямі секунды, і працэсы ўзнаўлення працаздольнасці павінны праводзіцца аўтаматызавана (бартавыя сістэмы ў авіяцыі, у некаторых сродках узбраення і транспарта).

Сістэмы другога класа прымяняюцца для кіравання працэсамі і апрацоўкі інфармацыі з асяроддзя, у якіх актыўна ўдзельнічаюць спецыялісты-аператары (адміністрацыйныя, банкаўскія, штабныя ваенныя сістэмы). Дапушчальны час рэакцыі на небяспечныя адмовы ў гэтых сістэмах можа складаць хвіліны, і аперацыі па аднаўленні працаздольнасці могуць быць даверaны спецыялістам-адміністратарам па забеспячэнні бяспекі.

Статыстычна адмоў можа быць у некалькі разоў менш, чым улічаных у значэннях надзейнасці. Аднак метады, якія ўплываюць фактары і рэальныя значэнні надзейнасці праграмных сродкаў могуць служыць арыенцірамі пры адзнацы бяспекі крытычных сістэм.

Шкода ад дэфектаў і памылак праграм і дадзеных можа выяўляцца ў сістэматычных адмовах. Назапашванне такіх адмоў з часам можа прыводзіць да наступстваў, якія парушаюць функцыянальную бяспеку сістэм і іх ужыванне. Такім чынам, збліжаюцца паняцці надзейнасці і бяспекі складаных сістэм і праграмных сродкаў.

Пры больш-менш аднолькавых крыніцах пагроз і іх праявах гэтыя паняцці можна падзяліць па велічыні наступстваў і ўрону пры ўзнікненні няштатных сітуацый.

Патрабаванні ітэрацыйна фармуюцца, дэталізуюцца і ўдакладняюцца па ўзгадненні паміж усімі ўдзельнікамі праекту з прычыны абмежаванасці першасных зыходных дадзеных і змены іх пад уплывам розных працэсаў на паслядоўных этапах жыццёвага цыклу.

Змена і адрозненні персанала, які ўжывае сістэму і праграмныя сродкі, дадаткова павялічвае нявызначанасць значэнняў бяспекі і цяжкасці яе прагназавання з улікам мноства суб'ектыўных фактараў розных адмыслоўцаў, якія ўдзельнічаюць у эксплуатацыі.

У працэсе праектавання, распрацоўкі і жыццёвага цыкла асноўных функцыянальных задач асяроддзя гэтыя кампаненты з цягам часу развіваюцца і адаптуюцца, што адбіваецца на неабходнасці адэкватнай змены метадаў, задач і сродкаў забеспячэння іх бяспекі.

Аб'ектыўнае павышэнне складанасці функцый, якія рэалізуюцца праграмамі ў сучасных сістэмах, непасрэдна прыводзіць да павелічэння іх аб'ёму і працаёмкасці стварэння.

Адпаведна росту складанасці праграм узрастае адносная і абсалютная колькасць дэфектаў і памылак, што выяўляюцца і застаюцца ў іх, што адбіваецца на зніжэнні бяспекі іх функцыянавання. Па меры павелічэння складанасці задач, развязальных праграмамі, узрастае ўплыў памылак, якія могуць пагражаць аварыямі і катастрофамі ў сістэмах, якія выконваюць крытычныя функцыі кіравання буйнымі, дарагімі і асабліва важнымі аб'ектамі ці працэсамі.

Упарадкаванае, рэгламентаванае праектаванне архітэктуры, распрацоўка і суправаджэнне складаных праграмных сродкаў на базе сучасных тэхналогій дае магчымасць папярэджваць і ўстараняць найбольш небяспечныя сістэмныя, алгарытмічныя і праграмныя дэфекты і памылкі на ранніх стадыях жыццёвага цыкла, а таксама выкарыстоўваць неаднаразова праверaныя ў іншых праектах бяспечныя праграмныя і інфармацыйныя праекты. Для забеспячэння бяспекі крытычных сістэм неабходны эфектыўныя метады і сродкі, якія папярэджваюць і выяўляюць дэфекты, а таксама якія сведчаць бяспеку выкарыстання праграм і баз даных, аператыўна абараняюць іх карэктнае функцыянаванне пры праяве любых дэфектаў і няштатных сітуацый.

Працаздольнасць праграмных сродкаў можа быць забяспечана пры зыходных дадзеных, якія выкарыстоўваліся пры іх распрацоўцы, адладцы і выпрабаваннях. Рэальныя зыходныя дадзеныя могуць мець значэнні, якія адрозніваюцца ад прадугледжаных тэхнічным заданнем і ад выкарыстоўваных пры эксплуатацыі праграм і баз дадзеных.

Пры такіх зыходных дадзеных функцыянаванне ПС цяжка прадказаць загадзя, і вельмі верагодныя розныя анамаліі, якія завяршаюцца адмовамі, якія адбіваюцца на бяспецы. Варта ўлічваць прынцыповыя цяжкасці аналітычнага ацэньвання і прагназавання значэнняў бяспекі праграмных

сродкаў з прычыны непрадказальнасці становішча, праявы і наступстваў дэфектаў і памылак у праграмах і дадзеных. Гэта прыводзіць да немагчымасці дакладных апрыёрных аналітычных разлікаў бяспекі комплексаў праграм пры яе высокіх значэннях.

Праблема дасягнення бяспекі сістэм, якія змяшчаюць праграмныя сродкі рэальнага часу, вырашаецца шляхам выкарыстання сучасных рэгламентаваных тэхналагічных працэсаў і інструментальных сродкаў забеспячэння іх жыццёвага цыкла.

Структура, паслядоўнасць і змест тэхналагічных працэсаў жыццёвых цыклаў у стандартах некалькі адрозніваюцца, аднак наменклатура базавых кампанентаў практычна супадае, што дазваляе іх выбіраць і прымяняць з улікам забеспячэння бяспекі канкрэтных праектаў праграмных сродкаў.

Для барацьбы з пагрозамі бяспекі праграмных сродкаў неабходны даследаванні фактараў, якія ўплываюць на функцыянальную бяспеку са боку дэфектаў і памылак, існых і патэнцыйна магчымых у пэўных сістэмах і комплексах праграм. Складанасць праграм і баз дадзеных, а таксама даступныя рэсурсы для іх рэалізацыі становяцца ўскоснымі крытэрыямі або фактарамі, якія ўплываюць на выбар метадаў распрацоўкі, на якасць і бяспеку праграмных сродкаў.

Усе этапы распрацоўкі і суправаджэння праграмных сродкаў, варта падтрымліваць метадамі і сродкамі верыфікацыі і сістэматычнага, аўтаматызаванага тэсціравання кампанентаў праграм. Тэставанне з'яўляецца асноўным метадам ухілення дэфектаў, вымярэнні і азначэнні рэальных характарыстак праграм на любых этапах іх жыццёвага цыклу. Наяўнасць дастаткова поўных эталонаў на аснове сукупнасці патрабаванняў спецыфікацый і паэтапная іх дэкампазіцыя - неабходная база тэсціравання і вымярэння бяспекі і якасці комплексаў праграм.

Распрацоўку сістэм і праграмных сродкаў павінны завяршаць комплексныя выпрабаванні і пасведчанне бяспекі і надзейнасці сістэм з

праграмнымі сродкамі, якія прадугледжваюць магчымасць удасканалення іх характарыстык шляхам адпаведных карэкціровак праграм.

Павышэнне бяспекі мэтазгодна шляхам рэалізацыі працэдур аналізу выяўленых дэфектаў і аператыўнага аднаўлення вылічальнага працэсу, праграм і даных (рэсарта) пасля выяўлення анамалій і адмоваў функцыянавання ПС. Гэтаму можа спрыяць назапашванне, маніторынг і захоўванне дадзеных аб выяўленых дэфектах, збоях і адмовах у працэсе выканання праграм і апрацоўкі дадзеных.

Асноўныя паняцці і фактары, якія вызначаюць бяспеку праграмных сродкаў

Праграмныя сродкі павінны мець эканамічную, тэхнічную, навуковую або сацыяльную эфектыўнасць прымянення, якая ў праектах павінна адлюстроўваць асноўную мэту іх жыццёвага цыкла ў сістэме. Гэта сістэмная эфектыўнасць можа быць апісана колькасна ці якасна, у выглядзе набору карысных характарыстык праграмных сродкаў, іх адрозненняў ад наяўных у іншых комплексаў праграм, а таксама фактараў і крыніц эфектыўнасці.

У выніку павінна быць фармалізаваная мэта выкарыстання і набор патрабаванняў замоўца і карыстача пры стварэнні ці набыцці праграмных сродкаў, а таксама яго меркаванае прызначэнне і сфера ўжывання.

У стандартах эфектыўнасць адлюстроўвае функцыянальная прыдатнасць праграмных сродкаў. У працэсе сістэмнага аналізу пры падрыхтоўцы тэхнічнага задання спецыфікацый, значэння розных фактараў, характарыстык якасці і бяспекі павінны выбірацца з улікам іх уплыву на функцыянальную прыдатнасць.

Паляпшэнне характарыстыкі якасці, у тым ліку бяспекі, патрабуе некаторых затрат рэсурсаў (працаёмкасці, фінансаў, часу), якія павінны адбівацца на характарыстыцы якасці – на прыдатнасці.

Мэты, прызначэнне і функцыі абароны комплексу праграм ад адмоваў цесна злучаны з асаблівасцямі прыдатнасці кожнага тыпу праграмных сродкаў. У працэсе сістэмнага аналізу і праектавання павінны быць выяўлены патэнцыйныя наўмысныя і пагрозы функцыянаванню ПС і ўстаноўлены ўзровень бяспекі гэтага комплексу праграм.

У адпаведнасць з гэтым узроўнем, заказчыкам і распрацоўшчыкамі павінны выбірацца і ўстанаўліваца патрабаваныя і неабходныя наборы метадаў і сродкаў забеспячэння бяспекі ПС з улікам абмежаваных рэсурсаў на іх рэалізацыю.

У выніку сфармаваныя патрабаванні павінны павінны забяспечваць роўнатрывалую абарону ад розных рэальных пагроз і рэалізацыю неабходных мер кантролю і пацверджанні патрабаваных характарыстык прыдатнасці комплексу праграм ва ўмовах пагроз бяспецы функцыянавання праграмных сродкаў. Для забеспячэння эфектыўнасці сістэмы, комплекс праграм бяспекі мэтазгодна грунтаваць на наступных агульных прынцыпах:

- абарона апаратуры сістэмы, функцыянальных праграм і даных павінна быць арыентавана на ўсе віды пагроз з улікам іх небяспекі для спажыўца;
- кошт (працаёмкасць) стварэння і эксплуатацыі сістэмы абароны павінна быць менш, чым памеры найбольш верагоднага або магчымага (у сярэднім) непрымальнага спажыўцамі сістэмы шкоды - рызыкі ад любых патэнцыйных пагроз;
- комплекс праграм абароны павінен мець мэтавыя, індывідуальныя кампаненты контрмер, прызначаныя для забеспячэння бяспекі функцыянавання кожнага асобна ўзятага кампанента і задачы сістэмы з улікам іх уразлівасці і ступені ўплыву на бяспеку сістэмы ў цэлым;
- сістэма праграм абароны не павінна прыводзіць да адчувальных цяжкасцяў, перашкод і зніжэнню эфектыўнасці ўжывання і рашэнні асноўных, функцыянальных задач карыстачамі сістэмы ў цэлым.

Характарыстыкі асяроддзя, прыкладныя сферы прымянення комплексаў праграм, мэты і задачы, узровень аўтаматызацыі іх функцый і

многія іншыя фактары вызначаюць метады забеспячэння бяспекі вылічальных сістэм. Адрозненне паміж відамі бяспекі не заўсёды дастаткова дакладнае і яго трэба разглядаць і ўлічваць у залежнасці ад канкрэтных функцый сістэм, задач і вынікаў забеспячэння бяспекі, а таксама ад катэгорый і характарыстык сітуацый.

Шкода пры сітуацыях адмовы вызначаецца ўразлівасцю і парушэннем карэктнага выканання прызначэння і патрабаваных функцый пры абмежаваных рэсурсах на іх рэалізацыю. Контрмеры пры гэтым абмяжоўваюцца дадатковымі сродкамі абароны ад адмоваў, змяненнем суадносін патрабаванняў да розных характарыстык і перазмеркаваннем даступных рэсурсаў для іх рэалізацыі.

Функцыі сістэм і іх праграмных сродкаў рэалізуюцца ў асяроддзі, характарыстыкі якіх істотна ўплываюць на функцыянальную прыдатнасць праграм. Для выканання патрабаваных функцый комплексу праграм неабходна адэкватная зыходная інфармацыя ад аб'ектаў асяроддзя, змест якіх павінен поўнасцю забяспечваць рэалізацыю функцый, дэкларацыяных у патрабаваннях да сістэмы.

Бо без дэфектаў і памылак прынцыпова немагчыма стварыць і ўжываць складаныя комплексы праграм, увага павінна быць засяроджана на характарыстыках дэфектаў функцыянальных праграм, вызначальных асноўнае прызначэнне сістэмы.

Асяроддзе забеспячэння бяспекі ПС уключае палітыкі і праграмы арганізацыі бяспекі прадпрыемстваў і сістэм, вопыт, спецыяльныя навыкі і веды, якія вызначаюць прымяненне сістэмы. Серада ўключае таксама магчымыя пагрозы бяспецы, прысутнасць якіх у асяроддзі ўстаноўлена або мяркуецца. Пры фармалізацыі асяроддзя бяспекі варта прымаць да ўвагі:

- прызначэнне сістэмы, уключаючы функцыі прадукта і меркаваную сферу яго прымянення;
- праграмы і дадзеныя функцыянальных задач сістэмы, а таксама кампаненты, якія падпарадкаваны патрабаванням бяспекі сістэмы;

•фізічнае асяроддзе ў той яго частцы, якая вызначае ўсе аспекты сістэмы, якія датычацца бяспекі, у тым ліку мерапрыемствы, якія адносяцца да сродкаў абароны і да персаналу.

На падставе распрацаваных палітык бяспекі, адзнак пагроз і рызык фармуюцца зыходныя дадзеныя, якія адносяцца да бяспекі асяроддзя сістэмы і асноўнага комплексу праграм:

•здагадкі, якім павінна задавальняць асяроддзе для таго, каб сістэма ці ПС лічыліся бяспечнымі;

•пагрозы бяспецы для актываў, у якіх былі б ідэнтыфікаваны ўсе пагрозы асяроддзя, прагназуемыя на аснове аналізу бяспекі як якія адносяцца да аб'екта бяспекі;

•пагрозы, якія раскрываюцца праз паняцці крыніцы пагроз, меркаванага метаду іх рэалізацыі, перадумовы для адмоваў і ідэнтыфікацыя кампанентаў, якія з'яўляюцца аб'ектамі адмоваў.

Выкарыстоўваецца наступная класіфікацыя сітуацый адмовы:

•сітуацыя, якая перашкаджае працаздольнасці і функцыянаванню сістэмы ў адпаведнасці з патрабаваннямі;

•сітуацыя, якая прыводзіць да значнага зніжэння працаздольнасці, прымянення і функцыянавання сістэмы або да адсутнасці здольнасці персаналу справіцца з неспрыяльнымі эксплуатацыйнымі рэжымамі, пры якіх узнікаюць: цяжкія сітуацыі або перагрузкі сістэмы, якія могуць выклікаць недакладнае ці няпоўнае выкананне задач з вялікай шкодай;

•сітуацыя, якая прыводзіць да зніжэння прыдатнасці сістэмы або да скарачэння здольнасці персаналу зладзіцца з неспрыяльнымі эксплуатацыйнымі рэжымамі, пры працягу якіх можа ўзнікаць, напрыклад, вялікае скажэнне інфармацыйных рэсурсаў ці скарачэнне функцыянальных, перагрузкі ці ўмовы, якія выклікаюць істотнае пагаршэнне працаздольнасці сістэмы ці персанала;

•сітуацыя, якая нязначна памяншае бяспеку функцыянавання і прымянення аб'екта, але адбіваецца на яго надзейнасці;

•сітуацыя, якая практычна не ўплывае на працаздольнасць, эксплуатацыйныя характарыстыкі і магчымасці аб'екта ці не павялічвае працоўную нагрузку персанала.

Працазатраты, рэсурсы і час, неабходныя для забеспячэння ўзгодненасці з патрабаваннямі заказчыка да якасці функцыянавання, мяняюцца ў залежнасці ад катэгорый сітуацый адмовы.

Ступень бяспекі сістэм характарызуецца прадухіленай і рэшткавым уронам рызыкі, магчымай пры праяве дэстабілізуючых фактараў і рэалізацыі канкрэтных пагроз бяспекі прымянення сістэмы.

Гэта збліжае паняцці і характарыстыкі ступені бяспекі з паказчыкамі надзейнасці сістэмы. Адрозненне ў тым, што ў паказчыках надзейнасці ўлічваюцца ўсе рэалізацыі адмоў, а ў характарыстыках бяспекі трэба рэгістраваць толькі тыя катастрафічныя, крытычныя або небяспечныя адмовы, якія адбіліся на парушэнні бяспекі з вялікай шкодай.

У некаторых выпадках наступствы адмоваў можа быць карысным адлюстроўваць працягласцю працаздольнага стану сістэмы паміж падзеямі адмоваў адносна працягласці прымянення сістэмы з улікам затрат часу на выяўленне і ліквідацыю адмоў (каэфіцыент гатоўнасці сістэмы). Дэстабілізуючымі фактарамі бяспекі сістэм з'яўляюцца:

•збоі і адмовы ў апаратуры вылічальных сродкаў;

•вірусы, збоі і адмовы, якія распаўсюджваюцца па каналах тэлекамунікацыі, якія ўплываюць на інфармацыйную і функцыянальную бяспеку;

•змены складу і канфігурацыі комплексу апаратуры сістэмы ці ПС за межы, праверaныя пры выпрабаваннях ці сертыфікацыі;

•сістэмныя памылкі пры пастаноўцы задач праектавання прыдатнасці сістэмы пры фармулёўцы патрабаванняў да функцый і характарыстыках сродкаў забеспячэння бяспекі;

•дэфекты і памылкі пры вызначэнні функцый, умоў і параметраў асяроддзя;

•алгарытмічныя памылкі праектавання функцый забеспячэння бяспекі апаратуры, праграмных сродкаў і баз даных пры вызначэнні структуры і кампанентаў функцыянальных комплексаў праграм, а таксама пры выкарыстанні інфармацыі баз даных;

•памылкі і дэфекты праграмавання ў тэкстах праграм і апісаннях даных, а таксама ў дакументацыі на кампаненты праграмных сродкаў;

•недастатковая эфектыўнасць выкарыстоўваных метадаў і сродкаў абароны праграм і дадзеных, забеспячэнні бяспекі функцыянавання.

Поўнае ўхіленне пералічаных вышэй пагроз бяспекі функцыянавання крытычных сістэм прынцыпова немагчыма. Пры стварэнні складаных комплексаў праграм праблема складаецца ў выяўленні фактараў, ад якіх яны залежаць, у стварэнні метадаў і сродкаў памяншэння іх уплыву на бяспеку.

Для забеспячэння бяспекі сістэм ствараюцца адпаведныя контрмеры – спецыялізаваныя сістэмы і сродкі, якія ўключаюць сукупнасць узаемазвязаных нарматыўных дакументаў, арганізацыйна-тэхнічных мерапрыемстваў і адпаведных ім метадаў і праграмных сродкаў.

Даступная велічыня і размеркаванне рэсурсаў на асобныя віды контрмер аказваюць значны ўплыў на дасяганую комплексную бяспеку сістэмы. Пры забеспячэнні бяспекі рэсурсы выкарыстоўваюцца ў мэтах:

•кантролю і карэкціроўкі дэфектаў інфармацыі;

•аператыўнага кантролю і выяўлення дэфектаў выканання праграм і апрацоўкі даных;

•размяшчэння і забеспячэння функцыянавання прымяняемых сродкаў абароны ад усіх відаў пагроз бяспекі сістэмы;

•генерацыі тэставых набораў ці захоўванні тэстаў для кантролю працаздольнасці, захаванасці і цэласнасці праграмных сродкаў пры функцыянаванні сістэмы;

•назапашвання, захоўвання і маніторынгу даных аб выяўленых інцыдэнтах, спробах несанкцыянаванага доступу да інфармацыі, аб дэфектах,

збоях і адмовах у працэсе выканання праграм і апрацоўкі даных, якія ўплываюць на бяспеку;

- рэалізацыі працэдур аналізу і маніторынгу выяўленых дэфектаў і аператыўнага аднаўлення вылічальнага працэсу, праграм і даных (рэсарта) пасля выяўлення дэфектаў і адмоў функцыянавання сістэмы.

Замоўцу, першым чынам, цікавяць функцыі, бяспека і якасць гатовага канчатковага прадукта – сістэмы і праграмнага сродку, і звычайна не вельмі турбуе, як яны дасягнуты. Патрабаваную функцыянальную бяспеку можна забяспечыць пасродкам ужывання рэгламентаваных тэхналогій і сістэм забеспячэння бяспекі і якасці ў працэсах праектавання, распрацоўкі і вырабы, якія прадухіляюць дэфекты і што гарантуюць высокую бяспеку і якасць прадукцыі падчас яе стварэння і/ці мадыфікацыі.

Палітыка забеспячэння і пасведчання бяспекі і якасці складаных праграмных сродкаў павінна грунтавацца на праверках і выпрабаваннях тэхналогій забеспячэння жыццёвага цыкла праграмных сродкаў, падтрыманых рэгламентаванымі сістэмамі якасці; функцыянавання гатовага праграмнага прадукта з поўным камплектам дакументацыі.

Функцыянальная прыдатнасць – найбольш адказная, нявызначаная, аб'ектыўна цяжка фармалізуецца і ацэньваецца ў праектах характарыстыка комплексаў праграм, якая значна вызначае патрабаванні да забеспячэння бяспекі сістэмы. Галіны прымянення, наменклатура і функцыі комплексаў праграм ахопліваюць такія разнастайныя сферы дзейнасці чалавека, што немагчыма цалкам вылучыць і ўніфікаваць дастаткова абмежаваную колькасць атрыбутаў для выбару і параўнання характарыстык у розных па прызначэнні комплексаў праграм.

Функцыянальная прыдатнасць – гэта набор і апісанні атрыбутаў, якія вызначаюць прызначэнне, асноўныя, неабходныя і дастатковыя функцыі праграмных сродкаў, зададзеныя тэхнічным заданнем і спецыфікацыямі патрабаванняў заказчыка або патэнцыйнага карыстальніка.

У працэсе праектавання комплексу праграм атрыбуты прыдатнасці павінны канкрэтызавацца ў спецыфікацыях. Атрыбутамі характарыстыкі якасці могуць быць функцыянальная поўнасць рашэння зададзенага комплексу задач.

Функцыянальная прыдатнасць вызначаецца якасцю ўзаемасувязі і ўзгодненасці паслядоўных фармулёвак зместу і рэалізацыі асноўных фрагментаў у ланцужку стандартызаваных патрабаванняў тэхнічнага задання. Функцыі праграмнага сродку рэалізуюцца ў асяроддзі сістэмы. Яе характарыстыкі істотна ўплываюць на функцыянальную прыдатнасць. Для выканання патрабаваных функцый комплексу праграм неабходна адэкватная зыходная інфармацыя ад аб'ектаў асяроддзя.

Асноўная задача пры праектаванні бяспекі праграмных сродкаў – аналіз і вызначэнне неабходных рэсурсаў для стварэння жыццёвага цыкла праграмных сродкаў у адпаведнасці з патрабаваннямі кантракта і тэхнічнага задання. Фактарам канкурэнтаздольнасці праграмных сродкаў з'яўляецца суадносіны паміж каштоўнасцю (эфектыўнасцю) наяўнага або меркаванага прадукта з пазіцыі яго выкарыстання спажыўцом і коштам яго пры стварэнні або набыцці ва ўмовах рэальнага рынку.

Для гэтага трэба вызначыць наяўнасць на рынку гамы блізкіх па прызначэнні праграмных сродкаў, ацаніць іх эканамічную эфектыўнасць, кошт, ужывальнасць і бяспека, а таксама магчымую канкурэнтаздольнасць меркаванага праграмнага прадукта.

Бяспека сістэмы праграмных сродкаў забяспечваецца стварэннем функцыянальных праграм высокай якасці з мінімальнай колькасцю дэфектаў і памылак, якія адлюстроўваюцца на бяспецы. Кіраўніцтва бяспекай складанага праекту ажыццяўляюць менеджэры.

Мэнэджар бяспекі праекту забяспечвае камунікацыю паміж замоўцам і адмыслоўцамі. Яго задача – вызначыць і забяспечыць поўнае задавальненне заказчыка па бяспецы сістэмы; менеджэр-архітэктар комплексу праграм павышэння бяспекі кіруе камунікацыямі і ўзаемаадносінамі ў камандзе,

з'яўляецца каардынатарам стварэння кампанентаў, распрацоўвае базавыя, функцыянальныя спецыфікацыі і кіруе імі, вядзе графік праекта і дае справаздачу за яго стан, ініцыюе прыняцце крытычных для ходу праекта рашэнняў.

Спецыфікатары падрыхтоўваюць апісанні функцый адпаведных кампанентаў з узроўнем дэталізацыі, дастатковым для распрацоўкі тэкстаў праграм праграмістамі; распрацоўнікі праграмных кампанентаў (праграмісты) ствараюць кампаненты, якія задавальняюць спецыфікацыям, рэалізуюць патрабаваныя функцыі прадукта; сістэмныя інтэгратары ствараюць на вынахадзе патрабаваныя буйныя кампаненты ці комплекс праграм. Тэсціроўшчыкі забяспечваюць праверку функцыянальных спецыфікацый, выконваюць тэсціраванне фаз і кампанента праекта.

Кіраўнікі забяспечваюць сінэргію кампанентаў і рэалізацыю версій праграмных сродкаў. Дакументатары ажыццяўляюць падрыхтоўку і выданне зводных тэхналагічных і эксплуатацыйных дакументаў у адпаведнасць з патрабаваннямі стандартаў.

Тэхнолагі, забяспечваюць ужыванне сістэмы якасці праекта або прадпрыемствы, кантралююць і інспектуюць яе выкарыстанне. Праграмныя сродкі павінны паступаць на эксплуатацыю, захоўваючы актуальнасць да таго, як у іх знікае неабходнасць. Іх мэты, канцэптуальная аснова і алгарытмы не павінны састарэць за час распрацоўкі.

Падрыхтоўка тэкстаў праграм, іх тэсціраванне, камплексаванне, дакументаванне і выпрабаванні могуць праводзіцца ў асноўным паслядоўна. Гэта патрабуе некаторага часу.

У сучасных праектах праграмных сродкаў большую ці меншую долю складаюць гатовыя апрабаваныя кампаненты з іншых падобных распрацовак. Гэта дае магчымасць значна паскараць работы і скарачаць затраты на стварэнне складаных комплексаў праграм.

Абарона інфармацыі

Разгледзім асноўныя моманты абароны інфармацыі ад несанкцыянаванага доступу. Гаворка ідзе аб такім парадку працы, пры якім:

- доступ да інфармацыі мае толькі той карыстач, які мае дазвол;
- будзем называць такога карыстальніка законным;
- кожны законны карыстальнік працуе толькі са сваёй інфармацыяй і не мае доступу да інфармацыі іншага законнага карыстальніка;
- кожны законны карыстальнік можа выконваць толькі тыя аперацыі, якія яму дазволена выконваць.

Для арганізацыі такога парадку неабходна забяспечыць распазнанне законнага карыстальніка. Гэты працэс часта называюць аўтарызацыяй карыстальніка.

Аўтарызацыя карыстальніка ўключае тры этапы.

- Ідэнтыфікацыя карыстальніка.
- Аўтэнтыфікацыя карыстальніка.
- Непасрэдна аўтарызацыя карыстальніка.

Ідэнтыфікацыя карыстальніка (identification) – гэта, з аднаго боку, прысваенне карыстачу ідэнтыфікатара – некаторай унікальнай прыкметы (ці некалькіх); з іншага боку, працэс, падчас якога карыстач паказвае прысвоены яму ідэнтыфікатар.

Ідэнтыфікацыя – гэта працэс, пры якім карыстач заве сябе.

У працэсе аўтарызацыі для законнага карыстальніка вызначаюцца правы карыстальніка, гэта значыць вызначаюцца даныя, з якімі яму дазволена працаваць; аперацыі, якія яму дазволена выконваць.

Ідэнтыфікацыя карыстальніка можа быць заснавана на

• веданні некаторай сакрэтнай інфармацыі (пароль, код);

• валоданні некаторым спецыяльным прадметам або прыладай (магнітная картка, электронны ключ);

• біяметрычных характарыстыках пальца, вока, голасу.

Да сістэм ведаў некаторай сакрэтнай інфармацыі ставяцца праграмныя механізмы парольнай абароны. Сістэмы, заснаваныя на валоданні некаторым спецыяльным прадметам або прыладай (магнітная картка, электронны ключ), як правіла, мяркуюць таксама веданне карыстальнікам некаторай сакрэтнай інфармацыі.

Сістэмы, заснаваныя на валоданні некаторым спецыяльным прадметам або прыладай, мяркуюць выкарыстанне магнітнай карткі. Сістэма абароны забяспечваецца прыладай чытання персанальнай інфармацыі (унікальнага кода карыстальніка), запісанай на магнітнай картцы.

Унікальны код карыстальніка захоўваецца на Proximity-карце, забяспечанай радыёперадавальнікам. Адмысловы счытвальнік стала выпраменьвае электрамагнітную энергію. Пры трапленні карты ў электрамагнітнае поле, карта пасылае счытвальніку свой код, які затым сістэма параўноўвае з эталонам.

Найбольшае распаўсюджванне атрымалі сістэмы абароны, якія выкарыстоўваюць смарт-карты (SmartCard – інтэлектуальная карта). У памяці смарт-карты таксама захоўваецца эталонная інфармацыя для аўтэнтыфікацыі карыстальніка, але ў адрозненне ад традыцыйнай магнітнай карткі, смарт-карта змяшчае мікрапрацэсар, які дазваляе вырабляць некаторыя пераўтварэнні ўнікальнага кода карыстальніка або некаторыя іншыя дзеянні.

Паралельна з развіццём смарткарт-тэхналогій развіваюцца тэхналогіі, заснаваныя на выкарыстанні электронных ключоў. Сістэмы выкарыстоўваюць унікальныя індывідуальныя асаблівасці будовы чалавечага цела для ідэнтыфікацыі асобы. У склад сістэм уваходзяць спецыяльныя счытвальныя прылады, якія генеруюць эталонныя ідэнтыфікатары карыстальнікаў, а таксама прылады або праграмнае забеспячэнне, якое аналізуе прад'яўлены ўзор і параўноўвае яго з захоўваецца эталонам.

Распрацаваны разнастайныя прылады, якія дазваляюць ідэнтыфікаваць асобу на аснове біяметрычных характарыстык. Прылады счытвання адбіткаў

пальцаў ідэнтыфікуюць асобу па форме і колькасці дэталяў – кропак пачатку і канца ліній на пальцы.

Сканары сятчаткі вока скануюць узоры сятчаткі вока карыстача, засяроджваючыся на ўнікальных крывяносных пасудзінах. З дапамогай інфрачырвонага выпраменьвання з яркасцю лямпачкі навагодняй ёлкі бяруцца дадзеныя па 300 кропках у вобласці сятчаткі вока, і сабраная інфармацыя пераўтворыцца ў лік.

Прылады верыфікацыі голасу будуюць матэматычную мадэль вакальнага дыяпазону гаворыць і выкарыстоўваюць яе для параўнання з узорам голасу. Распрацоўнікі такіх сістэм надаюць увагу рашэнню праблеме падману такіх сістэм з дапамогай магнітафонаў.

Прылады счытвання геаметрыі рукі выкарыстоўваюць святло для пабудовы трохмернай выявы рукі чалавека, правяраючы такія характарыстыкі, як даўжыня і шырыня пальцаў, і таўшчыня рукі.

Біяметрычныя сістэмы складана рэалізуюцца, патрабуюць захоўвання аб'ёмных баз дадзеных, надзейных тэхналогій распазнання выяў і дарагой счытвальнай апаратуры. Таму прымяняюцца такія сістэмы абароны ад несанкцыянаванага доступу ў асноўным ва ўстановах, якія патрабуюць асаблівага кантролю доступу да сакрэтнай інфармацыі.

Аўтэнтыфікацыя карыстальніка звычайна рэалізуецца па адной з двух схем: простая PIN-аўтэнтыфікацыя або абароненая PIN-аўтэнтыфікацыя. Абедзве схемы заснаваныя на ўсталяванні сапраўднасці карыстача пасродкам параўнання PIN-кода карыстача (PIN – Personal identification number, персанальны ідэнтыфікацыйны нумар) з эталонам.

Пры простай PIN-аўтэнтыфікацыі PIN-код дасылаецца ў ключ (смарт-карту). Ключ (смарт-карта) параўноўвае яго з эталонам, які захоўваецца ў яго (яе) памяці, і прымае рашэнне аб далейшай працы.

Працэс абароненай PIN-аўтэнтыфікацыі рэалізуецца па наступнай схеме. Абароненае прыкладанне пасылае запыт ключу (смарт-карце) на PIN-аўтэнтыфікацыю. Ключ (смарт-карта) вяртае выпадковы 64-разрадны лік.

Прыкладанне складае гэты лік па модулі 2 з PIN-кодам, які ўвёў уладальнік ключа (смарт-карты), зашыфроўвае яго DES-алгарытмам на адмысловым ключы аўтэнтыфікацыі і пасылае вынік ключу (смарт-карце). Ключ (смарт-карта) ажыццяўляе зваротныя пераўтварэнні і параўноўвае вынік з тым, што захоўваецца ў яго (яе) памяці.

У выпадку супадзення лічыцца, што аўтэнтыфікацыя прайшла паспяхова і карыстач (дадатак) можа працягваць працу.

Электронны ключ – гэта некаторая фізічная прылада. Ён можа быць выкананы або на аснове спецыялізаванага чыпа, або на мікрасхемах энерганезалежнай па-электрычнаму перапраграмуемай памяці, або на базе мікрапрацэсараў.

Стандарты і тэхналогіі, у прыватнасці, тэхналогія падлучэння прылад на аснове USB-шыны – Universal Serial Bus, дазваляюць мець дадатковыя парты ў зручных і лёгкадаступных месцах кампутара і тым самым спрыяюць шырокаму ўжыванню апаратных прылад абароны. У памяці электроннага ключа захоўваецца ўнікальная інфармацыя. Праграмная частка сістэмы абароны вызначае наяўнасць электроннага ключа пры запуску праграмы і правярае правільнасць якая змяшчаецца ў ключы інфармацыі.

Памяць электроннага ключа, акрамя ўнікальнай інфармацыі аб карыстачу (рэгістрацыйны нумар, пароль, PIN-код), можа ўтрымоўваць і іншыя параметры. Распрацоўнікі абароны з мэтай процідзеяння незаконнаму распаўсюджванню і выкарыстанню праграмнага забеспячэння ўключаюць у электронны ключ інфармацыю аб праграмным забеспячэнні, напрыклад, серыйны нумар праграмы; нумар версіі; дату выпуску (продажы).

Пры наяўнасці магчымасці праграмы працаваць у дэманстрацыйным рэжыме, ці ў рэжыме блакавання некаторых функцый, электронны ключ дапаўняецца інфармацыяй аб колькасці запускаў прыкладання, лімітавага часу (даты) працы. Заўважым, што пры гэтым электронны ключ можа служыць і для абароны ўмоўна-бясплатнага праграмнага забеспячэння.

Тэхналогіі дыстанцыйнага перапраграмавання памяці ключа выкарыстоўваюцца распрацоўшчыкамі, па-першае, для процідзеяння незаконнаму выкарыстанню праграм. Дыстанцыйнае перапраграмаванне памяці ключа дазваляе распрацоўніку з максімальнай ступенню выгоды для канчатковага карыстальніка суправаджаць праграмнае забеспячэнне.

Напрыклад, разам з новай версіяй прадукта карыстач атрымлівае і адмысловы модуль, які вырабляе мадыфікацыю поля нумара версіі ў памяці электроннага ключа. Модуль абароны заўсёды робіць параўнанне нумара версіі праграмы з адпаведным полем. Такі механізм перашкаджае нелегальнаму выкарыстанню праграмы. Парушальнік не зможа скарыстацца незаконна атрыманай копіяй новай версіі прадукта без перапраграмавання памяці электроннага ключа.

Зручны для карыстальніка і перавод праграмнага забеспячэння з працы ў дэманстрацыйным рэжыме на рэжым поўнага функцыянавання. Пасля аплаты карыстальнік таксама атрымлівае спецыяльны модуль, які мадыфікуе поле памяці электроннага ключа, адказнага за такі перавод. Пры гэтым карыстач вызваляецца ад неабходнасці пераўсталёўкі і пераналадкі прыкладання.

У залежнасці ад унікальнай інфармацыі аб карыстальніку і спецыяльных палёў у памяці ключа, карыстачу даступныя тыя ці іншыя функцыі праграмы. Перапраграмаванне памяці ключа дазваляе адкрыць або зачыніць доступ да некаторых функцый.

Электронныя ключы забяспечваюць таксама ліцэнзаванне ў сетках. Ліцэнзія – гэта абумоўленыя пры куплі праграмнага прадукта права на выкарыстанне праграмы.

Праблема вырашаецца з дапамогай спецыяльных праграм – адміністратараў ліцэнзій (licence manager). Кантроль такіх праграм ускладаецца на адміністратараў сетак і часта не абаронены ад падману. Таму неабходна, каб кантроль прадукта вырабляў сам распрацоўнік.

Для гэтага можна ў памяці электроннага ключа ў асобных, абароненых ад запісу палях, захоўваць лічыльнік ліцэнзій, а таксама максімальную колькасць карыстальнікаў ліцэнзуемага прыкладання. Сістэма, якая выкарыстоўвае такі электронны ключ, дазваляе кантраляваць і абмяжоўваць колькасць станцый, якія працуюць адначасова з абароненай праграмай.

Чыннікам, якая стрымлівае выкарыстанне праграмна-апаратнай абароны, з'яўляецца высокі кошт дадатковых апаратных прылад. Звычайна гэта дарагія счытвальныя прылады, так званыя рыдары (reader). Таму поспех на рынку сістэм праграмна-апаратнай абароны забяспечаны тым вытворцам, электронныя ключы якіх з'яўляюцца зручнейшымі і таннымі.

На практыцы галоўным чынам ужываюцца два спосабу ўзлому праграмна-апаратнай абароны: адключэнне (узлом) праграмнай часткі абароны; эмуляванне электроннага ключа.

Першы спосаб узлому складаецца ў выдаленні (мадыфікацыі) з абароненага прыкладання поўнасцю або часткова кодаў, звязаных з механізмам абароны. Напрыклад, часам дастаткова выдаліць з праграмы каманды апытання электроннага ключа і каманды параўнання з эталонам.

Эмуляванне электроннага ключа – гэта спосаб узлому шляхам эмулявання праграмнымі ці апаратнымі сродкамі працы электроннага ключа.

Эмулятар – праграма, якая выконвае функцыі, звычайна рэалізуемыя некаторай вонкавай прыладай. Праграма-эмулятар рэалізавана такім чынам, што вяртае абароненаму з дадаткам "правільныя" адказы на ўсе звароты да электроннага ключа. У выніку атрымоўваецца электронны ключ, рэалізаваны толькі на праграмным узроўні.

Для абароны ад эмуляцыі электроннага ключа рэкамендуецца выкарыстоўваць хаатычны парадак абмену інфармацыяй паміж абароненым дадаткам і электронным ключом. Звычайна эмулятар узаемадзейнічае з абароненым дадаткам альбо праз кропку ўваходу API выкліку ключа, альбо падменай драйвера працы з ключом.

Бяспека апаратных сродкаў

Сучасная канцэпцыя апаратных падыходаў да забеспячэння бяспекі абапіраецца на ўбудаваныя ў абсталяванне праграмы, таму пастаўшчыкам абсталявання і даследчай супольнасці неабходна змяняць менталітэт.

Да бяспекі прашывак варта ставіцца гэтак жа, як і да надзейнасці праграмнага забеспячэння. Кампутарныя сістэмы складаюцца з апаратнае і праграмнае забеспячэнне: фізічныя кампаненты, якія выконваюць фіксаваны набор аперацый; лагічныя элементы, якія складаюцца з дадзеных і інструкцый, якія вызначаюць сцэнары выканання апаратных аперацый; а таксама ўваходныя дадзеныя для іх.

Кожная асобна ўзятая функцыя можа быць рэалізавана з выкарыстаннем розных спалучэнняў апаратных і праграмных кампанентаў, ці поўнасцю апаратных сродкаў. Ад спалучэння апаратнага і праграмнага забеспячэння залежаць уласцівасці выканання функцыі: прадукцыйнасць і бяспека сістэмы.

Лічылася, што менавіта апаратная абарона лепш за ўсё супрацьстаіць патэнцыйным нападам. Гэта знайшло адлюстраванне ў даўно выкарыстоўваных апаратных модулях бяспекі (hardware security module, HSM), такіх як распазнаюць несанкцыянаваныя аперацыі і абароненыя ад нападаў крыптакарты IBM CryptoCards, а таксама Intel Software Guard Extensions (SGX) і ARM TrustZone.

Фізічная прырода кампанентаў азначае, што пасля адгрузкі прылады кліентам ухіліць магчымыя дэфекты будзе вельмі цяжка, што прымушае распрацоўнікаў абсталявання дзейнічаць кансерватыўна і ўдумліва. Усё гэта спрыяе фармаванню адчування дадатковай бяспекі і большай упэўненасці ў абароне ў параўнанні з выкарыстаннем праграмнага забеспячэння. Нязменнасць – гэта здольнасць функцыянальных уласцівасцяў супраціўляцца змене іх зыходнай архітэктуры.

Нязменнасць з'яўляецца перавагай ўдвая, паколькі апаратнае забеспячэнне не мае патрэбы ў рэалізацыі «машыны Цьюрынга». Усё гэта спрыяе абмежаванню магчымай шкоды, які наносіцца ў выпадку кампраметацыі ці няспраўнасці абсталявання: стан апаратнага перамыкача ў ланцугі можа быць зменена зламыснікам з выключаны на ўключаны, але перамыкач нельга перапраграмаваць нейкім зусім іншым чынам.

Праграмнае забеспячэнне, наадварот, мае поўнафункцыянальны механізм для выканання чагосьці, істотна адрознага ад запланаванага функцыяналу. У выніку скампраметаванае або дэфектнае праграмнае забеспячэнне дае зламысніку доступ да поўнага па Цьюрынгу асяроддзі, дзе можна выконваць выпадкова зададзеныя функцыі.

Пад прывілеямі разумеецца магчымасць назіраць і кантраляваць аперацыі іншых кампанентаў. Гэтае азначэнне мае досыць тонкае адрозненне ад характарыстыкі прывілеяў на ўзроўні магчымасцяў ядра, супрацьпастаўленых паўнамоцтвам карыстача, паколькі праграмнае забеспячэнне з больш высокімі прывілеямі звычайна ахапляе і аперацыі праграм, прывілеі якіх апыняюцца ніжэй. Апаратныя і праграмныя прывілеі адрозніваюцца тым, што абсталяванне і праграмнае забеспячэнне не могуць выконваць адзін і той жа набор працэдур.

Прывілеяванае праграмнае забеспячэнне мае магчымасць кіраваць, запускаць, спыняць і перарываць не прывілеяванымі праграмамі, а таксама назіраць (чытанне, запіс) за станам іх выканання. Аналагічнай выявай абсталяванне, у якога прысутнічае механізм выканання праграмнага забеспячэння, валодае такой жа здольнасцю кіраваць любымі запускаемымі ім праграмамі і ажыццяўляць назіранне за іх станам.

Сучасныя кампутары маюць універсальную шматузроўневую архітэктуру, пачынальна з абсталявання і ўбудаванага праграмнага забеспячэння, гіпервізара віртуальных машын, аперацыйнай сістэмы і заканчваючы праграмамі.

Гіпервізар абаронены ад ядра аперацыйнай сістэмы, якое абаронена ад прыкладанняў. Абсталяванне ў гэтым стэку займае найболей прывілеяванае становішча і абаронена ад уразлівасцяў і нападаў, якія ініцыююцца на меней прывілеяваных праграмных узроўнях.

Існуе гібрыдны тып рэалізацыі вылічальных функцый – мікрапраграмная прашыўка, або ўбудаванае праграмнае забеспячэнне. Тэрмін «прашыўка» быў прапанаваны Ашэрам Оплерам у 60-х гадах XX стагоддзя.

Прашыўка мае з праграмным забеспячэннем шэраг агульных уласцівасцяў, паколькі рэалізавана ў выглядзе праграмных інструкцый, якія выконваюцца на поўным па Цьюрынгу апаратным працэсары агульнага прызначэння.

Каб лепш зразумець, што ўяўляюць сабой абсталяванне, прашыўка і праграмнае забеспячэнне, параўнаем чатыры параметры гэтых кампанентаў: нязменнасць, прывілеі, эфектыўнасць і кошт.

Нязменнасць характарызуе магчымасць змены функцыянальнасці кампанента. Калі ў абсталявання нязменнасць з'яўляецца яго неад'емнай уласцівасцю, то з прашыўкай і праграмным забеспячэннем справа ідзе інакш. Нязменнасць тут забяспечваецца нейкім іншым кампанентам (апаратным ці праграмным). Адрасная прастора прашыўкі звычайна зачынена для прыкладанняў. Нязменным з'яўляецца толькі абсталяванне.

Прашыўка і праграмнае забеспячэнне могуць свядома змяняцца пэўнымі кампанентамі сістэмы або падвяргацца зменам з прычыны недахопаў праектавання і рэалізацыі. Пры гэтым выключаецца магчымасць нападаў падчас пастаўкі прадукта яшчэ да яго траплення да карыстача.

Але нават у гэтым выпадку абсталяванне ў скампраметаванай прылады застаецца нязменным. Траяны, укаранёныя распрацоўшчыкам або вытворцам, не могуць быць выдалены сродкамі прашыўкі або праграмнага забеспячэння.

Прывілеі вызначаюцца загадзя. Яны характарызуюць магчымасць кампанента з больш высокімі прывілеямі назіраць за выкананнем праграм на

элементе з меншымі паўнамоцтвамі і кіраваць імі. Паколькі ўсё праграмнае забеспячэнне павінна выконвацца на абсталяванні, тое яно мае больш высокія прывілеі, чым прашыўка і праграмнае забеспячэнне.

Прашыўка знаходзіцца на апаратным баку апаратна-праграмнага інтэрфейсу. Яна мае больш высокія прывілеі, чым праграмнае забеспячэнне, уключаючы ядро аперацыйнай сістэмы і прыкладанні. Такім чынам, прывілеі абсталявання з'яўляюцца самымі высокімі, прывілеі прашыўкі – сярэднімі, а прывілеі праграмнага забеспячэння – самымі нізкімі.

Прашыўка знаходзіцца бліжэй да абсталявання і можа мець доступ да спецыяльных апаратных функцый і сродкаў, што робіць яе больш эканамічнай у параўнанні з праграмным забеспячэннем. Напрыклад, прашыўка працэсара (мікракод) не залежыць ад кантэкстных пераключэнняў і планавальніка аперацыйнай сістэмы, у адрозненне ад звычайнага прыкладнога праграмнага забеспячэння.

Кошт абсталявання ў кожнай сістэмы, як правіла, фіксаваная, а дадатковыя выдаткі на разгортванне праграмнага забеспячэння фактычна роўныя нулю. У выніку сістэмы, якія змяшчаюць больш спецыялізаванае абсталяванне, абыходзяцца ў вытворчасці даражэй, што павялічвае іх кошт для канчатковага карыстальніка. Хутчэйшыя сістэмы, якія выкарыстоўваюць апаратныя паскаральнікі, каштуюць даражэй.

Прашыўка забяспечвае інтэраперабельнасць паміж мноствам розных інтэрфейсаў кампутарных сістэм. Интероперабельность азначае, што розныя рэалізацыі кампанентаў змогуць нармальна ўзаемадзейнічаць сябар з сябрам, паколькі ўсе яны прытрымваюцца стандартнага інтэрфейсу.

Рэалізацыя гэтага інтэрфейсу на аснове спалучэнняў апаратных і праграмных кампанентаў дазваляе вытворцам ствараць розныя прадукты з рознымі суадносінамі кошту і эфектыўнасці. Так, сеткавыя платы выконваюць адну і тую ж функцыю. Даражэйшыя і хуткія прадукты могуць утрымоўваць розныя паскаральнікі і тэхналогіі разгрузкі, што спрашчае паскораную апрацоўку пакетаў.

Яны спажываюць менш энергіі, вызваляючы вылічальныя цыклы агульнага прызначэння на асноўным працэсары. Прыкладна такімі ж уласцівасцямі валодаюць спецыялізаваныя крыптаграфічныя паскаральнікі. Аперацыі, якія не патрабуюць высокай прадукцыйнасці, могуць быць рэалізаваны ў прашыўцы. Паколькі ўсе гэтыя варыянты не ўплываюць на інтэрфейс, іх можна ўзаемна замяняць, не мяняючы праграмнага забеспячэння і іншыя апаратныя кампаненты.

Перавага прашыўкі злучана з магчымасцю абнаўлення і выпраўлення апаратных памылак. Дзякуючы гэтаму можна ўсталёўваць абнаўленні падчас эксплуатацый. Так, важнай умовай выбару той ці іншай мадэлі смартфона з'яўляецца час, на працягу якога вытворца абавязваецца ўстараняць выяўленыя ў прашыўцы ўразлівасці, выпускаючы адпаведныя абнаўленні.

Ключавой умовай бяспекі абсталявання з'яўляецца яго нязменнасць пад уздзеяннем праграмнага забеспячэння, што адбываецца натуральным чынам.

Многія функцыі сучаснага абсталявання на практыцы рэалізаваны на ўзроўні прашыўкі і ўкараняюцца ітэрацыйна: гэта значыць спачатку – SGX (Software Guard Extensions), затым – SGX2. Зараз не патрабуецца замена кампанентаў, паколькі дэфекты ў апаратным забеспячэнні могуць быць выпраўлены шляхам змены ўбудаванага праграмнага забеспячэння. У выніку ў абсталявання з'яўляюцца як дадатковыя перавагі (гнуткасць і магчымасць абнаўлення), так і недахопы (складанасць і зменлівасць), уласцівыя праграмнаму забеспячэнню.

Калі прылады скампраметаваць, то яны могуць выконваць функцыі, якія не прадугледжваліся пры праектаванні. Адзін з такіх прыкладаў – клавіятура, якая на прыладзе Apple з дапамогай простых праграмных сродкаў пераўтвораная ў рэгістратар націску клавіш. Калі апаратныя функцыі рэалізуюцца з дапамогай прашыўкі, гэта адбіваецца на нязменнасці абсталявання і саслабляе яго ўстойлівасць да нападаў.

Перыферыйныя прылады кампутараў – дыскавыя назапашвальнікі, клавіятуры, мышы і друкаркі звычайна лічацца занадта простымі, для таго

каб іх кампраметаваць і выкарыстоўваць для нападаў. Аднак гэтыя прылады ўсё часцей прапануюць функцыянальнасць, якая рэалізуецца убудаваным праграмным забеспячэннем, што прыводзіць да з'яўлення ўразлівасцяў.

Жорсткія дыскі і цвёрдацельныя назапашвальнікі, якія звычайна разглядаюцца як простыя блокавыя прылады, утрымоўваюць шмат убудаванага праграмнага забеспячэння. Падчас аналізу бяспекі цвёрдацельных назапашвальнікаў, на прыладу Crucial MX100/MX200 была праведзена паспяховая атака з пяра прашыўкай убудаванага праграмнага забеспячэння, выкананая з выкарыстаннем некалькіх недакументаваных каманд канкрэтнага пастаўшчыка.

Выяўленая ўразлівасць дазваляе хакеру выдалена і ўтойліва перахапляць любыя дадзеныя з дыска, не пакідаючы на кампутары ніякіх слядоў. Хакеру не патрэбен фізічны доступ.

У адрозненне ад звычайных шкоднасных праграм, у дадзеным выпадку шкоднасны код утрымоўваўся ў прашыўцы, таму нават поўная пераўсталёўка аперацыйнай сістэмы не прывядзе да ліквідацыі заражэння. У 2013 годзе было прадэманстравана, што на механічнай цвёрдай кружэлцы могуць быць усталяваныя ўтоеныя шчыліны.

У 2006-2007 гадах было паказана, як можна ўсталяваць частковы кантроль над сеткавым адаптарам Broadcom шляхам мадыфікацыі яго прашыўкі, а крыху пазней спектр дзеяння гэтага нападу быў пашыраны з мэтай атрымання поўнага кантролю над кампутарам з выкарыстаннем уразлівасці ў сеткавым адаптары Broadcom NetXtreme.

Уразлівасць была выяўлена ў прашыўцы, якая апрацоўвала пратакол Alert Standard Format – малавядомую працэдуру, прызначаную для выдаленага адміністравання.

Відэаплаты ў кампаненце відэа-BIOS (VBIOS) таксама ўтрымоўваюць убудаванае праграмнае забеспячэнне, якое загружаецца і выконваецца цэнтральным працэсарам прыкладна гэтак жа, як гэта адбываецца са звычайным BIOS. Прадпрымаліся спробы (у якасці прыкладу можна

прывесці nvresolution) наладзіць VBIOS такім чынам, каб палепшыць дазвол за рахунак драйвера видеобуфера.

Аднак відэаплаты могуць быць скарыстаны хакерамі для выканання шкоднаснага кода, што дапамагае пазбегнуць традыцыйнага выяўлення шкоднасных праграм. Графічны працэсар і відэапамяць ствараюць паўнавартаснае асяроддзе для выканання шкоднасных праграм.

А агульная памяць і цэнтральны працэсар выкарыстоўваюцца ў якасці дадатковых рэсурсаў для правядзення нападаў. У 2013 годзе даследнікі ўкаранілі ў кампутар праграму перахопу націску клавіш на клавіятуры, якая выконвалася не цэнтральным, а графічным працэсарам.

Розныя прылады ажыццяўляюць узаемадзеянне з іншымі кампанентамі праз шыны, такія як PCI і USB. У прыладах, што падключаюцца да гэтых шын, рэалізаваны агульныя функцыянальныя магчымасці іх аўтаматычнага выяўлення і налады.

А таксама дазволы канфліктаў паміж асобнымі кампанентамі. Гэты функцыянал звычайна рэалізуецца на ўзроўні прашыўкі і становіцца крыніцай рознага роду ўразлівасцяў. У 2006 годзе, напрыклад, была даследавана асаблівая роля PCI-пашырэння пастаяннай памяці (read-only memory, ROM). Да гэтай катэгорыі адносіцца і VBIOS.

Адпаведная частка прашыўкі прылады можа загружацца аперацыйнай сістэмай падчас ініцыялізацыі. Было паказана, што з-за адсутнасці праверкі сігнатуры прашыўкі пашырэнне ROM платы PCI можа быць перапрашыта шкоднаснай праграмай.

Пасля гэтага поплатак можна выкарыстоўваць для правядзення розных перадзагрузных нападаў, у тым ліку для маніпуляцый з ядром аперацыйнай сістэмы пры падлучэнні да іншага кампутара.

Існаванне вялікай колькасці разнастайных USB-прылад тлумачыцца тым, што інтэрфейс USB прапануе развіты і гнуткі функцыянал. Інтэрфейс USB дазваляе эмуляваць кампаненты практычна любога тыпу, у адрозненне

ад інтэрфейсу SATA, да якога можна падлучаць толькі прылады захоўвання, калі аперацыйная сістэма не скампраметаваная.

Група даследнікаў прадэманстравала канцэпцыю BadUSB, якая прадугледжвае перапраграмаванне USB-прылад з наступным нападам на кампутар, да якога яны падлучаныя. Даследнікі, у прыватнасці, змаглі перапраграмаваць адну прыладу для эмуляцыі іншага – напрыклад, для эмуляцыі клавіятуры, якая стала накіроўваць дэструктыўную паслядоўнасць уводу на машыну ахвяры.

Уразлівасці ўзнікаюць з-за адсутнасці праверкі сігнатуры ў прашыўцы USB-прылад. Такім чынам, шкоднасная праграма, размешчаная на адной машыне, можа выкарыстоўваць USB-прылады для заражэння іншых.

Яна ў стане змяніць прашыўку вэб-камеры або назапашвальніка з інтэрфейсам USB з наступным заражэннем чарговай машыны, да якой будуць падключаны адпаведныя прылады. Адсутнасць кантролю цэласнасці прашыўкі распаўсюджана вельмі шырока. З 52 сямействаў мікрасхем і 33 рэальных прылад толькі ў адным сямействе была рэалізавана прымітыўная форма абароны.

Праблема пагаршаецца тым, што карыстачы, як правіла, надаюць менш увагі абнаўленню сістэмы бяспекі сваіх перыферыйных прылад у параўнанні з традыцыйнымі праграмнымі сістэмамі – асноўнай аперацыйнай сістэмай і сэрвісамі. Калі для большасці аперацыйных сістэм і прыкладанняў прапануюцца аўтаматычныя абнаўленні, якія абараняюць сістэмы ад вядомых уразлівасцяў, то абнаўленні прашыўкі перыферыйных прылад, напрыклад, цвёрдых кружэлак або адаптараў Bluetooth/Wi-Fi, выконваюцца значна радзей і павінны кіравацца самімі карыстачамі.

Галоўная рада пры правядзенні такіх абнаўленняў складаецца ў тым, што ініцыяваць іх варта толькі тады, калі ў гэтым ёсць відавочная неабходнасць. Таму і ўстанаўліваюцца яны даволі рэдка.

Калі ў 2017 годзе былі выяўлены ўразлівасці AMT і ME (CVE-2017-5689), гэта выклікала вялікую занепакоенасць сярод спецыялістаў па

бяспецы, паколькі адначасова высветлілася, што як ME, так і адпаведныя ўразлівасці маглі прысутнічаць у сістэмах яшчэ ў 2008 годзе.

Складовай часткай Intel AMT з'яўляецца дадатак (трастлет), якое выконваецца ў асяроддзі ME і дазваляе выдалена кіраваць кампутарам. Гэты вельмі важны функцыянал быў рэалізаваны ў прашыўцы, якая можа быць перазапісана і мадыфікавана патрэбным хакеру чынам.

У выніку атакавалы атрымлівае выдалены кантроль над сістэмай незалежна ад таго, якія праграмныя сродкі абароны прысутнічаюць у аперацыйнай сістэме. Размяшчаючыся на апаратным узроўні скампраметаванай сістэмы, Intel ME карыстаецца неабмежаванымі прывілеямі ў адносінах да ўсіх іншых частак сістэмы.

Фактычна нельга быць цалкам упэўненым у тым, што шкоднасны код сапраўды выдалены. Даследнікі пытанняў бяспекі актыўна вывучаюць Intel ME з 2009 года і прапанавалі тэрмін "руткіт трэцяга кольца", за якім хаваецца код, укаранёны ў ME з больш высокімі, чым у любога іншага праграмнага забеспячэння і прашывак кампутара, прывілеямі.

Ін'екцыйная атака выкарыстоўвае ўразлівасць у тэхналогіі аднаўлення памяці, характэрнай для працэсараў Intel. Узнікае магчымасць няправільнага перапрызначэння памяці, якое павінна быць забаронена.

Функцыя аднаўлення памяці, якая палегчыла правядзенне нападу, служыць для таго, каб сістэмнае праграмнае забеспячэнне магло перапрызначыць дынамічную аператыўную памяць пры канфліктах з дыяпазонам фізічных адрасоў, якія адлюстроўваюцца на прыладах уводу-высновы. Першапачатковая тэхналогія аднаўлення памяці не ўлічвала неабходнасці належнага кантролю доступу і праверкі памяці, якая выкарыстоўваецца Intel ME.

Хоць у Intel і ўхілілі гэтую ўразлівасць, зашыфраваўшы памяць ME і спрабуючы прадухіліць новыя кампраметацыі ізаляцыі ME, іншыя ўразлівасці ў ядры прашыўкі ME (напрыклад, CVE-2017-5705, 6, 7) прывялі да наступных кампраметацыяў прашыўкі і палёгкі.

У 2017 годзе ў чыпсэце Lewisburg кампанія Intel прадставіла новую тэхналогію Innovation Engine (IE). У адрозненне ад ME, тут дапушчаецца толькі выкананне ўбудаванага праграмнага забеспячэння ад Intel. IE прызначана для OEM-вытворцаў, што патэнцыйна павялічвае колькасць уразлівасцяў прашыўкі чыпсэта.

Чыпсэты, якія не адносяцца да ліку простых непраграмуемых элементаў матчынай платы, рэалізуюць складаны функцыянал. Яны змяшчаюць цэлы шэраг таямнічых прашывак, пра якія большасць карыстальнікаў маюць вельмі слабое ўяўленне.

Прашыўку, якая апрацоўваецца цэнтральным працэсарам у адрозненне ад іншых чыпаў, будзем зваць прашыўкай хаста. У параўнанні з прашыўкай чыпсэта, прашыўку хаста, вядомая як BIOS / UEFI (Unified Extensible Firmware Interface), – гэта нешта большае, чым проста адлюстраванне экрана пачатковай загрузкі і ініцыялізацыя кампутарнага абсталявання.

Нават пасля загрузкі сістэмы істотная частка прашыўкі хаста працягвае працаваць у рэжыме SMM (system management mode), у якім выконваецца высока прывілеяванае праграмнае забеспячэнне, якое рэалізуе найважнейшыя нізкаўзроўневыя сістэмныя функцыі, такія як кіраванне сілкаваннем і кантроль за абсталяваннем.

Паколькі SMM-код працуе з прывілеямі, якія пераўзыходзяць нават прывілеі аперацыйнай сістэмы, ён з'яўляецца мэтай для нападаў. На старых матчыных поплатках (выпускаліся да 2006 г) SMM-код мог быць пашкоджаны шкоднасным кодам ядра, паколькі праграма BIOS не магла хаваць аператыўную памяць кіравання сістэмай SMRAM (system management RAM), дзе выконваецца SMM-код, ад звычайнага/сістэмнага праграмнага забеспячэння. У рэгістры кіравання SMRAM (SMRAMC) біт D_OPEN вызначае бачнасць SMRAM, а біт D_LOCK блакуе ўвесь рэгістр SMRAMC і D_OPEN да наступнай перазагрузкі. На некаторых матчыных поплатках біт D_LOCK не ўсталёўваўся.

Хоць усё гэта было выпраўлена ў матчыных поплатках, якія выпускаліся ў наступным, слабасці ў прашыўцы SMM на гэтым не скончыліся. З 2008 гады эксплойты SMM выяўляюцца рэгулярна. Пазнейшыя кампраметацыі былі абумоўлены няздольнасцю абараніць SMM ад розных не звязаных паміж сабой механізмаў.

Напрыклад, дэфект аднаўлення памяці, які выкарыстоўваецца для кампраметацыі Intel ME, быў задзейнічаны і для нападаў на SMM. Гэта дазволіла шкоднаснай праграме ў аперацыйнай сістэме атрымаць доступ да SMRAM, выкарыстоўваючы тэхналогію аднаўлення, і перапрызначыць вобласць SMRAM у даступную вобласць памяці.

Выяўлена яшчэ адна кампраметацыя SMM з дапамогай нападу заражэння кэша. Звычайна сістэмнае праграмнае забеспячэнне можа наладжваць рэгістры дыяпазону тыпаў памяці MTRR (memory-type range registers) для кіравання тым, якая вобласць памяці кэшуецца, а якая не. Аднак для SMRAM ніякіх адрозненняў рабіць не сталі.

Такім чынам, у атакавалага ёсць магчымасць мадыфікаваць скапіяваны ў кэш SMM-код без непасрэднага доступу да SMRAM. У наступны раз мадыфікаваны код выконваецца ў SMM і робіць патрэбныя маніпуляцыі над актуальнай копіяй у SMRAM. Для вырашэння гэтага пытання быў створаны новы рэгістр дыяпазону кіравання сістэмай рэгістраў. Ён быў даступны толькі з SMM і мог наладжваць уласцівасці кэшавання SMRAM.

У 2009 годзе даследнікі выявілі, што няправільна напісаны SMM-код можа выклікаць функцыі, змешчаныя па-за SMRAM, што прыводзіць да патэнцыйнай магчымасці выканання адвольнага кода ў SMM.

Каб прадухіліць гэта, у рэгістр MSR_SMM_FEATURE_CONTROL быў дададзены новы элемент кіравання – біт SMM_Code_Chk_En, дзякуючы чаму магчымасць запуску ў SMM кода, выдатнага ад SMRAM, можна было наладзіць у першапачатковым кодзе SMM. Мірны перыяд працягнуўся да 2015 года, калі была выяўленая яшчэ адна ўразлівасць SMM, на гэты раз звязаная з тым, што SMM трэба было прымаць вонкавыя аргументы.

Калі перададзены паказальнік выкарыстоўваецца без праверкі, то SMM-код можа быць падманным шляхам запісаны ў SMRAM, пазначаную паказальнікам, што палягчае правядзенне нападаў.

Усё гэта ў сукупнасці прымусіла Intel прапанаваць у тым жа годзе высокаўзроўневае рашэнне – манітор пераносу SMM (SMM transfer monitor, STM). Замест выдалення ўсіх уразлівасцяў у SMM, STM імкнецца паменшыць магчымасці падвышэння прывілеяў праз SMM, змяншаючы прывілеі SMM-кода шляхам яго кантролю з дапамогай манітора.

Пасля правядзення неабходных праверак маніторам STM SMM-код паводзіць сябе як чакаецца. Аднак карыснасць STM не была гэтак пераканаўчай з прычыны таго, што ў гэты працэс было ўцягнута мноства розных бакоў: тыя, хто пісаў код універсальнага маніторынгу, які правярае спецыфічны для розных мадэляў SMM-код (ва ўмовах існавання мноства розных пастаўшчыкоў і мадэляў).

Тыя, хто вызначаў, як каардынаваць дзеянні распрацоўшчыкаў АС, распрацоўшчыкаў BIOS і пастаўшчыкоў абсталявання, паколькі праверкі STM можна ажыццяўляць толькі пасля таго, як усе кампаненты ўзгоднены. Шматлікія выяўленыя ўразлівасці (ускладненні, злучаныя з прашыўкамі; тэхналогіі матчыных поплаткаў, напрыклад бяспечная загрузка праз BIOS/UEFI; тэхналогія Intel Boot Guard, рэалізаваная праз Intel ME) не дазваляюць лічыць убудаванае праграмнае забеспячэнне надзейным.

Працэсар ніколі не быў чыста апаратным рашэннем. Пры выкананні складаных аперацый і рэалізацыі новых функцый усё гушчару выкарыстоўваецца мікракод, які можна разглядаць як яшчэ адзін узровень апаратных інструкцый.

Высветлілася, што нават калі дазволеныя толькі праверaныя пастаўшчыком абнаўлення, то хакер, які кіруе гэтым працэсам, усё роўна можа абраць абнаўленне такім чынам, каб палегчыць сабе правядзенне нападу. Але, ніводны з апошніх працэсараў пры правядзенні нападаў вытрымаў крытэр бяспекі.

Небяспека ўбудавання праграм у абсталяванне можна аналізаваць з двух бакоў: статыкі і дынамікі. Першая дакранаецца сталага захоўвання ўбудаванага праграмнага забеспячэння, а другая – бяспекі выкананага асяроддзя прашыўкі падчас выканання ўбудаваных праграм.

Адным з ключавых пераваг прашыўкі з'яўляецца магчымасць яе абнаўлення. Аднак убудаваныя праграмы павінны працаваць у энергазалежнай памяці, а такім чынам, патрэбна іх ізаляцыя ад іншых праграм. Усім гэтым можна занядбаць, калі прашыўка лічыцца часткай абсталявання.

Датуль пакуль прашыўка падае інтэрфейс абнаўлення, даступны кампанентам з ніжэйшымі прывілеямі, уключаючы сістэмную аперацыйную сістэму, існуе верагоднасць яе пашкоджання. Хаця многія з такіх інтэрфейсаў дазваляюць правядзенне толькі абнаўленняў, у якіх цэласнасць праверана з дапамогай крыптаграфічных сродкаў, існуюць розныя спосабы абыходу сертыфікатаў, што прыводзіць да кампраметацыі.

Паколькі прашыўка сама па сабе – гэта проста праграма, яна ўспадкоўвае ўразлівасці, якія могуць быць агульнымі для ўсіх тыпаў праграм. Пашкоджанне памяці ставіцца да шырокага спектру нападаў, дзе праграмныя дэфекты могуць дазволіць атакаваламу змяняць памяць праграмы спосабам, не прадугледжаным першапачатковым распрацоўшчыкам.

Уласны код і дадзеныя могуць служыць мэтам хакера. Адбываецца гэта таму, што прашыўка для выканання павінна быць загружана ў энергазалежную памяць, нават калі захоўваецца ў нязменным месцы. Бяспека памяці пакуль застаецца адкрытым пытаннем, не кажучы ўжо пра менш фармалізаваную распрацоўку ўбудаваных праграм. Тыповым прыкладам тут з'яўляюцца апошнія ўразлівасці ME: у ядры прашыўкі ME узнікаюць шматлікія перапаўненні буфера.

Фізічнай ізаляцыі ў прашыўкі можа не быць. Маецца толькі лагічная ізаляцыя ад звычайнага праграмнага забеспячэння, які працуе ў той жа сістэме, што вядзе да з'яўлення дэфектаў і ўразлівасцяў. У гэтым

заключаецца адрозненне ад няпоўнага па Цьюрынгу абсталявання, якое не падзяляе рэсурсы з праграмным забеспячэннем або з'яўляецца фізічна ізаляваным.

Прамы доступ да памяці (direct memory access, DMA) ставіцца да прашыўкі ўсіх прылад з высокай прапускной здольнасцю. Каб пазбегнуць ператварэнні цэнтральнага працэсара ў вузкае месца з пункта гледжання прадукцыйнасці, кантролер памяці працэсара дазваляе прыладам і сістэмнаму праграмнаму забеспячэнню наладжваць дыяпазоны памяці, якія будуць даступныя як працэсару прылады, так і цэнтральнаму працэсару.

Пасля гэтага працэсар прылады можа перамяшчаць дадзеныя аўтаномна. Які прадстаўляецца кантролерамі прамы доступ да памяці спараджае пралом ва ўжо падзеленых прасторах – адчыняе памяць для USB-прылад, сховішчаў SATA і сеткавых прылад.

Убудаванне праграм у абсталяванне ўжо само па сабе выклікае асцярогі, але сітуацыю яшчэ мацней пагаршае тое, што архітэктура і рэалізацыя большасці прашывак застаюцца прапрыетарнымі і па большай частцы недакументаванымі. Супольнасць спецыялістаў па бяспецы належыць галоўным чынам на зваротнае праектаванне, з тым, каб хаця б часткова раскрыць дэталі. Такая непразрыстасць хавае ад грамадскасці патэнцыйныя праблемы, у той час як рэальныя напады не абавязкова праводзяцца з выкарыстаннем даступнай інфармацыі.

Умацаванню бяспекі невядомасць не садзейнічае. Хутчэй, наадварот, можа прывесці да таго, што сур'ёзныя ўразлівасці застануцца незаўважанымі, паколькі даследчыкам пытанняў бяспекі давядзецца патраціць дадатковыя намаганні для атрымання базавай інфармацыі, перш чым яны змогуць выявіць і раскрыць слабыя месцы.

Напады на прашыўкі паказваюць, што для кампраметацыі сістэмы фізічны доступ да яе не патрэбен: жаданая ўласцівасць абсталявання, у адпаведнасці з якім для мадыфікацыі абавязкова патрабуецца фізічны доступ,

больш не працуе. Гэта цалкам супярэчыць агульнапрынятаму ўяўленню аб нязменнасці апаратных сродкаў.

Акрамя таго, бяспека праграмнага забеспячэння залежыць ад базавага абсталявання. Паколькі мадэль пагроз кампутарнай сістэмы мяркуе, што абсталяванне павінна быць надзейным, скампраметаванае апаратнае забеспячэнне падрывае ўсе гарантыі бяспекі. Такім чынам, убудаванне праграм у абсталяванне прыводзіць да збояў, як абсталяванні, так і праграмнага забеспячэння.

Напады на ўбудаванае праграмнае забеспячэнне накіраваны на «перапрашыўку» сталага сховішча і з'яўляюцца статычнымі, якія ўплываюць на нязменлівасць. Калі б убудавання праграм у абсталяванне не існавала, то не было б і ніякіх механізмаў абнаўлення. Правядзенне нападаў падобнага роду было б выключана. Пры адсутнасці ўбудавання праграм у абсталяванне такія напады пацярпелі б няўдачу, паколькі апаратнае забеспячэнне не мае патрэбы ў агульнай адраснай прасторы і неўспрымальна да парушэнняў памяці. Такім чынам, і гэты вектар нападу таксама быў бы ліквідаваны.

Простым спосабам забеспячэння бяспекі з'яўляецца адмова ад прашывак. Але для выкарыстання прашыўкі існуе мноства прычын, не злучаных з бяспекай. Прашыўка адкрывае шлях да стварэння розных рэалізацый, якія фарміруюць баланс паміж эфектыўнасцю і коштам, што вельмі важна для захавання кампутарнай галіны. Наяўнасць апаратнага забеспячэння, якое часткова абнаўляецца на месцах, мае шмат важных пераваг, якія нельга ігнараваць.

У апаратным забеспячэнні без якая абнаўляецца прашыўкі могуць прысутнічаць памылкі. Адзін з варыянтаў уразлівасці Spectre не можа быць ліквідаваны шляхам абнаўлення прашыўкі (мікракода), паколькі ён убудаваны непасрэдна ў апаратную логіку.

Магчымасць выпраўлення абсталявання з'яўляецца перавагай убудаванага праграмнага забеспячэння з пункта гледжання бяспекі. Перавагі ўбудаванага праграмнага забеспячэння перавешваюць пагрозы сістэме

бяспекі, а такім чынам, для абсталявання з убудаванымі праграмамі трэба шукаць метады забеспячэння такога ж узроўня бяспекі, як і для чыста апаратных рэалізацый.

Паколькі ўбудаванне праграм у абсталяванне непазбежна, важна прызнаць, што велізарны аб'ём кода, які выконвае апаратныя функцыі, заслугоўвае такой жа (ці нават больш пільнай) увагі, як і звычайнае праграмнае забеспячэнне. Высоканадзейныя нізкаўзроўневыя праграмныя кампаненты часцяком непразрыстыя ў сваёй функцыянальнасці. Іх прапрыетарная прырода перашкаджае аўдыту і праверцы бяспекі. Нізкаўзроўневыя прывілеі падахвочваюць рэалізоўваць складаную і не мелую адносіны да першапачатковага праекту функцыянальнасць.

Канцэпцыя апаратных падыходаў да забеспячэння бяспекі абапіраецца на ўбудаваныя ў абсталяванне праграмы. Таму пастаўшчыкам абсталявання і даследчай супольнасці неабходна змяняць менталітэт: да прашыўкі варта ставіцца гэтак жа, як і да звычайнага праграмнага забеспячэння.

Прынцыпы праектавання сістэм бяспекі, шырока прымяняюцца ў праграмным забеспячэнні, можна прымяніць і да прашыўкі. Грамадскі кантроль дапамагае звесці да мінімуму ўзнікненне пытанняў, выкліканых непразрыстасцю. Некаторыя адкрытыя фрэймворкі (напрыклад, coreboot і OpenWrt) выступаюць у ролі арыенціраў для праектавання бяспечных прашывак.

Пры выяўленні рызык, якія прычыняюць шкоду, памяншэнне шкоды, якую яны могуць нанесці, гэтак жа важна, як і іх прадухіленне. Прывілеі прашыўкі могуць кіравацца на яшчэ ніжэйшым узроўні для дэталізаванага кантролю доступу. Каб вырашыць пытанне недастатковага падзелу, можна абраць падыход з найменшымі прывілеямі для далейшага разгляду палепшанай мадэлі прашыўкі, якая яшчэ больш абстрагуецца ад праграмнага забеспячэння і не падзяляе функцыі з кантролем доступу.

Як і ў выпадку са звычайным праграмным забеспячэннем, асноўнай прычынай уразлівасці з'яўляецца складанасць. Традыцыйна распрацоўшчыкі

абсталявання, выпраўляць якое было вельмі цяжка, прытрымліваліся тэхналагічнай эканоміі, абумоўленай неабходнасцю.

Перш чым давяраць прыладзе, неабходна праверыць яго паводзіны з улікам загадзя вызначанага набору спецыфікацый. Функцыянал усё большай часткі сучаснага абсталявання рэалізуецца на праграмным узроўні. Гэтая тэндэнцыя аказвае адмоўны ўплыў на бяспеку будучых кампутарных сістэм.

Бяспека ў інжынерным асяроддзі

Актуальнасць даследавання сацыяльна-антрапалагічных асноў бяспекі тэхнікі абумоўлена неабходнасцю забеспячэння бяспекі чалавека ў тэхнічнай рэальнасці, паколькі тэхнічныя канструкцыі павінны функцыянаваць без пагрозы для жыцця і здароўя суб'екта тэхнічнай дзейнасці. Унутраная супярэчнасць бяспекі тэхнікі заключаецца ў адзінстве двух аспектаў: змест першага складае адсутнасць пагроз чалавеку з боку тэхнікі, другі аспект прадугледжвае адсутнасць пагроз для тэхнікі з боку чалавека.

У рамках першага аспекта асноўная ўвага надаецца тэхніка-тэхналагічным параметрам тэхнічных канструкцый, праектаванне, канструяванне і эксплуатацыя якіх не павінны наносіць шкоду чалавеку і адпавядаць яго біялагічным, псіхалагічным і сацыяльным характарыстыкам.

Другі аспект звязаны з аналізам прычын памылковых дзеянняў суб'екта тэхнічнай дзейнасці. Размова ідзе аб высвятленні меж безаварыйнага функцыянавання тэхнікі, аб магчымасці яе адпаведнасці, адэкватнасці структурным характарыстыкам суб'екта, які выступае сувязным звяном названых аспектаў. Таму праблема бяспекі тэхнікі ў філасофіі мяркуе даследаванне зместу чалавечага фактару, дэструктыўны ўплыў якога ў цяперашні час разглядаецца як пагроза існаванню не толькі тэхнічнага, але і іншых кампанентаў сацыяльнага быцця.

У тэхнагеннай рэальнасці людзі, ствараючы складаныя тэхнічныя канструкцыі, нярэдка забываюць аб абмежаванасці сваіх сацыяльных,

псіхалагічных і фізіялагічных магчымасцяў, увасобленых у створаныя імі ўзоры тэхнікі і якія накладаюць вызначаныя межы забеспячэнню іх бяспекі. Бяспека не можа быць бязмежнай, яна заўсёды існуе ў вызначанай прасторы чалавечых параметраў.

Рашэнне праблемы рацыянальнага спалучэння чалавека і тэхнікі натыкаецца на цэлы шэраг цяжкасцяў. Яшчэ М. Хайдэгер перасцерагаў, што да тэхнікі немагчыма ставіцца абыякава, як да інструмента, што ў тэхнікі ёсць свае прэтэнзіі да чалавека – да таго, якім ён павінен быць, каб найлепшым чынам адпавядаць яе патрабаванням.

Антрапалагічныя абмежаванні фармуюць чалавечы фактар бяспекі тэхнікі, дзеянне якога можа быць дэструктыўным у выпадку дэфармацыі яго асобных складнікаў, альбо пазітыўным у выпадку захавання антрапалагічнай меры бяспекі. Тры групы якасцяў, ігнараванне якіх выступае асновай узнікнення памылак ва ўзаемадзеянні чалавека і тэхнікі.

Фізіялагічныя адлюстроўваюць агульны фізічны стан чалавека.

Псіхалагічныя – асобасныя характарыстыкі чалавека, з асаблівасцямі яго псіхікі, псіхалагічнымі працэсамі, якія праходзяць у яго нервовай сістэме.

Эрганамічныя – абумоўленыя няўзгодненасцю характарыстык чалавека і машыннай часткі тэхнічнай сістэмы.

Штучны інтэлект і кібернетычная бяспека

Нейронная сетка (англ.: Neural network) – узаемазвязанае мноства штучных нейронаў, якія выконваюць простыя лагічныя аперацыі, якое валодае здольнасцю машыннага навучання

Машыннае навучанне (англ.: Machine learning, ML) – гэта тэхніка навучання інфармацыйнай сістэмы на аснове прадстаўленых набораў дадзеных (англ. dataset) без выкарыстання наканаваных правіл, з'яўляецца прыватным выпадкам штучнага інтэлекту.

Агульнай задачай машыннага навучання з'яўляецца пабудова алгарытму (праграмы) на падставе прадстаўленых уваходных дадзеных і

зададзеных дакладных/чаканых вынікаў – такім чынам, працэс працы ML-сістэмы падзелены на першапачатковае навучанне на якія прадстаўляюцца датасетах і на наступнае прыняцце рашэнняў ужо навучанай сістэмай.

Існуе некалькі спосабаў машыннага навучання, напрыклад:

Навучанне з настаўнікам (англ.: Supervised learning) – гэта спосаб машыннага навучання, у якім выкарыстоўваюцца размечаныя наборы дадзеных (праклаcіфікаваныя аб'екты з вылучанымі характэрнымі прыкметамі), для якіх нейкі "настаўнік" (чалавек або навучальная выбарка) паказвае правільныя пары "пытанне-адказ", на падставе чаго патрабуецца пабудаваць алгарытм прадастаўлення адказаў на далейшыя аналагічныя пытанні

Навучанне без настаўніка (англ. Unsupervised learning – гэта спосаб машыннага навучання, у якім не выкарыстоўваюцца размечаныя наборы дадзеных, не пазначаны правільныя пары "пытанне-адказ", а ад інфармацыйнай сістэмы патрабуецца на падставе вядомых уласцівасцяў аб'ектаў знайсці розныя ўзаемасувязі паміж імі

Навучанне з частковым прыцягненнем настаўніка (англ.: Semi-supervised learning) – спосаб машыннага навучання, у якім камбінуецца невялікая колькасць размечаных набораў дадзеных і вялікая колькасць неразмечаных. Такі падыход апраўданы тым, што атрыманне якасных размечаных дата-сэтаў з'яўляецца дастаткова рэсурсаёмістым і працяглым працэсам.

Навучанне з падмацаваннем (англ.: Reinforcement learning) – прыватны выпадак навучання з настаўнікам, пры якім «настаўнікам» з'яўляецца асяроддзе функцыянавання, якое дае зваротную сувязь інфармацыйнай сістэме ў залежнасці ад прынятых ёю рашэнняў.

Пры гэтым у машынным навучанні могуць выкарыстоўвацца і іншыя алгарытмы, такія як байесаўскія сеткі, ланцугі Маркава, градыентны бустынг.

Глыбокае навучанне (англ. Deep learning) – гэта прыватны выпадак машыннага навучання, у якім выкарыстоўваецца складаная шматслаёвая

штучная нейронавая сетка для эмуляцыі працы чалавечага мозгу і апрацоўкі гаворкі (англ. natural language processing), гукавых (англ. speech recognition) і візуальных вобразаў (англ. англ.: computer vision).

Машынны зрок (computer vision) у цяперашні час шырока выкарыстоўваюцца ў сістэмах забеспячэння бяспекі, кантролю транспарта і пасажыраў. Сістэмы апрацоўкі маўлення (natural language processing) і распазнання слоў (speech recognition) дапамагаюць галасавым асістэнтам Сіры ці Алісе адказваць на пытанні карыстальнікаў.

Вялікія дадзеныя (Big Data) – вялікі аб'ём структураваных і неструктураваных дадзеных у лічбавым выглядзе, які характарызуецца аб'ёмам (volume), хуткасцю змены (velocity) і разнастайнасцю (variety).

Для апрацоўкі Big Data могуць прымяняцца спецыялізаваныя праграмныя інструменты, такія як Apache Hadoop / Storm / Spark, Kaggle, СКБД класа NoSQL. Лічыцца, што для падвышэння business-value пры выкарыстанні Big Data патрабуецца перайсці ад разнастайных дадзеных да структураванай інфармацыі, а затым – да ведаў (звестак).

Апрацаваны, структураваны і размечаны dataset, атрыманы з рэлевантнага масіва Big Data, з'яўляецца неабходным (і адным з самых каштоўных) кампанентам для машыннага навучання ў сучасных сістэмах.

Глыбокі аналіз дадзеных (Data mining) – структураванне і вылучэнне карыснай інфармацыі з разнастайнай і неструктураванай масы дадзеных, у тым ліку з Big Data.

Невыразная логіка (англ.: Fuzzy logic) – ужыванне нястрогіх правіл і невыразных адказаў для рашэння задач у сістэмах штучнага інтэлекту і нейронавых сетках. Можа прымяняцца для мадэлявання паводзін чалавека, напрыклад, для звужэння або абмежавання ўмоў пошуку адказу на пытанне ў залежнасці ад кантэксту.

Разгледзеўшы асноўныя вызначэнні і прынцыпы, пяройдзем да пытання практычнага прымянення сістэм штучнага інтэлекту ў кібернетычнай бяспецы. Выкарыстанне штучнага інтэлекту ў інфармацыйнай

бяспецы абгрунтавана двума фактарамі: неабходнасцю аператыўнага рэагавання пры надыходзе кібернетычнага інцыдэнту і недахопам кваліфікаваных спецыялістаў па кібернетычнай абароне.

Калі ў кампаніі адсутнічае кругласутачная дзяжурная змена аналітыкаў інфармацыйнай бяспекі, то без сістэмы аператыўнага аўтаномнага рэагавання на кібернетычныя інцыдэнты будзе цяжка забяспечыць якасную абарону ў не працоўны час.

Хакеры перад нападам могуць выканаць які адцягвае манеўр – напрыклад, запусціць DDoS-напад або актыўнае сеткавае сканаванне, адцягваючы кібернетычных адмыслоўцаў. У такіх сітуацыях дапаможа сістэма рэагавання на кібернетычныя інцыдэнты на аснове штучнага інтэлекту, якая можа адначасова апрацоўваць вялікую колькасць падзей, аўтаматызаваць руцінныя дзеянні аналітыкаў і забяспечваць аператыўнае рэагаванне на інцыдэнты без удзелу чалавека.

Так, у рашэнні IRP / SOAR Security Vision выкарыстоўваюцца алгарытмы прэдыктыўнага рэагавання на кібернетычныя інцыдэнты: навучаная сістэма дазваляе спрагназаваць вектар атакі і яе наступнае развіццё ў інфраструктуры, паказаць тэндэнцыі, а затым аўтаматычна спыніць шкоднасныя дзеянні і даць парады аналітыкам.

Сістэмы абароны на аснове штучнага інтэлекту незаменныя для выяўлення анамалій шляхам аналізу часопісаў, даных з SIEM-сістэм або SOAR-рашэнняў. Гэтая інфармацыя з дадзенымі ўжо адпрацаваных і зачыненых інцыдэнтаў, будзе ўяўляць якасны размечаны dataset. Сістэме можна будзе лёгка навучыцца.

Класічныя сістэмы аналізу адхіленняў пабудаваны на некаторых загадзя зададзеных аператарамі правілах: напрыклад, перавышэнне аб'ёму спецыфічнага трафіку, пэўную колькасць няўдалых спроб аўтэнтыфікацыі, некаторая колькасць паслядоўных спрацоўванняў.

Дэтэктаванне анамалій можа дапамагчы ў абароне карыстацкіх дадзеных – напрыклад, банкаўскі інтэрнэт-сэрвіс можа збіраць і аналізаваць

дадзеныя аб патэрнах (характэрных прыкметах, шаблонах) працы кліентаў з тым, каб аператыўна выяўляць скампраметаваныя ўліковыя запісы. Фінансавыя арганізацыі могуць выкарыстоўваць сістэмы машыннага навучання і штучнага інтэлекту таксама для правядзення ацэнкі (скорынгу) пазычальнікаў, аналізу фінансавых рызык, у анты-фрод сістэмах.

Сістэмы абароны, абсталяваныя кампутарным зрокам і апрацоўкай гаворкі, змогуць аператыўна апавяшчаць ахову аб спробах праходу праз прахадную старонніх або супрацоўнікаў па чужых пропусках, аналізаваць працоўную актыўнасць супрацоўнікаў з дапамогай вэб-камер, ацэньваць карэктнасць зносін мэнэджараў з кліентамі па тэлефоне.

Сістэмы на базе штучнага інтэлекту выкарыстоўваюць і кібернетычныя злачынцы. Выкарыстоуваюцца ашуканскія прыёмы стварэння рэалістычнай віртуальнай выявы чалавека для падману анты-фрод сістэм. Таксама выкарыстоуваюцца падробкі галасоў для ашуканскіх званкоў сваякам атакаваных асоб з просьбай перавесці грошы.

Маюць месца ужыванні тэлефонных IVR-тэхналогій для фішынгу і крадзяжы грашовых сродкаў. Таксама выкарыстоўваюцца элементы штучнага інтэлекту, якія дазваляюць атакавалым значна хутчэй павялічваць свае прывілеі, перамяшчацца па карпаратыўнай сетцы, а затым знаходзіць і выкрадаць якія цікавяць іх дадзеныя.

Лічбавая ўстойлівасць

Лічбавая ўстойлівасць азначае выкарыстанне тэхналогій у паўсядзённых бізнес-дадатках для абароны навакольнага асяроддзя. Людзі ва ўсім свеце імкнуцца зменшыць шкоднае ўздзеянне лічбавых тэхналогій і ўстойлівага развіцця на навакольнае асяроддзе.

Для дасягнення лічбавай устойлівасці прадпрыемствы выкарыстоўваюць пашыраную аналітыку. Прадпрыемствы, якія ставяць сваёй мэтай лічбавую ўстойлівасць, могуць выкарыстоўваць лічбавыя

працэсы, прылады і мадэлі прагназавання, каб супаставіць магчымыя выгады з уздзеяннем на навакольнае асяроддзе ад іх дасягнення.

Гэтыя прадпрыемствы могуць імкнуцца звесці да мінімуму магчымае ўздзеянне сваёй дзейнасці на навакольнае асяроддзе, пры гэтым пастаўляючы спажыўцам карысныя тавары і паслугі. Лічбавая ўстойлівасць дазваляе арганізацыям выкарыстоўваць экалагічна бяспечныя тэхналогіі, не рызыкуючы сваёй прыбытковасцю.

Па меры таго як прадпрыемствы пераходзяць да наступнага пакалення інтэлектуальных лічбавых тэхналогій, якія кіруюцца дадзенымі, расце запатрабаванне ў разуменні ўсяго тэрміна службы тавараў і прыкладанняў з пункта гледжання іх уздзеяння на навакольнае асяроддзе і грамадства. Разгледзім прыклад распрацоўкі лічбавых прыкладанняў, такіх як прыкладанне для абмену файламі.

Кожны раз пры запуску кода дадатку для абмену файламі будуць адбывацца выкіды вугляроду. Базавае сховішча і інфраструктура таксама будуць садзейнічаць павелічэнню вугляроднага следу. Памер файла і спосаб, якім ён транспартуецца паміж геаграфічнымі рэгіёнамі і дастаўляецца праз шматлікія пераходы і сеткі, – усё гэта робіць свой унёсак у агульную суму.

Спосаб прадстаўлення інфармацыі на шматлікіх прыладах, а таксама тэхнічныя характарыстыкі абсталявання і UX/дызайн – усё гэта ўносіць свой уклад у вугляродны агрэгат. Усе гэтыя фактары патрабуюць пераасэнсавання працэсаў, тавараў і паслуг, а таксама больш комплекснага падыходу да распрацоўкі, прадастаўлення і кіравання ўстойлівымі лічбавымі рашэннямі.

Для дызайнера гэта будзе азначаць стварэнне аптымізаванага кода. Згодна з фундаментальнай пункту гледжання, гэта можа азначаць мадэрнізацыю інфраструктуры, выкарыстанне зялёнага аблокі або паспяховае выкарыстанне пераваг аблокі, такіх як выкарыстанне бессервернай інжынерыі.

Спосабы функцыянавання бізнесу мяняюцца ў выніку лічбавай устойлівасці. Прадпрыемствы становяцца ўсё больш экалагічна свядомымі,

прызнаючы ўплыў лічбавых аперацый на доўгатэрміновую экалагічную ўстойлівасць.

У той жа час прадпрыемствы пачынаюць усведамляць важнасць укладу ў навакольнае асяроддзе, што дае магчымасць распрацоўваць планы лічбавай устойлівасці, якія ўключаюць як спажывецкія, так і экалагічныя мэты.

Думкі кліентаў павінны ўважліва адсочвацца бізнэсам. Перавагі кліентаў часта ўплываюць на тое, як людзі марнуюць свае грошы. Калі кліенты шануюць абарону навакольнага асяроддзя, прадпрыемствы імкнуцца зрабіць устойлівасць грамадскім прыярытэтам. Апеляцыя да спажывецкага стаўлення мае на ўвазе паказчык таго, як фірма, клапоціцца аб тых жа пытаннях, што і спажыўцы.

Жаданне кампаніі зрабіць уражанне на кліентаў можа прывесці да таго, што яна зойме пэўную палітычную пазіцыю або падтрымае сацыяльную парадак дня.

Дзякуючы лічбавай устойлівасці кампаніі могуць адлюстроўваць жаданні кліентаў, не ставячы пад пагрозу сваю доўгатэрміновую прадукцыйнасць. Укараненне лічбавых рашэнняў, якія зніжаюць уздзеянне кампаніі на навакольнае асяроддзе, можа палепшыць яе доўгатэрміновыя далягляды.

Кампаніі па вытворчасці спажывецкіх тавараў часта належаць на сетцы паставак для распрацоўкі і распаўсюджвання сваіх тавараў сярод кліентаў. Кампаніі заўсёды аддавалі перавагу прадастаўляць тавары кліентам як мага хутчэй, нават калі гэтая хуткасць дасягаецца за кошт пагрозы навакольнаму асяроддзю.

Прадпрыемствы могуць выкарыстоўваць тэхналогіі для паляпшэння свайго ланцужка паставак, не аказваючы негатыўнага ўплыву як на мясцовыя, так і на нелакальныя экалагічныя ўмовы. Падвышаная аўтаматызацыя часта выкарыстоўваецца ў праектах лічбавай устойлівасці для ланцужкоў паставак.

Аўтаматызаваныя тэхналогіі могуць дапамагчы павысіць эфектыўнасць працэсаў, а таксама павялічыць хуткасць ланцужкі паставак і практычна выключыць чалавечы фактар. Прадпрыемствам, якія перамяшчаюць свае анлайн-базы дадзеных у воблака, таксама можа спатрэбіцца менш сервераў для дасягнення тых жа вынікаў, што прыводзіць да зніжэння выкідаў вугляроду.

Тая ж тактыка, якая дапамагае фірмам выпрацаваць дадатныя адносіны да навакольнага асяроддзя, можа таксама дапамагчы ім павялічыць сваю кліенцкую базу. У выніку кампаніі, якія выкарыстоўваюць метады лічбавай устойлівасці, могуць пашырыць свой уплыў.

Кампаніі таксама могуць выкарыстоўваць лічбавыя сістэмы ўстойлівага развіцця, каб дапамагчы выдаленаму персаналу ў іншых выпадках. Калі гэта магчыма, шматлікія кампаніі, якія дасягнулі поспеху ў кіраванні выдаленымі камандамі, выбіраюць віртуальныя сустрэчы над асабістымі сустрэчамі. Выдаленыя сустрэчы скарачаюць патрэбнасць у транспартных расходах і памяншаюць уздзеянне фізічнага транзіту на навакольнае асяроддзе.

Сапраўды гэтак жа кампутарызаваныя працоўныя месцы ўхіляюць неабходнасць у паперы, чарнілах, сашчэпках і іншых офісных матэрыялах, якія часта выкідваюцца пасля аднаразовага выкарыстання. Лічбавыя рэсурсы аказваюць непасрэдны дабратворны ўплыў на карпаратыўную дзейнасць: супрацоўнікі могуць адначасова працаваць над аднымі і тымі ж анлайн-рэсурсамі, абмен дадзенымі адбываецца імгненна, а ўнутрыкарпаратыўныя зносіны спрашчаюцца.

Дбайнае стаўленне да сваіх аперацый мае вырашальнае значэнне для таго, каб лічбавая ўстойлівасць працавала на кампанію. Фірмы актыўна інвестуюць у праграмнае забеспячэнне для выдаленага маніторынгу і кіравання, якое дазваляе ім адначасова падвысіць эфектыўнасць працы кампаніі і экалагічную ўстойлівасць за рахунак кансалідацыі IT-падтрымкі з пастаўшчыкамі кіраваных паслуг.

Гэтыя арганізацыі могуць падтрымліваць выдаленыя працоўныя сілы, адначасова кіруючы ІТ-задачамі супрацоўнікаў з дапамогай пашыранай аўтаматызацыі ІТ, сцэнараў і кіраванні выпраўленнямі, пазбаўляючы навакольнае асяроддзе ад наступстваў энергаспажывання на працоўным месцы.

У хатнім ці дзелавым кантэксце інтэлектуальныя электрычныя сеткі рэгулююць і мінімізуюць агульнае спажыванне энергіі. Тэхналогіі аналізу землекарыстання могуць дапамагчы абмежаваць высечку лясоў і пазбегнуць няправільнага выкарыстання зямлі. Удасканаленае мясцовае прагназаванне надвор'я прыводзіць да павышэння гадавой ураджайнасці сельскагаспадарчых культур;

Інтэлектуальныя метады перапрацоўкі памяншаюць колькасць адходаў на звалках, а таксама павялічваюць паўторнае выкарыстанне прадуктаў. Бескантактны ўваход уключае асвятляльныя і ацяпляльныя прыборы. Палепшанае кіраванне дарожным рухам і структуры парковак могуць дапамагчы звесці да мінімуму выкарыстанне выкапнёвага паліва, а таксама павысіць бяспеку дарожнага руху.

Сістэмны аналіз бяспекі

Сістэмны аналіз з'яўляецца важным інструментам для выяўлення і змякчэння пагроз бяспекі ў лічбавым ландшафце. Ужываючы структураваны і метадычны падыход да аналізу пагроз, спецыялісты па бяспецы лепш аснашчаны для выяўлення патэнцыйных уразлівасцей і распрацоўкі эфектыўных стратэгій па іх зніжэнню.

Адным з ключавых пераваг выкарыстання сістэмнага падыходу з'яўляецца тое, што ён дазваляе аналітыкам цэласна зірнуць на ландшафт бяспекі, улічваючы такія фактары, як бізнес-мэты арганізацыі, тэхналагічная інфраструктура і адпаведныя нарматыўныя патрабаванні. Такі комплексны

падыход дапамагае забяспечыць эфектыўнасць і доўгатэрміновую ўстойлівасць распрацаваных стратэгій па зніжэнні рызык.

Выкарыстоўваючы інструменты і метады, заснаваныя на дадзеных, такія як алгарытмы машыннага навучання і перадавыя аналітычныя платформы, аналітыкі могуць выяўляць заканамернасці і тэндэнцыі ў дзейнасці пагроз, якія могуць быць не відавочныя.

Гэта дазваляе прадбачыць і рэагаваць на ўзнікаючыя пагрозы да таго, як яны змогуць прычыніць шкоду. Уключыўшы сістэматычны аналіз у свае праграмы бяспекі, арганізацыі могуць больш эфектыўна кіраваць рызыкамі і абараняць свае крытычна важныя актывы.

Сістэмны аналіз патэнцыйных пагроз бяспекі ўключае ў сябе шэраг крокаў, накіраваных на выяўленне патэнцыйных рызык бяспекі, ацэнку іх уплыву і вызначэнне аптымальнага курса дзеянняў па іх зніжэнню. Важна сабраць усе неабходныя даныя і інфармацыю для поўнага разумення праблемы. Неабходна прааналізаваць сабраныя дадзеныя і інфармацыю, каб выявіць першапрычыну праблемы. Важна разгледзець усе магчымыя рашэнні, вызначыўшы іх плюсы і мінусы.

Важна ўлічваць такія фактары, як здзяйсняльнасць, кошт і патэнцыйны ўплыў кожнага рашэння. Далей ідзе ўкараненне выбранага рашэння, і маніторынг яго эфектыўнасці на працягу пэўнага часу. Прытрымліваючыся гэтых крокаў, арганізацыі могуць эфектыўна выкарыстоўваць сістэмны аналіз для выяўлення і прадухілення патэнцыйных пагроз бяспецы.

Аўдыт адпаведнасці ISO 27001 накіраваны на праверку палітык бяспекі арганізацыі. Ен прадпісвае выконваць правілы галіны, бо адсутнасць адпаведнасці можа прывесці да штрафаў і страты кліентаў. Многія кампаніі разглядаюць ISO як знак прэстыжу, бо гэта найбуйнейшы ў свеце набор прызнаных бізнес-прынцыпаў, а больш за мільён кампаній ва ўсім свеце маюць тую ці іншую форму сертыфікацыі ISO.

Стандарты ISO 27001 спецыяльна распрацаваны для абароны канфідэнцыйнай інфармацыі карыстальніка, а іх захаванне з'яўляецца

прыкладам аўдыту адпаведнасці. Але, выкарыстанне тэхналогіі (брандмаўэры, антывірусы і рэзервовыя копіі) не гарантуе поўнай абароны ад уцечак дадзеных і эксплуатацыйных праблем.

Гэта звязана з тым, як людзі выкарыстоўваюць гэтыя інструменты бяспекі, працэдуры і пратаколы. Стандарты ISO 27001 вырашаюць гэтую праблему, патрабуючы ўкараненні сістэм выяўлення рызык і прадухіленні інцыдэнтаў бяспекі.

Рызыка-арыентаваны падыход уяўляе сабой ацэнку рызык у дачыненні да інфармацыйнай бяспекі, заснаваную на аналізе пагроз і тэхнічных, прававых, фінансавых і арганізацыйных рызык. Пастаяннае паляпшэнне заключаецца ў абнаўленні, карэкціраванні і ўдасканаленні сістэмы ў адпаведнасці з зменлівымі ўмовамі ўнутры і па-за арганізацыяй. Цыкл PDCA прымяняецца для кіравання і дазваляе ацэньваць і паляпшаць сістэму ў адпаведнасці са стандартам ISO 27001.

Сістэмны аналіз бяспекі мяркуе разгляд усёй сістэмы, а не толькі асобных кампанентаў ці ўразлівасцяў. Такі падыход асабліва карысны пры выяўленні ўтоеных ці складаных рызык бяспекі, якія інакш не былі б выяўлены.

Каб выкарыстоўваць сістэмны аналіз у мэтах бяспекі, важна выканаць некалькі ключавых крокаў: вызначыць усе кампаненты сістэмы, ад апаратнага і праграмнага забеспячэння да чалавечых і культурных элементаў; ацаніць, як кампаненты сістэмы могуць быць скарыстаны хакерамі; вызначыць, як кампаненты сістэмы ўзаемадзейнічаюць сябар з сябрам і як пагрозы могуць распаўсюджвацца па ўсёй сістэме.

На аснове аналізу рызык і ўразлівасцяў можна распрацаваць стратэгіі змякчэння наступстваў і рашэнні, накіраваныя на ўхіленне праблем, выяўленых падчас аналізаў.

Сістэмны аналіз можа быць скарыстаны для аналізу баз дадзеных з мэтай выяўлення ўразлівасцяў і пагроз бяспекі. Напрыклад, для выяўлення SQL-ін'екцый можна правесці аналіз SQL-кода, які выкарыстоўваецца

дадаткам для доступу да базы дадзеных. Адзін з магчымых спосабаў апрацоўкі шкоднаснага SQL-кода:

Сістэмны аналіз можа дапамагчы ў выяўленні ўразлівасцяў у інфармацыйнай сістэме кампаніі. Для гэтага можна правесці аналіз архітэктуры сістэмы і яе кампанентаў. Напрыклад, можна праверыць, ці адпавядае сістэма стандартам бяспекі, такім як HIPAA ці PCI DSS.

HIPAA (Health Insurance Portability and Accountability Act) – гэта заканадаўчы акт, прыняты ў ЗША ў 1996 годзе, які рэгулюе апрацоўку, захоўванне і перадачу медыцынскіх дадзеных (Protected Health Information, PHI). HIPAA змяшчае стандарты бяспекі, якія абавязковыя для захавання ўсімі медыцынскімі арганізацыямі і кампаніямі, якія працуюць з медыцынскімі дадзенымі пацыентаў у ЗША.

Стандарты бяспекі HIPAA уключаюць патрабаванні да абароны прыватнасці, цэласнасці і даступнасці медыцынскіх дадзеных. Яны ахопліваюць наступныя вобласці:

- патрабаванні да абмежаванняў доступу да памяшканняў, дзе захоўваюцца медыцынскія дадзеныя, камеры відэаназірання, прылады кантролю доступу і іншае;
- патрабаванні да абароны медыцынскіх дадзеных у электронным выглядзе, уключаючы шыфраванне даных, кантроль доступу і аўдыт логаў;
- патрабаванні да дакументацыі працэдур апрацоўкі медыцынскіх даных, навучанню супрацоўнікаў і правядзенню аўдытаў.

Сістэмны аналіз можа быць ужыты для аналізу кода прыкладання і выяўлення патэнцыйных пагроз бяспецы. Напрыклад, пры апрацоўцы ўваходных дадзеных прыкладанне павінна праводзіць праверку на карэктнасць і адсякаць шкоднасны код.

Межы сістэмы могуць ахопліваць сістэму кіравання замовамі, сховішча кліенцкіх дадзеных і плацежныя шлюзы. Гэтыя складнікі сістэмы з'яўляюцца важнымі актывамі, важнымі для бяспекі.

Пасля выяўлення патэнцыйных пагроз неабходна вывучыць сістэму, каб вызначыць пэўныя ўразлівыя месцы. Напрыклад, неабароненыя кропкі доступу або састарэлыя пратаколы бяспекі могуць быць уразлівыя.

На апошнім этапе распрацоўваецца план па ўхіленні кожнай уразлівасці. Для зніжэння рызык могуць прымяняцца розныя меры бяспекі, уключаючы ўкараненне новых тэхналогій, абнаўлення пратаколаў бяспекі, навучанне персаналу перадавым метадам. Напрыклад, кампанія можа прыняць рашэнне ахоўваць дадзеныя двухфактарнай аўтэнтыфікацыяй або выкарыстоўваць лепшыя праграмныя рашэнні бяспекі.

Сістэмны аналіз дапамагае выявіць і ацаніць патэнцыйныя рызыкі кібернетычнай бяспекі, забяспечваючы разуменне, якое дазваляе прымаць рашэнні па ўмацаванні пратаколаў бяспекі.

Выкарыстанне сістэмнага аналізу дапамагае выявіць любыя патэнцыйныя парушэнні ў сістэме бяспекі. Сістэмны аналіз можа прымаць розныя формы, ад комплекснай адзнакі рызык бяспекі да фармальнай адзнакі праграмы бяспекі. Незалежна ад формы, выкарыстанне правільных інструментаў можа дапамагчы выявіць сістэматычныя слабыя месцы ў сістэме бяспекі, што гарантуе бяспеку арганізацыі.

Сістэма захопу парушэнняў бяспекі (SIEM) выкарыстоўваецца для збору і аналізу даных ад розных крыніц з мэтай выяўлення пагроз бяспекі. SIEM можа выкарыстоўвацца для выяўлення шкоднасных дзеянняў, нападаў на сетку і парушэнні палітык бяспекі. Прыкладам можа быць праграмнае забеспячэнне Tripwire, Nagios, SolarWinds і AlienVault.

CISM праграмнае забеспячэнне выкарыстоўваецца для ацэнкі пагроз бяспекі, выяўлення ўразлівых месцаў, фарміравання планаў кіравання рызыкамі, а таксама для ўхілення ўразлівасцяў. Прыклады праграмнага забеспячэння CISM могуць быць SecurityMetrics, IBM QRadar і Symantec Control Compliance Suite.

Аўдыт бяспекі выкарыстоўваецца для выяўлення пагроз і адзнакі рызык, а таксама для забеспячэння адпаведнасці правілам і палітыкам

бяспекі. Прыклады праграмнага забеспячэння для аўдыту бяспекі могуць быць Qualys, Nessus і OpenVAS. Праверка бяспекі вэб-прыкладанняў на наяўнасць уразлівасцяў ажыццяўляецца прыладамі OWASP ZAP, Acunetix і Burp Suite. Маніторынг доступу карыстальніка можа быць рэалізаваны з дапамогай Active Directory, LogRhythm, Splunk і Netwrix.

Індыкатары кампраметацыі выкарыстоўваюцца для выяўлення прысутнасці хакераў у сетцы. Індыкатары кампраметацыі дапамагаюць выявіць наяўнасць шкоднасных праграм і іншых анамальных актыўнасцяў у сетцы. Прыкладамі індыкатараў кампраметацыі могуць быць McAfee Threat Intelligence Exchange, IBM QRadar і Cisco Stealthwatch.

Дадзеныя карыстальнікаў, уключаючы інфармацыю аб уваходзе, адрас электроннай пошты, URL-адрасах канферэнцый і ключах хастоў, могуць выкарыстоўвацца злачынцамі для доступу да канферэнцый і для іншых ашуканскіх дзеянняў.

Кампраметацыя дадзеных можа прывесці да юрыдычных пазоваў ад супрацоўнікаў і штрафаў ад якія рэгулююць органаў у большасці краін. Каб прадухіліць падобныя выпадкі ў будучыні, арганізацыям неабходна праводзіць шырокія праграмы інфармацыйнай бяспекі, а таксама рэгулярна навучаць супрацоўнікаў правілам працы ў анлайн-асяроддзі.

Аўдыт бяспекі і сістэмны аналіз могуць дапамагчы арганізацыям вызначыць уразлівасці і палепшыць меры бяспекі, што дапаможа прадухіліць будучыя парушэнні бяспекі і захаваць асабістыя дадзеныя кліентаў.

Кампутарны вірус

Кампутарны вірус – гэта праграма, здольная ствараць свае копіі. Яна ўкараняе іх у рэсурсы камп'ютарных сістэм, сетак. Таксама яна робіць дзеянні без удзелу карыстальніка.

Вірус заражае іншыя праграмы, а таксама выконвае запланаваныя дэструктыўныя дзеянні. Для маскіроўкі вірус актывізуецца не заўсёды, а

толькі пры выкананні пэўных умоў (час, дзеянне). Падобна сапраўдным вірусам, кампутарныя вірусы хаваюцца, размнажаюцца.

Вірусы выконваюць розныя дэструктыўныя дзеянні. Яны выводзяць на экран якія замінаюць тэкставыя паведамленні; ствараюць гукавыя эфекты; ствараюць відэа эфекты. Яны запавольваюць працу кампутара, паступова памяншаюць аб'ём аператыўнай памяці і павялічваюць знос абсталявання; выклікаюць адмову асобных прылад, завісанне ці перазагрузку кампутара.

Яны імітуюць паўтаральныя памылкі працы аперацыйнай сістэмы; знішчаюць FAT-табліцу, фарматуюць цвёрдую кружэлку, сціраюць BIOS, сціраюць або змяняюць усталёўкі ў CMOS, сціраюць сектары на дыску, знішчаюць або скажаюць дадзеныя, сціраюць антывірусныя праграмы.

Яны ажыццяўляюць навуковы, тэхнічны, прамысловы і фінансавы шпіянаж; выводзяць з ладу сістэмы абароны інфармацыі, даюць хакерам таемны доступ да вылічальнай машыны.

Яны робяць незаконныя адлічэнні з кожнай фінансавай аперацыі.

Галоўная небяспека самаўзнаўляльных кодаў складаецца ў тым, што праграмы-вірусы пачынаюць жыць уласным жыццём, практычна не якая залежыць ад распрацоўніка праграмы. Асноўныя сімптомы віруснага заражэння кампутара наступныя:

- запаволенне працы некаторых праграм; павелічэнне памераў файлаў;
- з'яўленне не існавалых раней файлаў;
- памяншэнне аб'ёму даступнай аператыўнай памяці;
- з'яўленне збояў у рабоце аперацыйнай сістэмы;
- запіс інфармацыі на дыскі ў моманты, калі гэтага не павінна адбывацца.

Згодна з класіфікацыяй вірусаў вылучаюць

- сеткавыя вірусы, якія распаўсюджваюцца рознымі кампутарнымі сеткамі;
- файлавыя вірусы інфікуюць выкананыя файлы, якія маюць пашырэнне exe і com.

Да гэтага ж класу ставяцца макравірусы, напісаныя з дапамогай макракаманд. Яны заражаюць невыканальныя файлы ў Word і Excel.

Загрузачныя вірусы ўкараняюцца ў загрузны сектар дыска або ў сектар, які змяшчае праграму загрузкі сістэмнага дыска. Некаторыя вірусы запісваюцца ў вольныя сектары дыска, пазначаючы іх у FAT-табліцы як дрэнныя. Загрузачна-файлавыя вірусы інтэгруюць рысы апошніх двух груп.

Рэзідэнтны вірус можна падзяліць на дзве часткі – усталёўнік і рэзідэнтны модуль. Не рэзідэнтныя вірусы не заражаюць аператыўную памяць і праяўляюць сваю актыўнасць толькі аднаразова пры запуску інфікаванай праграмы.

Не небяспечныя вірусы ствараюць гукавыя і відэаэфекты. Небяспечныя вірусы знішчаюць частку файлаў на дыску. Вельмі небяспечныя вірусы самастойна фарматуюць цвёрдую кружэлку.

Кампаньён – вірусы не змяняюць файлы. Яны ствараюць для exe-файлаў новыя файлы-спадарожнікі (дублікаты), якія маюць тое ж імя, але з пашырэннем com. Com-файл выяўляецца першым, а затым вірус запускае exe-файл.

Паразітычныя вірусы пры распаўсюджванні сваіх копій абавязкова змяняюць змесціва дыскавых сектараў ці файлаў. Да іх адносяцца ўсе вірусы акрамя кампаньёнаў і чарвякоў.

Чарвякі (рэплікатары) аналагічна кампаньёнам не змяняюць файлы і сектары дыска. Яны пранікаюць у кампутар па сетцы, вылічаюць сеткавыя адрасы іншых кампутараў і рассылаюць па гэтых адрасах свае копіі.

Чарвякі памяншаюць прапускную здольнасць сеткі, запавольваюць працу сервераў. Невідзімкі (стэлс) выкарыстоўваюць набор сродкаў маскіроўкі сваёй прысутнасці ў кампутары. Іх цяжка выявіць. Яны перахапляюць звароты аперацыйнай сістэмы да здзіўленых файлаў ці сектарам і падстаўляюць незаражаныя ўчасткі файлаў.

Паліморфікі (здані, мутанты) шыфруюць уласнае цела рознымі спосабамі. Іх цяжка выявіць. Іх копіі практычна не ўтрымоўваюць цалкам

супадаючых участкаў кода. Траянская праграма маскіруецца пад карысную ці цікавую праграму, выконваючы падчас свайго функцыянавання яшчэ і разбуральную працу. Яна збірае на камп'ютары інфармацыю, якая не падлягае разгалашэнню. У адрозненне ад вірусаў, траянскія праграмы не валодаюць уласцівасцю самастойнага ўзнаўлення.

Вірусная праграма можа функцыянаваць як адзіны блок. Яна можа быць таксама падзелена на часткі. Гэтыя часткі змяшчаюць інструкцыі, якія паказваюць, як сабраць іх разам, каб узнавіць вірус.

Для барацьбы з вірусамі распрацоўваюцца антывірусныя праграмы. гэта праграмны прадукт ці прылада, якое выконвае адну, альбо некалькі з наступных функцый:

1) абарону дадзеных ад разбурэння;

2) выяўленне вірусаў;

3) нейтралізацыю вірусаў.

Праграмы-дэтэктары разлічаны на выяўленне канкрэтных, загадзя вядомых праграме вірусаў і заснаваныя на параўнанні характэрнай паслядоўнасці байтаў (сігнатур), якія змяшчаюцца ў целе віруса, з байтамі правяраемых праграм. Праграмы-дэтэктары забяспечваюцца блокамі эўрыстычнага аналізу. У гэтым рэжыме робіцца спроба выявіць новыя ці невядомыя вірусы па характэрным для ўсіх вірусаў кодавым паслядоўнасцям.

Праграмы-дэзінфектары (фагі) не толькі знаходзяць заражаныя файлы, але і лечаць іх, выдаляючы з файла цела праграмы-віруса. Праграмы-рэвізоры аналізуюць бягучы стан файлаў і сістэмных абласцей дыска і параўноўваюць яго з інфармацыяй, захаванай раней у адным з файлаў рэвізара. Правяраецца стан загрузнага сектара, FAT-табліцы, а таксама даўжыня файлаў, іх час стварэння, атрыбуты, кантрольныя сумы.

Праграмы-фільтры (маніторы) апавяшчаюць карыстальніка аб усіх спробах якой-небудзь праграмы выканаць падазроныя дзеянні. Фільтры кантралююць абнаўленне праграмных файлаў і сістэмнай вобласці дыска, фарматаванне дыска.

Пры працы ў сетцы абавязкова павінна быць усталявана праграма-фільтр. Перад счытваннем з дыскет інфармацыі, запісанай на іншых кампутарах, варта заўсёды правяраць гэтыя дыскеты на наяўнасць вірусаў. Пры пераносе файлаў у архіваваным выглядзе неабходна іх правяраць адразу ж пасля разархівацыі.

Пры працы на іншых кампутарах неабходна абараняць свае дыскеты ад запісу. Рабіць архіўныя копіі каштоўнай інфармацыі на іншых носьбітах. Не пакідаць дыскету ў дыскавод пры ўключэнні або перазагрузцы кампутара, гэта можа прывесці да заражэння загрузнымі вірусамі.

Атрымаўшы электронны ліст, да якога прыкладзены выкананы файл, не варта запускаць гэты файл без папярэдняй праверкі. Неабходна мець аварыйную загрузную дыскету, з якой можна будзе загрузіцца, калі сістэма адмовіцца зрабіць гэта звычайнай выявай.

Вызначэнне воблачнай бяспекі

Воблачная бяспека – гэта набор палітык, сродкаў кантролю і тэхналогій для абароны дадзеных, прыкладанняў і інфраструктурных сэрвісаў. Усе гэтыя кампаненты працуюць разам, дапамагаючы забяспечыць бяспеку даных, інфраструктуры і прыкладанняў. Гэтыя меры бяспекі абараняюць асяроддзе воблачных вылічэнняў ад знешніх і ўнутраных пагроз і ўразлівасцяў кібернетычнай бяспекі.

Шырокае ўкараненне стварае новыя магчымасці для здзяйснення кібернетычнага махлярства кібернетычнымі злачынцамі. Паколькі гэтыя арганізацыі пераходзяць да лічбавай трансфармацыі сваёй дзейнасці вельмі хутка, думаць пра эфектыўныя сродкі кантролю бяспекі часта не застаецца часу. Часта прадпрыемствы адмаўляюцца ад ужывання праверaных практычных рэкамендацый, што абцяжарвае (ці нават робіць немагчымым) дакладную адзнаку рызык і кіраванне імі.

Па меры таго як прадпрыемствы адаптуюцца да пастаянных змен і актыўна пераходзяць на хмарныя тэхналогіі, узнікае патрэбнасць аб'яднання разрозненых поглядаў і праграм дзеянняў у цэласную стратэгію.

Арганізацыям, якія разглядаюць пераход да воблака як магчымасць актыўна культываваць стратэгію "бяспека вышэй за ўсё", давядзецца балансаваць паміж забеспячэннем магчымасці выкарыстання воблачных сэрвісаў і абаронай канфідэнцыйных транзакцый і дадзеных.

Перавагі хмарнай бяспекі мяркуюць выкарыстанне штучнага інтэлекту (AI) і машыннага навучання (ML) для аўтаматычнай адаптацыі да пагроз бяспекі і іх ухілення; выкарыстанне аўтаномных магчымасцяў для маштабавання рэагавання, нейтралізацыі рызык і ўхіленні памылак у сферы бяспекі.

Воблачная бяспека дае арганізацыям падыход да вырашэння праблем бяспекі і забяспечвае выкананне нарматыўных патрабаванняў.

Эфектыўнае забеспячэнне бяспекі аблокі патрабуе наяўнасці некалькіх узроўняў абароны ў рамках стэка хмарных тэхналогій, у які ўваходзяць:

сродкі прэвентыўнага кантролю, прызначаныя для блакавання аўтарызаванага доступу да канфідэнцыйных сістэм і дадзеных;

дэтэктыўнага кантролю, прызначаныя для выяўлення несанкцыянаванага доступу да сістэм і даных і іх змяненняў з дапамогай правядзення аўдыту, маніторынгу і справаздачнасці;

аўтаматычнага кантролю, прызначаныя для прадухілення, выяўлення і рэагавання на абнаўленні бяспекі, як рэгулярныя, так і крытычна важныя;

адміністрацыйнага кантролю, распрацаваныя для кантролю за прымяненнем палітык, стандартаў, практык і працэдур бяспекі.

Машыннае навучанне і штучны інтэлект дазваляюць дапоўніць партфель сістэм воблачнай бяспекі тэхналогіямі кантэкстнай дасведчанасці. Воблачная бяспека дазваляе прадпрыемствам абараняць IaaS, PaaS і SaaS, распаўсюджваючы абарону на сеткавы, апаратны, аперацыйны, прыкладной узроўні, узровень крышталяў і ўзровень захоўвання дадзеных.

Воблачнае бяспеку аблокі – гэта агульная адказнасць правайдэра аблокі і кліента за бяспеку. Мадэль агульнай адказнасці за бяспеку ў воблаку – гэта базавая канструкцыя для кіравання бяспекай і рызыкамі ў воблаку, якая дазваляе падзяліць абавязкі паміж пастаўшчыком воблачных сэрвісаў і абанентам. Дакладнае разуменне мадэлі агульнай адказнасці за бяспеку для ўсіх тыпаў воблачных сэрвісаў мае вырашальнае значэнне для праграм воблачнай бяспекі.

Нажаль, можна таксама сказаць, што мадэль агульнай адказнасці за бяспеку з'яўляецца адной з найменш зразумелых канцэпцый бяспекі ў воблаку. На самай справе, калі параўноўваць з пастаўшчыком воблачных паслуг (CSP), толькі 8% CISO цалкам разумеюць сваю ролю ў забеспячэнні бяспекі SaaS.

Мадэль агульнай адказнасці за бяспеку вызначае зону адказнасці пастаўшчыка хмарных паслуг па забеспячэнні бяспекі і даступнасці паслугі, а таксама зону адказнасці кліента за забеспячэнне бяспечнага карыстання паслугай, дзе кожнаму адводзяцца свае пэўныя абавязкі.

Няздольнасць адэкватна абараніць дадзеныя можа прывесці да сур'ёзных і дарагіх наступстваў. Многія арганізацыі, якія сутыкнуцца з наступствамі ўзлому, могуць аказацца не ў стане пакрыць выдаткі, нават буйныя кампаніі могуць адчуць наступствы для сваіх фінансавых паказчыкаў. Сэнс мадэлі агульнай адказнасці за бяспеку заключаецца ў забеспячэнні гнуткасці з дапамогай убудаваных сродкаў абароны, якія дазваляюць хутка разгортваць сістэму. Таму арганізацыі павінны разумець свае абавязкі па забеспячэнні бяспекі ў воблаку: звычайна гэта завуць бяспекай "з" аблокі і бяспекай "у" воблаку.

Прадпрыемствам прапануецца шырокі спектр сродкаў абароны воблачных асяроддзяў для забеспячэння бяспекі пры пераносе працоўных нагрузак і дадзеных у воблака.

Аднак некаторыя з гэтых інструментаў пастаўляюцца з індывідуальнымі інструкцыямі і прапануюцца як асобныя паслугі.

Карыстальнікі і адміністратары воблачных рашэнняў павінны ведаць, як працуюць сэрвісы хмарнай бяспекі, як іх правільна наладзіць і як падтрымліваць разгорнутыя хмарныя рашэнні. Хоць сёння няма недахопу ў розных сістэмах забеспячэння бяспекі, іх можа быць складана наладжваць і можна лёгка дапусціць памылку ў адной вобласці.

Пастаянны рызыка фішынгу і шкоднасных праграм, якое расце кібернетычнае махлярства і цэлы шэраг няправільна сканфігураваных хмарных сэрвісаў аказваюць яшчэ большы ціск на праграмы кібернетычнай бяспекі, якія вырашаюць складаныя задачы. У выніку арганізацыі сутыкаюцца з уцечкай дадзеных, а гэта цягне за сабой шкоду брэнду, выдаткі на аднаўленне і штрафы.

Давер мае першараднае значэнне пры выбары партнёра па воблаку, які будзе адказваць за сваю частку мадэлі агульнай бяспекі. Арганізацыі павінны дакладна разумець свае ролі і абавязкі, а таксама мець доступ да незалежных іншых аўдытаў і атэстацыяў сістэм бяспекі.

Для складаных пагроз патрабуюцца новыя сучасныя рашэнні бяспекі, якія здольныя прагназаваць, прадухіляць, выяўляць пагрозы і рэагаваць на іх з дапамогай машыннага навучання.

Шматузроўневая сістэма бяспекі па ўсім тэхналагічным стэку павінна ўключаць сродкі прэвентыўнага, дэтэктыўнага і адміністрацыйнага кантролю адпаведнымі людзьмі, працэсамі і тэхналогіямі для забеспячэння бяспекі цэнтраў апрацоўкі гэтых хмарных паслуг.

Па меры таго як мабільныя прылады, прыкладанні і звесткі аб карыстачах выкарыстоўваюцца ўсё шырэй, уліковыя запісы становяцца новым перыметрам. Найважнейшае значэнне мае кантроль доступу і прывілеяў у воблаку і лакальных сістэмах.

Брокер абароны доступу ў воблака і рашэнне для кіравання сродкамі забеспячэння бяспекі ў воблаку павялічваюць празрыстасць і кантроль над усім хмарным асяроддзем арганізацыі.

Пастаўшчык воблачных паслуг павінен актываваць сродкі кантролю бяспекі па змаўчанні, а не патрабаваць ад прадпрыемства памятаць аб тым, што іх трэба ўключаць. Не ўсе маюць дакладнае ўяўленне аб розных сродках кіравання бяспекай і аб тым, як яны працуюць разам для зніжэння рызыкі і стварэння паўнавартаснай сістэмы бяспекі. Напрыклад, шыфраванне дадзеных павінна быць уключана па змаўчанні. У аблоках павінны прымяняцца ўзгодненыя сродкі кантролю і палітыкі абароны дадзеных.

Для забеспячэння бяспекі працоўных нагрузак адміністратарам палітык бяспекі варта наладзіць і забяспечыць захаванне палітык бяспекі для хмарных карыстальнікаў і секцый. Уніфікаванае прадстаўленне ўсіх сродкаў кантролю хмарнай бяспекі па ўсіх карыстальнікам аблокі таксама неабходна для выяўлення памылак канфігурацыі рэсурсаў і небяспечных дзеянняў па ўсіх карыстальнікам, што дае адміністратарам бяспекі магчымасць адсочваць і вырашаць праблемы бяспекі аблокі.

Прынцыпы падзелу абавязкаў і доступу з мінімальнымі прывілеямі – гэта практычныя рэкамендацыі па бяспецы, якія варта ўжываць у воблачных асяроддзях. Гэта гарантуе, што асобныя асобы не будуць валодаць празмернымі адміністрацыйнымі правамі і не змогуць атрымаць доступ да канфідэнцыйных звестак без дадатковай аўтарызацыі.

Паколькі ўкараненне хмарных асяроддзяў працягвае паскарацца як вынік прыярытэтных мэт лічбавай трансфармацыі, кампаніі павінны прадбачыць складанасці забеспячэння бяспекі сваіх воблачных асяроддзяў і ўмець разбірацца ў іх. Вельмі важна абраць пастаўшчыка хмарны паслуг, які зможа распрацаваць сістэму бяспекі, аўтаматычна ўбудаваную ва ўвесь стэк воблачных тэхналогій (IaaS, PaaS, SaaS).

Пры разглядзе перспектыў развіцця воблачнай бяспекі актуальная бяспека воблачнай інфраструктуры: абарона працоўных нагрузак з ужываннем падыходу «бяспека вышэй за ўсё», арыентаванага на бяспеку вылічэнняў, сетак і сістэм захоўвання хмарнай інфраструктуры, пачынальна з

яе архітэктуры. Прымяненне асноўных службаў бяспекі для забеспячэння неабходнага ўзроўню бяспекі найважнейшых бізнес-нагрузак.

Воблачная бяспека баз дадзеных мяркуе памяншэнне рызыкі ўцечкі дадзеных і паскарэнне захавання нарматыўных патрабаванняў у воблаку. Укараненне рашэнняў па забеспячэнні бяспекі баз дадзеных, якія ўключаюць шыфраванне, кіраванне ключамі, маскіраванне дадзеных, кантроль доступу прывілеяваных карыстальнікаў, маніторынг актыўнасці і аўдыт.

Бяспека хмарных прыкладанняў разглядаецца як абарона крытычна важных прыкладанняў ад махлярства і неправамернага выкарыстання абсалютна неабходная для абароны важных бізнес-дадзеных кампаніі. Дэталёвы кантроль доступу, празрыстасць і маніторынг з'яўляюцца ключавымі кампанентамі сучаснай шматузроўневай абароны.

Карпаратыўная бяспека і канфідэнцыяльнасць трактуецца як абарона канфідэнцыяльнасці, цэласнасці і даступнасці дадзеных і сістэм, размешчаных у воблаку, незалежна ад абранага воблачнага прадукта. Пры пераходзе да хмарных воблачных і мульцівоблачным асяроддзям расце паверхня нападу.

Для вырашэння гэтых праблем выкарыстоўваюцца перадавыя сэрвісы ад пастаўшчыка хмарных паслуг для кантролю доступу да дадзеных, тыпу доступу да канкрэтных рэсурсаў, выкарыстоўваючы абароненыя ўліковыя дадзеныя, незалежна ад таго, размешчаны яны ў воблаку ці лакальна.

Мэнэджмент бяспекі

У агульным вызначэнні пад бяспекай разумеецца стан абароненасці аб'екта ад шкодных уздзеянняў навакольнага ці ўнутранага асяроддзя. Мэнэджмент бяспекі бярэ на сябе функцыю праверкі і рэгуляванні захавання правіл бяспечнай працы кампаніі як вытворчага кірунку, так і сферы паслуг.

Распрацоўка і ўкараненне гэтай канцэпцыі праводзяцца спецыялістамі, якія маюць высокую кваліфікацыю ў прадстаўленых пытаннях, што дае

магчымасць правільна скласці і ў далейшым выконваць прадпісанні правіл бяспекі прадпрыемства на выбраным рынку.

Пад мэнэджментам бяспекі прадпрыемствы разумеюць скаардынаваны і сістэматызаваны набор дзеянняў і метадаў, накіраваных на аптымальнае кіраванне рызыкамі і звязанымі з імі патэнцыйнымі пагрозамі і іншымі ўздзеяннямі. Дасягненне гэтай канцэпцыі ва ўмовах сучаснай кампаніі магчыма толькі з дакладнай пастаноўкай канкрэтных задач. Распрацоўка правіл бяспекі павінна ажыццяўляцца таксама кваліфікаванымі спецыялістамі і адказнымі прадстаўнікамі кампаніі.

Мэтай менеджменту бяспекі з'яўляецца забеспячэнне няўхільнага захавання прадпісаных правіл і рэкамендацый супрацоўнікамі кампаніі. У гэтым выпадку дасягаецца высокая ступень бяспекі тэхнічных аперацый (вытворчасць гатовай прадукцыі і падаванне паслуг); камерцыйных аперацый (купля, продаж і аб'ём); фінансавых аперацый (прыцягненне фінансаў і далейшае распараджэнне імі).

Таксама дасягаецца высокая ступень страхавых аперацый (страхаванне, ахова жыцця і здароўя персанала і маёмасці кампаніі); уліковых аперацый (бухгалтэрыя, улік, статыстыка і калькуляцыя). Падобны ўзровень забяспечваецца для адміністрацыйных аперацый (прадбачанне, арганізацыя, кантроль і каардынаванне).

Кожная з гэтых аперацый можа служыць крыніцай небяспекі, як з прычыны няправільнага яе выканання, так і ў якасці шляху пранікнення ў структуру арганізацыі хакераў.

Пагрозы, якія разглядаюцца канцэпцыяй менеджменту бяспекі ўнутры кампаніі, класіфікуюцца як часовыя ці пастаянныя, а таксама знешнія ці ўнутраныя. Тэорыя бяспекі выдзяляе пагрозы, звязаныя з канкурэнцыяй, чалавечым фактарам, злачыннасцю, тэхнагеннымі і прыроднымі фактарамі.

У прадпрымальніцкай дзейнасці асноўныя віды пагроз падзяляюцца на фізічныя і эканамічныя пагрозы. Кожная з іх драбніцца таксама на падвіды, якія разглядаюцца па асобнасці ў кожным выпадку.

Найболей значнымі функцыямі сістэмы бяспекі з'яўляюцца выяўленне рэальных і прагназаванне патэнцыйных пагроз;

прымяненне спосабаў іх устаранення, а таксама ліквідацыя наступстваў; падбор сродкаў і інструментаў, накіраваных на паляпшэнне сістэмы бяспекі прадпрыемства; стварэнне і забеспячэнне для супрацоўнікаў прадпрыемства абароненага асяроддзя, якое дае магчымасць бяспечна выконваць ускладзеныя на іх абавязкі.

Павінна быць дакладна прапрацавана стратэгія бяспекі, якая дае магчымасць выконваць самыя важныя задачы кампаніі ў плане стварэння і забеспячэння бяспечнага і канкурэнтаздольнага асяроддзя ўнутры арганізацыі. Дзякуючы гэтаму кожны супрацоўнік можа бяспечна і эфектыўна праяўляць свае прафесійныя здольнасці і паднімацца па кар'ернай лесвіцы.

У структуры павінны быць дакладна прапісаны суб'екты і аб'екты сістэмы бяспекі. Яны ўяўляюць сабой узаемазвязаныя элементы, аб'яднаныя ў сістэму, якая забяспечвае бяспечнае асяроддзе для дзейнасці прадпрыемства. Аб'ектамі сістэмы з'яўляюцца элементы, на якія накіраваны ўсе намаганні па забеспячэнні бяспекі.

Да такіх адносяцца адміністрацыйныя службы, аддзелы забеспячэння, вытворчы сектар і камерцыйныя аддзелы. Суб'екты – гэта адказныя аддзелы прадпрыемства, якія непасрэдна займаюцца стварэннем і мадэрнізацыяй сістэмы бяспекі.

Сістэма менеджменту інфармацыйнай бяспекі – частка агульнай сістэмы менеджменту, заснаваная на выкарыстанні метадаў ацэнкі бізнес-рызыкоў для распрацоўкі, укаранення, функцыянавання, маніторынгу, аналізу, падтрымкі і паляпшэння інфармацыйнай бяспекі.

СМІБ уключае ў сябе арганізацыйную структуру, палітыкі, дзейнасць па планаванні, размеркаванне адказнасці, практычную дзейнасць, працэдуры, працэсы і рэсурсы.

Стандарт устанаўлівае патрабаванні інфармацыйнай бяспекі бізнес-рызыкаў арганізацыі. Стандарт устанаўлівае патрабаванні па ўкараненню мер кіравання інфармацыйнай бяспекай і яе кантролю, якія могуць быць выкарыстаны арганізацыямі або іх падраздзяленнямі ў адпаведнасці з установленымі мэтамі і задачамі забеспячэння інфармацыйнай бяспекі.

У выніку дасягаецца:

- абарона інфармацыйных актываў і гарантыя даверу зацікаўленых бакоў;
- забеспячэнне магчымасці санкцыянаванага своечасовага атрымання дакладнай і поўнай інфармацыі;
- задавальненне патрабаванняў бяспекі кліентаў і іншых зацікаўленых асоб;
- паляпшэнне планаў і дзеянні арганізацыі;
- адпаведнасць мэтам інфармацыйнай бяспекі арганізацыі;
- інтэграцыя з адпаведнымі патрабаваннямі іншых сістэм менеджменту;
- аблягчэнне бесперапыннага ўдасканалення і рэгулявання бягучых арганізацыйных мэт і знешніх умоў;
- разуменне патрабаванняў інфармацыйнай бяспекі арганізацыі і неабходнасці ўстанаўлення палітыкі і мэт інфармацыйнай бяспекі;
- укараненне і выкарыстанне мер кіравання для менеджменту рызык бізнес-рызыкоў арганізацыі;
- павышэнне гарантый таго, што інфармацыйныя актывы ў дастатковай меры на бесперапыннай аснове абаронены ад пагроз інфармацыйнай бяспекі.

Этычны эгаізм

Этычны эгаізм – уяўленне аб перасследзе ўласных інтарэсаў, а таксама аб поўным выключэнні абавязкаў абароны кімсьці нечых інтарэсаў. Гаворка ідзе аб нарматыўнай (прадпісальнай) тэорыі, якая тычыцца моманту паводзін

чалавека. Этычны эгаізм істотна адрозніваецца ад тэорыі псіхалагічнага эгаізму, дзе адзначаецца, што любыя дзеянні людзей, у выніку, пераследуюць карысць.

Аргументы падтрымкі этычнага эгаізму заснаваныя на тым, што любы, хто адданы ўласным інтарэсам, удзельнічае ў прасоўванні агульнага дабра. Вынік дасягаецца дзякуючы выступленням людзей у якасці найлепшых суддзяў у сваіх інтарэсах. У людзей значна больш матывацыі да таго, каб старанна працаваць для сябе, чым дзеля дасягнення іншых вынікаў. Аднак існуе відавочнае пярэчанне, што аргумент не падтрымлівае этычны эгаізм.

Важнай мэтай указваецца дабрабыт грамадства. Пры гэтым сцвярджаецца, што аптымальны спосаб дасягнення такой мэты – клопат кожнага аб самім сабе. Але калі атрымаецца давесці, што такое стаўленне не спрыяе агульнаму дабру, аўтары аргумента, хутчэй за ўсё, перастануць абараняць эгаізм. Іншае пярэчанне складаецца ў не заўсёды дакладных сцвярджэннях аргументу.

Этычны эгаізм не здольны прапанаваць рашэнні, калі ўзнікае праблема, звязаная з канфліктам інтарэсаў. Этычны эгаізм выключае любыя спробы заставацца бесстароннімі. Людзям застаецца адрозніваць сябе і ўсіх астатніх людзей і даваць сабе прэферэнцыйны рэжым.

Многія ўспрымаюць гэта супярэчнасьцю самой сутнасьці маралі. Залатое правіла розных версій абвяшчае: людзям варта ставіцца сябар да сябра, абапіраючыся на ўласныя пажаданні ў адносінах.

Ананімнасць у сацыяльных сетках

Многім людзям хочацца дабіцца ананімнасці ў інтэрнэце. Ёсць таямніца асабістага жыцця і таямніца перапіскі – іх хочацца абараняць. Дрэнная навіна ў тым, што нярэдка правайдэры і інтэрнэт-сэрвісы ў пошуках камерцыйнага прыбытку гатовыя занядбаць правамі сваіх карыстачоў. Акрамя таго, інфармацыя можа патрапіць да хакераў.

Ананімнасцю можна назваць стан, калі немагчыма супаставіць дзеянне ў сетцы і фізічная асоба, якая дадзенае дзеянне здзейсніла. Па вызначанай асобе немагчыма скласці спіс яго дзеянняў у сетцы.

Забяспечыць поўную ананімнасць у сетцы немагчыма – застаецца лічбавы след. Пры наяўнасці дастатковых рэсурсаў ён прывядзе да рэальнага чалавека. Але простаму чалавеку, не кібернетычнаму злачынцу, дастаткова выконваць некалькі правіл, якія зробяць яго амаль інкогніта.

Дадзеныя перадаюцца ў адкрытым выглядзе па змаўчанні. Хакер, атрымаўшы сеткавы трафік, зможа ўбачыць усе якія перадаюцца ў ім дадзеныя. Каб пазбегнуць такой пагрозы, многія сайты выкарыстоўваюць крыпта пратаколы для перадачы даных. Асноўным пратаколам у сетцы Інтэрнэт з'яўляецца HTTP. Яго версія, якая падтрымлівае шыфраванне, называецца HTTPS. HTTPS з'яўляецца стандартам, які дазваляе абараніць перадаюцца дадзеныя паміж сайтам і карыстальнікам. Яго выкарыстоўваюць практычна ўсе значныя сэрвісы і сайты.

IP-адрас па-ранейшаму з'яўляецца асноўным ідэнтыфікатарам карыстальніка ў сетцы. Цяпер доступ прадастаўляецца толькі пасля ідэнтыфікацыі чалавека па пашпарце, таму правайдэр заўсёды зможа сказаць, хто менавіта ў пэўны момант часу працаваў па IP-адрасу.

Каб схаваць IP-адрас, у асноўным выкарыстоўваюць VPN-тунэль, які дазваляе зашыфраваць трафік і схаваць яго ад інтэрнэт-правайдэра. У выпадку выкарыстання VPN-сэрвісу ўвесь трафік будзе даступны яго ўладальнікам. Варта выбіраць сэрвісы з праверанай рэпутацыяй. Таксама трэба быць гатовым да таго, што VPN-сэрвіс, хутчэй за ўсё, будзе платным.

TOR ужывае так званую цыбульную маршрутызацыю, калі на кожным з участкаў сеткі пакет з дадзенымі шыфруецца па-над папярэднім пакетам, а потым расшыфроўваецца ў зваротным парадку. Па аналогіі з VPN трафік выпускаецца ў інтэрнэт у нейкім іншым месцы, аднак ужо не ў адзіным, а на шматлікіх кропках выйсця, што істотна абцяжарвае доступ да яго і яго аналіз.

Апроч ананімнага доступу да звычайных сайтаў праект TOR выкарыстоўваецца для арганізацыі даркнета. Хуткасць інтэрнэт-злучэння праз TOR будзе істотна павольней звычайнай. Затое вы зможаце захаваць ананімнасць у інтэрнэце.

Пры працы з лічбавымі пляцоўкамі на кампутары ствараюцца файлы, у якіх сайт захоўвае інфармацыю падчас і паміж сеансамі працы з імі – кукі-файлы. Яны захоўваюць налады карыстальніка, каб упрасіць працу з рэсурсам і палепшыць многія сэрвісы. Напрыклад, каб кожны раз не ўводзіць пароль, сайт устанаўлівае аўтарызаваную сесію і захоўвае яе ідэнтыфікатар у cookie-файле. Тэрмін жыцця кукі можна абмежаваць.

Каб сайт распазнаваў карыстальніка, трэба або выдаліць яго cookie-файлы праз спецыяльныя плагіны для браўзэраў, або выкарыстоўваць для ўваходу рэжым "Інкагніта". У адрозненне ад звычайных cookie-файлаў, іншыя ствараюцца сайтамі. Гэтыя cookie усталёўваюцца кнопкамі «Like» на Facebook і сэрвісамі ад інтэрнэт-гігантаў. Пазней гэтыя cookie могуць быць прачытаныя самім Facebook. Алгарытм выкарыстоўвае гэтую інфармацыю, каб паказаць у стужцы навін таргетаваную рэкламу.

Каб заставацца ананімным у частцы іншых cookie-файлаў, можна выкарыстоўваць рэжым "Інкагніта" у браўзэры або спецыяльныя плагіны, якія блакуюць кнопкі "Like" і падобныя "жучкі" на сайтах. Але ў выпадку блакавання нярэдка ўзнікаюць праблемы з адлюстраваннем кантэнту, бо частка карыснага функцыяналу блакуецца разам з які адсочвае блокам.

Па змаўчанні сайтам даступна вельмі абмежаваную колькасць інфармацыі аб канчатковай сістэме карыстальніка, яго кампутары. Напрыклад, недаступны MAC-адрас – унікальны нумар сеткавай карты карыстальніка. Таксама недаступным застаецца серыйны нумар працэсара.

Аднак сёе-тое ўсётакі даступна: версія браўзэра і аперацыйнай сістэмы, дазвол экрана, гадзінны пояс, усталяваная мова і пашырэнні браўзэра і таму падобныя дробязі. Не варта недаацэньваць названы набор інфармацыі.

Вектар, складзены з гэтых параметраў, будзе ўнікальным. Сайт можа запомніць злепак, а потым параўноўваць яго кожны раз пры ўваходзе на сайт.

Каб абараніцца ад гэтага і забяспечыць поўную ананімнасць у сетцы, устанаўліваюцца спецыяльныя плагіны для браўзэра, якія будуць аддаваць выпадкова сфарміраваны злепак пры запыце сайтаў.

Ёсць яшчэ адзін метад – паводніцкі аналіз. Сутнасць метаду зводзіцца да аналізу рухаў мышы і клавіятурнаму почырку карыстальніка. Клавіятурны почырк – тое, як чалавек набірае тэкст. Мікра паўзы паміж рознымі сімваламі – гэта ўнікальная велічыня. Складанасць метаду складаецца ў тым, што для правядзення аналізу кожны раз трэба чакаць набору тэксту ці дастатковага аб'ёму рухаў мышкай.

Кібернетычная злачыннасць

Кібернетычная злачыннасць – незаконныя дзеянні, якія ажыццяўляюцца людзьмі, якія выкарыстоўваюць інфармацыйныя тэхналогіі для злачынных мэт. Сярод асноўных відаў кібернетычнай злачыннасці вылучаюць распаўсюджванне шкоднасных праграм, узлом пароляў, крадзеж нумароў крэдытных карт і іншых банкаўскіх рэквізітаў, а таксама распаўсюджванне супрацьпраўнай інфармацыі праз Інтэрнет.

Асноўныя прыкметы камп'ютарных злачынстваў былі сфармуляваны ў 1974 годзе на Канферэнцыі Амерыканскай асацыяцыі адвакатаў. Выдзелены тры напрамкі камп'ютарных злачынстваў:

1) выкарыстанне ці спроба выкарыстання кампутара, вылічальнай сістэмы ці сеткі кампутараў з мэтай атрымання грошай, уласнасці ці паслуг;

2) наўмыснае несанкцыянаванае дзеянне, якое мае на мэце змяненне, пашкоджанне, знішчэнне або выкраданне камп'ютара, вылічальнай сістэмы, сеткі камп'ютараў або змяшчаюцца ў іх сістэм матэматычнага забеспячэння, праграм або інфармацыі;

3) наўмыснае несанкцыянаванае парушэнне сувязі паміж кампутарамі, вылічальнымі сістэмамі або сеткамі кампутараў.

Несанкцыянаваны доступ ажыццяўляецца з выкарыстаннем чужога імя, змяненнем фізічных адрасоў тэхнічных прылад, выкарыстаннем інфармацыі, якая засталася пасля рашэння задач, мадыфікацыяй праграмнага і інфармацыйнага забеспячэння, крадзяжом носьбіта інфармацыі, устаноўкай апаратуры запісу, якая падключаецца да каналаў перадачы даных.

Увод у праграмнае забеспячэнне "лагічных бомбаў", якія спрацоўваюць пры выкананні вызначаных умоў і часткова ці цалкам выводзяць з ладу кампутарную сістэму. "Часовая бомба" – разнавіднасць "лагічнай бомбы", якая спрацоўвае па дасягненні вызначанага моманту часу. "Траянскі конь" складаецца ў таемным увядзенні ў чужую праграму каманд. Яны дазваляюць ажыццяўляць новыя, не якія планаваліся ўладальнікам праграмы функцыі, але адначасова захоўваць і ранейшую працаздольнасць.

Вірусы пераследуюць мэту хакера сцерці ўсе дадзеныя праграмы, перайсці ў наступную кампутарную праграму і зрабіць тое ж самае. Яны валодаюць ўласцівасцямі пераходзіць праз камунікацыйныя сеткі з адной сістэмы ў іншую сістэму. Яны распаўсюджваюцца як віруснае захворванне. Выяўляецца вірус не адразу.

Першы час кампутар выношвае інфекцыю, паколькі для маскіроўкі вірус нярэдка выкарыстоўваецца ў камбінацыі з "лагічнай бомбай" ці "часовай бомбай". Вірус назірае за ўсёй апрацоўванай інфармацыяй і можа перамяшчацца, выкарыстоўваючы перасылку інфармацыі.

Супраць вірусаў выкарыстоўваюцца тэкставыя праграмы-антывірусы. Ахоўныя праграмы падпадзяляюцца на тры выгляду: якія фільтруюць (якія перашкаджаюць пранікненню віруса), супрацьінфекцыйныя (пастаянна кантралюючыя працэсы ў сістэме), супрацьвірусныя (настроеныя на выяўленне асобных вірусаў).

Асаблівасцю камп'ютарнай неасцярожнасці з'яўляецца тое, што беспамылковых праграм у прынцыпе не бывае. Калі праект практычна ў

любой вобласці тэхнікі можна выканаць з велізарным запасам надзейнасці, то ў вобласці праграмавання такая надзейнасць умоўная, а ў шэрагу выпадкаў амаль не дасягальная.

Падробка кампутарнай інфармацыі з'яўляецца разнавіднасцю несанкцыянаванага доступу з той розніцай, што карыстацца ім можа, як правіла, не старонні карыстач, а сам распрацоўнік, прычым які мае досыць высокую кваліфікацыю.

Ідэя злачынства складаецца ў падробцы выходнай інфармацыі кампутараў з мэтай імітацыі працаздольнасці вялікіх сістэм, складовай часткай якіх з'яўляецца кампутар. Пры досыць спрытна выкананай падробцы часцяком атрымоўваецца здаць замоўцу загадзя няспраўную прадукцыю.

Прысваенне машыннай інфармацыі, у тым ліку праграмнага забеспячэння, шляхам несанкцыянаванага капіравання не кваліфікуецца як крадзеж, паколькі крадзеж спалучаны з канфіскацыяй каштоўнасцей з фондаў арганізацыі. Пры неправамерным звароце ва ўласнасць машынная інфармацыя можа не адбірацца з фондаў, а капіявацца.

Інфармацыя павінна быць выдзелена як самастойны прадмет крымінальна-прававой аховы.

Слова хакер (першапачаткова той, хто робіць мэблю сякерай) мае некалькі азначэнняў:

- Чалавек, які любіць даследаваць і выцягваць максімум магчымасцяў праграмуемых сістэм, у адрозненне ад большасці карыстальнікаў, якія не лезуць глыбей неабходнага мінімуму.
- Той, хто праграмуе захоплена, нават апантана ці атрымлівае асалоду ад працэсам распрацоўкі больш, чым тэорыямі праграмавання.
- Чалавек, здольны хутка схапіць сутнасць з'явы.
- Чалавек, здольны да хуткай распрацоўцы праграм.
- Эксперт па вызначанай сістэме, як правіла, часта выкарыстоўвалы яе.
- Эксперт або энтузіяст любога роду.

- Той, хто адчувае інтэлектуальную асалоду ад творчага пераадолення або абыходу абмежаванняў.
- Чалавек, які спрабуе выявіць неабходную інфармацыю.

Сучаснае паняцце "хакер" характарызуе ўсіх сеткавых узломшчыкаў і стваральнікаў кампутарных вірусаў.

Віды хакераў

Кракер – займаецца ўзломам прыкладнога праграмнага забеспячэння для таго, каб атрымаць з shareware-праграм (праграм з абмежаванай функцыянальнасцю, прызначаных, у асноўным, для дэманстрацыі карыстачу магчымасцяў поўнай версіі) паўнавартасныя камерцыйныя версіі. Кракер з'яўляецца праграмістам дастаткова высокага ўзроўню.

Фрыкер – даследуе тэлефонныя сеткі з мэтай знайсці магчымасць тэлефанаваць бясплатна. Гістарычна фрыкерства – самы першы від хакерскай дзейнасці, які ўзнік у 60-70-ыя гады XX стагоддзі. У апошнія гады фрыкеры сталі займацца таксама і даследаваннем сетак для мабільных тэлефонаў.

Кардэр – займаецца нелегальным атрыманнем нумароў крэдытных карт і звестак аб іх уладальніках. Часта гэтая дзейнасць спалучаецца з хакерскай дзейнасцю. Кардэрства лічыцца найбольш сур'ёзным злачынствам, і таму з'яўляецца самым небяспечным відам хакерскай дзейнасці.

У апошні час шырокае распаўсюджванне атрымліваюць толькі паштовыя вірусы, якія распаўсюджваюцца за рахунак памылак у паштовай праграме Outlook, а пошук такіх памылак і можна лічыць хакерскай дзейнасцю.

Асноўнай мэтай інтэрнэт-махлярства з'яўляецца падман карыстальнікаў глабальнага павуціння і крадзеж канфідэнцыйнай інфармацыі, якая пасля выкарыстоўваецца ў асабістых мэтах злачынца. У выніку такой дзейнасці, мільёны людзей ва ўсім свеце нясуць значныя страты кожны год.

Існуе вялікая колькасць розных відаў інтэрнэт-махлярства. Але ўсіх іх аб'ядноўвае адно: поспех усіх гэтых метадаў напроста залежыць ад ступені даверлівасці і бязладнасці карыстача. Неабходна выконваць некалькі простых правіл:

− не давяраць усім незразумелым паведамленням, у якіх змяшчаецца просьба прадставіць асабістыя дадзеныя;

− ігнараваць спам;

− не адкрываць падазроныя лісты, якія прыходзяць на электронную пошту;

− не паведамляць персанальныя дадзеныя;

− быць акуратнымі пры здзяйсненні анлайн – пакупак, выбіраць для гэтага сайты, якія забяспечваюць бяспеку здзелак і канфідэнцыяльнасць асабістых дадзеных.

Неабходна карыстацца шматузроўневай сістэмай бяспекі. Для гэтага неабходна ўсталяваць і рэгулярна абнаўляць праграмы для забеспячэння бяспекі кампутара (антывірус і фаервол).

У сацыяльнай сетцы заўсёды ёсць рызыка натыкнуцца на шкодную інфармацыю, якая заклікае да ўжывання наркотыкаў, суіцыду, інфармацыю аб псеўдарэлігійных і містычных дзеяннях і сектах.

У сетцы можна сутыкнуцца з рознымі паслугамі, якія прапануюцца пасля аплаты на кароткі нумар. Часцей за ўсё гэта звычайнае махлярства. Таму не варта прымаць файлы ад незнаёмых людзей, адчыняць сумнеўныя спасылкі, таму што ў выніку гэтага можна заразіць кампутар вірусамі.

Прапаганда гвалту, забароненых ідэй, распаўсюджванне парнаграфіі мае месца ў сацыяльных сетках. Нягледзячы на маніторынг і блакіроўку падобных старонак, яны з'яўляюцца зноў і ўсяляк хаваюць сваю скіраванасць.

Магчымасці Інтэрнэта выкарыстоўваюцца прадстаўнікамі экстрэмісцкіх плыняў.

Выдалены напад або эксплойт арыентаваны на захоп дадзеных, заражэнне сетак вірусным праграмным забеспячэннем, нанясенне істотных

страт сеткі і асобным кампутарам. У залежнасці ад выкарыстоўваных тэхнік, можна вылучыць некалькі тыпаў выдаленых нападаў: пашкоджанне кэша DNS, дэсінхранізацыя TCP, DoS-напад, ICMP-напад і сканаванне партоў.

З-за разнастайнасці сродкаў выдаленых нападаў спосабаў абароны ад іх мноства. Улічваючы размах тэхнічных сродкаў, дастаткова вялікая група хакераў заўсёды зможа знайсці пралом у сістэме.

Атака з кліенцкага боку заснавана на ўзаемадзеянні з карыстачом сеткі або кампутара. Хакеры спрабуюць прымусіць карыстальніка ўвесці свае дадзеныя на падробленым (фішынгавым) сайце. У ход ідуць усе даступныя спосабы: шкоднасныя спасылкі, дакументы і прыкладанні. Нават дасведчаны карыстач не заўсёды можа адрозніць фішынгавы сайт ад арыгінальнага – копіі праўдападобныя, заўважыць малаважную памылку друку ў адрасе сайта вельмі цяжка.

Хакеры вельмі цярплівыя і гатовыя чакаць месяцамі, пакуль карыстач сваімі дзеяннямі не адкрые ім доступ. Таму ўсе супрацоўнікі павінны ведаць аб такой небяспецы і разумець, якую адказнасць яны на сябе бяруць.

Карпаратыўныя кампутары павінны выкарыстоўвацца толькі для працоўных патрэб, а колькасць праграмнага забеспячэння на іх павінна быць зведзена да мінімуму, павінны выкарыстоўвацца толькі аўтарызаваныя праграмы. Памяншэнне магчымых кропак узлому праз браўзэры, паштовыя кліенты, прыкладанні і медыя-плэеры – выдатны метад для папярэджання хакерскай атакі.

Метад "грубай сілы" выкарыстоўваецца хакерамі, калі ні адна з іх спроб атрымаць доступ да сеткі стандартнымі метадамі не ўвянчалася поспехам. Сутнасць метаду складаецца ў тым, каб ужыць усе вядомыя спосабы пранікнення ў надзеі, што адзін з іх ці ўдалая камбінацыя метадаў дазволіць узламаць сістэму абароны.

Часта выкарыстоўваецца поўны перабор значэння палёў (напрыклад, адрасоў і пароляў) датуль, пакуль не будзе падабраны дакладны варыянт. Гэты тып атаки часцей за ўсё наносіць шмат страт сеткі і абсталяванню,

аднак яго лёгка адсачыць па вялікіх масівах невядомых дадзеных, якія з'явіліся ў сеткі.

Для абароны ад анлайн-атак метадам поўнага перабору значэнняў выкарыстоўваюцца абмежаваную колькасць спроб уводу пароля, затрымка паміж спробамі ўводу, спецыяльныя пытанні для аднаўлення пароля, выкарыстанне CAPTCHA або верыфікацыі па СМС і блакіраванне акаўнта пасля некалькіх няўдалых спроб уваходу.

Сацыяльная інжынерыя мяркуе псіхалагічную маніпуляцыю. У выпадку поспеху, карыстач добраахвотна перадае хакеру канфідэнцыйную інфармацыю: нумары тэлефонаў, адрасы, паролі, нумары крэдытных карт.

Часам гэта самы просты і эфектыўны метад атрымання доступу да добра абароненай сеткі (менавіта так Эдвард Сноўдэн атрымаў доступ да сеткі АНБ ЗША).

"Чалавек пасярэдзіне" ўяўляе сабой перахоп і падмену паведамленняў паміж двума карыстальнікамі. Для нападу выкарыстоўваюцца неабароненыя пратаколы перадачы дадзеных і практычна ў 100% выпадкаў карыстачы і не падазраюць, што іх паведамленні перахапляюцца, а хакеры кантралююць увесь працэс камунікацыі.

Варта звярнуць увагу на налады роўтара і сервера, выкарыстоўваць моцнае шыфраванне і абароненыя пратаколы перадачы дадзеных, усталёўваць убудовы для браўзэраў, якія аўтаматычна шыфруюць выходную інфармацыю і пазбягаць доступу праз публічны Wi-Fi.

Хакеры становяцца разумнейшыя з кожным днём. Напады эвалюцыянавалі ад кароткіх нападаў і агрэсіўных да метадычных, добра спланаваных, працяглых аперацый, улучальных некалькі (калі не ўсё) спосабы ўзлому.

Традыцыйныя метады абароны антывірус, фаервалы, VPN, менеджэры пароляў, адсочванне трафіку, інтэрнэт-шлюзы служаць у першую чаргу для адсочвання першых крокаў хакераў у сетцы. Хакеры разбіраюцца ва ўсіх магчымых тыпах абароны не горш, а часта і лепш, адмыслоўцаў па бяспецы,

таму ўсе сучасныя метады пранікнення па змаўчанні ствараюцца так, каб абыходзіць абарону карпаратыўных сістэм.

Вялікая колькасць кібернетычных нападаў з'яўляецца паспяховым па некалькіх прычынах. Яны не залежаць ад месцазнаходжання кібернетычнага злачынца і аддаленасці ад яго патэнцыйнай ахвяры, а таксама часавых рамак і гадзінных паясоў.

Узламанае IT-асяроддзе можа пацягнуць за сабой крытычныя для бізнэсу наступствы:

нанесці рэпутацыйную шкоду і знізіць узровень даверу з боку кліентаў, бо іх дадзеныя таксама могуць патрапіць у чужыя рукі.

Узлом інфраструктуры спалучаны і з фінансавымі рызыкамі: з прычыны адтоку заказчыкаў і страты ўнікальных інавацыйных распрацовак арганізацыі, яе канкурэнтаздольнасць можа значна зваліцца на рынку.

Сітуацыя ўскладняецца тым, што метады і тактыкі зламыснікаў увесь час эвалюцыянуюць. Хакеры бесперапынна адаптуюць свае напады да новых рэалій і тэхналогіям. Сучасныя кібернетычныя напады максімальна аўтаматызаваны, што дазваляе хакерам паскараць іх правядзенне і выкарыстоўваць штучны інтэлект для падвышэння поспеху іх рэалізацыі.

Выкарыстоўваныя сродкі абароны эфектыўна выконваюць сваю задачу па забеспячэнні бяспекі. Яны блакуюць тыпавыя напады, аднак яны пакуль не дасканалыя ў стаўленні кропкавых, мануальных пагроз.

Дзеянні хакераў можна падзяліць на два асноўных выгляду – размеркаваныя і мэтавыя напады. Размеркаваныя кібернетычныя атакі ўяўляюць сабой выкарыстанне бот-сеткі і накіраваны адначасова на вялікую колькасць карыстальнікаў і рэсурсаў кампаній. У такіх нападах выкарыстоўваюцца якія ўцяклі базы дадзеных арганізацый і карыстачоў.

Мэтавымі атакамі называюць загадзя спланаваны напад на пэўную кампанію або інфраструктуру. Пры гэтых інцыдэнтах хакер не толькі атрымлівае доступ да ўнутраных рэсурсаў, але і застаецца ў сетцы кампаніі, пакуль яго не выявяць. Гэта могуць быць дні, месяцы і нават гады.

Мэтавыя атакі рэалізуюцца хакерамі з высокімі тэхнічнымі кампетэнцыі. Яны выкарыстоўваюць аўтаматызаваныя прылады, самастойна вызначаюць вектары нападу, эксплуатуюць 0-day уразлівасці і некаторыя асаблівасці сістэмы, абапіраючыся на свой досвед.

Кібернетычныя напады ўяўляюць небяспеку, як для звычайных карыстачоў, так і для бізнэсу. У абодвух выпадках наступствы могуць быць не проста непрыемнымі, але і крытычнымі. DDoS-напады, фішынг і напады на відэаканферэнцыі ўзначалілі спіс кібернетычных пагроз.

Аднак і іншыя тыпы нападаў прыносяць масу праблем, як бізнэсу, так і звычайным карыстачам. Хакеры шантажуюць карыстальнікаў месэнджараў з дапамогай ботаў, залазяць у сетку праз QR-коды і выкарыстоўваюць уразлівасці ў наладах або шыфраванні легальнай сеткі, а таксама звяртаюцца да нападаў "грубай сілы". Для таго, каб лепш разумець дзеянні хакераў, неабходна ведаць, якія існуюць тыпы нападаў на інфраструктуру і іх ключавыя асаблівасці.

DDoS-напады ўяўляюць размеркаваныя напады тыпу "адмова ў абслугоўванні". Яны рэалізуюцца за кошт выкарыстання некалькіх скампраметаваных кампутарных сістэм у якасці крыніц атакавалага трафіку. Гэтыя напады забіваюць сістэмы вялікай колькасцю запытаў, у выніку чаго прапускная здольнасць зніжаецца, і сістэмы становяцца перагружанымі і недаступнымі.

У аснове фішынгавых нападаў ляжыць выкарыстанне электронных лістоў, якія могуць быць замаскіраваныя пад легітымныя паведамленні ад розных кампаній. У такім фэйкавым паведамленні хакеры могуць прапаноўваць перайсці па спасылцы, спампаваць заражаны файл або прасіць перадаць канфідэнцыйныя дадзеныя карыстача – лагіны, паролі і нумары рахункаў банкаўскіх карт.

Brute-force прадстаўляюць напады "грубай сілай". Яны з'яўляюцца даволі простым метадам пранікнення ў інфраструктуру і ўяўляюць сабой "адгадванне" уліковых запісаў карыстальніка. Некаторыя хакеры

выкарыстоўваюць прыкладанні і скрыпты ў якасці прылад перабору, якія спрабуюць мноства камбінацый пароляў, каб абыйсці працэсы аўтэнтыфікацыі. Калі пароль слабы, то хакерам спатрэбіцца ўсяго пару секунд, таму бізнэс павінен ужываць строгую палітыку пароляў.

Бот – гэта праграмны робат, які імітуе або замяняе паводзіны чалавека і выконвае простыя задачы з хуткасцю, якая перавышае карыстацкую актыўнасць. Некаторыя робаты бываюць карыснымі, і іх дзеянні накіраваны на падтрымку карыстальнікаў, аднак існуюць і шкоднасныя. Да прыкладу, яны выкарыстоўваюцца для аўтаматычнага сканавання вэб-сайтаў і пошуку ўразлівасцяў, а таксама выкананні простых кібернетычных нападаў.

У рамках нападу праз пасярэдніка (MITM) кібернетычны злачынец становіцца "трэцім лішнім" і прапускае ўвесь вэб-трафік праз сябе. У гэты момант патэнцыйная ахвяра ні пра што не падазрае, што прыводзіць да таго, што ўсе ўліковыя дадзеныя для ўваходу ў сістэмы аказваюцца ў распараджэнні хакера.

Пасля атрыманая інфармацыя можа быць выкарыстана для крадзяжу карпаратыўных даных або несанкцыянаваных пераводаў сродкаў.

Экалагічныя кампаненты бяспекі

Тая ці іншая праява бяспекі ўзаемазвязана з характарам небяспечнай змены навакольнага асяроддзя, фармуючы тым самым няўстойлівае светаадчуванне ў чалавека, сацыяльных груп і сучаснага грамадства. Прытрымліваючыся такой логікі, атрымліваецца, што, калі б у прыродным свеце не было небяспек, то не было б і праблем, звязаных з забеспячэннем бяспекі. Бяспека ўяўляе пэўны, суцэль вызначаны вынік спецыфічнай дзейнасці па нейтралізацыі, папярэджанні пагроз, забеспячэнню абароны.

З гэтай тэзы выцякаюць два падыходы ў разуменні прыроды бяспекі: як праява аб'ектыўнай прыроды жывых сістэм захоўваць сваю цэласнасць дзякуючы ўстойліваму або няўстойліваму ўзаемадзеянню і стану; як

суб'ектыўная натуральная ахоўная рэакцыя або дзейнасць па стварэнні вызначанага асяроддзя для свайго самазахавання.

Бяспека – якаснае сістэмнае ўласцівасць арганічнага жыцця, якое не толькі забяспечвае выжыванне розных арганізмаў, але і спрыяе іх развіццю. Асноўнай мэтай любога з гэтых жывых структурных узроўняў з'яўляецца яго ўласнае выжыванне за рахунак стварэння бяспечнага асяроддзя існавання.

Праблема сацыяльнай бяспекі мае ў сістэме філасофскага пазнання ўніверсальны характар. Гэта абумоўлена наступнымі прычынамі:

Усе сферы жыццядзейнасці чалавека ў вызначанай ступені злучаны з фактарам бяспекі. Адны з іх выступаюць у якасці найважнейшых дэтэрмінант сацыяльнай бяспекі. Іншыя – паўстаюць у выглядзе следстваў сацыяльных дзеянняў і працэсаў, накіраваных на забеспячэнне бяспекі ў той ці іншай яе форме.

Грамадства выступае ў форме падсістэмы аб'ектыўнай рэальнасці, адносна адасобленай ад прыродных утварэнняў, але арганічна звязанай з імі. Яно падпарадкоўваецца ўсеагульным законам быцця. Характэрная для грамадства, сацыяльная форма руху ў якасці перадумовы свайго існавання абапіраецца на найнізкія формы руху матэрыі (механічную, фізічную, хімічную і біялагічную) і ўтрымоўвае іх у сабе. Гэта ўказвае на значнасць прыродных асноў сацыяльнай бяспекі, без якіх само існаванне грамадства становіцца немагчымым.

Галоўным адрозненнем грамадства ад іншых падсістэм аб'ектыўнай рэальнасці з'яўляецца тое, што яно заўсёды ўяўляе сабой вызначанае спалучэнне матэрыяльнага і ідэальнага, аб'ектыўнага і суб'ектыўнага, стыхійнага і планамернага, выпадковага і заканамернага.

Гэта звязана з тым, што ў грамадстве, у адрозненне ад прыроды, дзейнічаюць людзі, надзеленыя свядомасцю і воляй, іх учынкі заўсёды мэтанакіраваны. Але дзейнасць людзей далёка не заўсёды прыводзіць да чаканых вынікаў, паколькі ў складаных грамадскіх з'явах адбываецца сутыкненне сіл, дзеянняў, учынкаў розных суб'ектаў, што і вызначае

аб'ектыўнасць агульнага ходу сацыяльнага працэсу. Падобная аб'ектыўнасць заканамернасцей функцыянавання і развіцця грамадства выступае адной з найважнейшых дэтэрмінант сацыяльнай бяспекі.

Бяспека як стан захаванасці мяркуе падтрыманне вызначанага балансу паміж уздзеяннем на аб'екты навакольнага асяроддзя.

Размеркаваныя сеткавыя напады часта завуцца размеркаванымі нападамі тыпу "адмова ў абслугоўванні" (Distributed Denial of Service, DDoS). Гэты тып нападу выкарыстоўвае пэўныя абмежаванні прапускной здольнасці, якія характэрны для любых сеткавых рэсурсаў, напрыклад, інфраструктуры, якая забяспечвае ўмовы для працы сайта кампаніі. DDoS-напад адпраўляе на атакаваны вэб-рэсурс вялікую колькасць запытаў з мэтай перавысіць здольнасць сайта апрацоўваць іх усё і выклікаць адмову ў абслугоўванні.

Простымі словамі, гэта напад на вылічальную сістэму з мэтай давесці яе да адмовы, гэта значыць стварэнне такіх умоў, пры якіх добрасумленныя карыстачы сістэмы не могуць атрымаць доступ да якія прадстаўляюцца сістэмным рэсурсам (серверам), або гэты доступ абцяжараны.

У цяперашні час DoS і DDoS-напады папулярныя тым, што дазваляюць давесці да адмовы практычна любую сістэму. Звычайна атака арганізуецца пры дапамозе траянскіх праграм. Папярэдне траяны заражаюць нядосыць абароненыя кампутары звычайных карыстачоў і могуць даволі доўгі час ніяк сябе не выяўляць на заражаным кампутары, чакаючы каманды ад свайго гаспадара. Кампутар можа падвергнуцца такой атацы пры наведванні розных заражаных сайтаў, пры атрыманні электроннай пошты ці пры ўсталёўцы неліцэнзійнага праграмнага забеспячэння.

Калі зламыснік збіраецца пачаць атаку, ён дае каманду, і ўсе раней заражаныя кампутары пачынаюць адначасова дасылаць запыты на сайт-ахвяру. Найбольш масавая DoS-атака ў Беларусі была праведзена экстрэмісцкімі каналамі ў 2021 годзе.

Зламыснікі, наўмысна утойваючы інфармацыю аб крымінальнай адказнасці за ўдзел у DoS-нападзе, прыцягнулі да ўдзелу ў ёй больш за 10

тысяч грамадзян (пераважна з ліку моладзі). Практычна ўсе ўдзельнікі гэтага супрацьпраўнага дзеяння былі ўстаноўлены, а найбольш актыўныя з іх былі прыцягнуты да крымінальнай адказнасці.

Інструменты забеспячэння бяспекі IT-ландшафту

Пісьменны выбар прылад забеспячэння бяспекі IT-ландшафту – заклад захавання прыватнасці і захаванасці карпаратыўных дадзеных. Меры па забеспячэнні інфармацыйнай бяспекі можна падзяліць на тры ключавыя віды: тэхнічныя сродкі, арганізацыйныя меры і прафілактычныя праверкі ўзроўню абароненасці. Разгледзім тэхнічныя сродкі.

WAF-комплекс – гэта міжсеткавы экран для вэба-прыкладанняў, асноўнымі функцыямі якога з'яўляюцца выяўленне і блакіроўка нападаў. З дапамогай WAF-комплексу можна не толькі выяўляць шкоднасны трафік, але і таксама вызначаць, якія напады былі накіраваныя на бізнэс крытычныя сістэмы. Укараненне гэтага інструмента дазваляе бізнэсу абараніцца ад нападаў на бізнес-логіку прыкладанняў.

Міжсеткавыя экраны (FW) з'яўляюцца лічбавым ахоўным бар'ерам вакол IT-інфраструктуры, які абараняе сетку і прадухіляе несанкцыянаваны доступ. Міжсеткавыя экраны забяспечваюць бяспеку сеткі шляхам фільтрацыі ўваходнага і выходнага сеткавага трафіку на аснове набору правіл. Задача міжсеткавых экранаў складаецца ў тым, каб паменшыць ці выключыць узнікненне непажаданых сеткавых падлучэнняў, дазваляючы пры гэтым вольна працякаць усім законным камунікацыям.

Антывірус – гэта праграма, якая выяўляе заражэнне і выконвае дзеянні па яго ўстараненню: лечыць або выдаляе заражаныя файлы. Антывіруснае праграмнае забеспячэнне працуе і як прафілактычны сродак. Яно не толькі дужаецца, але і прадухіляе заражэнне кампутара ў будучыні. Антывіруснае праграмнае забеспячэнне дазваляе бізнэсу абараніцца ад шпіёнскага

праграмнага забеспячэння, шкоднасных праграм, фішынгавых нападаў, спам нападаў і іншых кібернетычных пагроз.

DLP – гэта набор інструментаў і працэсаў, якія прымяняюцца для прадухілення страты і нелегітымнага выкарыстання канфідэнцыйных дадзеных. DLP-сістэма адсочвае ўвесь трафік у абароненай карпаратыўнай сетцы і дазваляе выяўляць парушэнне палітык, несанкцыянаваны доступ да дадзеных з боку неаўтарызаваных карыстальнікаў і блакаваць спробы несанкцыянаванай перадачы крытычна важных карпаратыўных дадзеных.

Асноўная лінія абароны карпаратыўнай пошты – гэта бяспечны шлюз. Ён фільтруе шкоднасныя паведамленні і адпраўляе іх у карантын. Бяспечны шлюз электроннай пошты можа блакаваць да 99,99% спаму, выяўляць і выдаляць лісты, якія змяшчаюць шкоднасныя спасылкі ці ўкладанні.

SIEM-сістэмы збіраюць і аб'ядноўваюць дадзеныя са ўсёй IT-інфраструктуры: ад хост-сістэм і прыкладанняў да прылад бяспекі. Пасля адбываецца класіфікацыя і аналіз інцыдэнтаў і падзеяў. SIEM-сістэмы на аснове правіл карэляцыі атрымоўваных падзей выяўляюць патэнцыйныя інцыдэнты ИБ і апавяшчаюць пра гэта адміністратара бяспекі.

Арганізацыйныя меры мяркуюць рэгулярныя ўнутрыкарпаратыўныя вебинары і навучанне асновам лічбавай бяспекі. Гэта дазваляе падвысіць дасведчанасць супрацоўнікаў і пераканацца, што яны валодаюць навыкамі, неабходнымі для выяўлення і супрацьдзеянні нападам.

Поўны доступ кожнага супрацоўніка да ўсіх дадзеных кампаніі мае свае рызыкі - уцечка кліенцкіх баз, інсайдэрскі гандаль і раскрыццё інфармацыі аб інавацыйнай дзейнасці. Кампаніям неабходна выразна размяжоўваць правы доступу карыстачоў да карпаратыўных сістэм, файлаў і абсталяванню.

Аўдыт інфармацыйнай бяспекі IT-інфраструктуры – гэта незалежная ацэнка ўзроўню абароненасці кампаніі на адпаведнасць прызнаным практыкам у галіне забеспячэння лічбавай бяспекі, а таксама заканадаўчым патрабаванням: міжнароднаму стандарту ISO/IEC 27001, ФЗ-152 "Аб

персанальных дадзеных" і ФЗ-187 "Аб бяспецы крытычнай інфармацыйнай інфраструктуры». У аўдыт уваходзяць ацэнка эфектыўнасці і надзейнасці існуючых метадаў абароны, аналіз слабых месцаў і ўразлівасцяў, а таксама ацэнка іх крытычнасці і распрацоўка рэкамендацый па іх устараненню.

Аўдыт лічбавай бяспекі – найважнейшая мера пры распрацоўцы канцэпцыі абароны IT-ландшафту. Аднак па-сапраўднаму яна эфектыўная толькі ў тым выпадку, калі ажыццяўляецца з вызначанай перыядычнасцю, а не як разавая ініцыятыва.

Апроч аўдыту, варта звярнуць увагу і на тэставанне на пранікненне – PenTest. Гэта імітацыя рэальнага нападу з ужываннем тэхнік і метадаў, якія выкарыстоўваюць зламыснікі з мэтай выяўлення ўразлівых кропак у IT-інфраструктуры кампаніі.

Правядзенне PenTest дазваляе бізнэсу атрымаць рэальную ацэнку і паўнавартасную карціну ўзроўню абароненасці інфраструктуры і ўсіх інфармацыйных сістэм, а таксама сфарміраваць спіс дзеянняў і мерапрыемстваў, неабходных для павышэння ўзроўню бяспекі.

Інфармацыйныя войны і бяспека

Асноўнай мэтай інфармацыйнай вайны з'яўляецца забеспячэнне нацыянальнай бяспекі краіны, калі неабходна вырашэнне задач уздзеяння на супрацьлеглы бок і абарона ўласнага інфармацыйнага рэсурсу і звязаных з ім сістэм. Дадзены варыянт канцэптуальных асноў інфармацыйнай вайны зыходзіць з яе прамежкавага статуту паміж "халоднай" вайной, якая ўключае ў сябе эканамічную, і "гарачай" вайной з яе рэальнымі баявымі дзеяннямі.

Інфармацыйная вайна мяркуе валоданне сітуацый. Кагнітыўная вайна, гэта значыць вайна ведаў і сэнсаў, відавочна не зводзіцца толькі да інфармацыйных нападаў. Адзін з ключавых напрамкаў сучаснай кагнітыўнай вайны – гэта ўкараненне новых адукацыйных стандартаў і тэхналогій.

Страта нацыянальнай сістэмы адукацыі не менш небяспечная, чым паражэнне на інфармацыйным фронце. Цэнтры арганізацыі кагнітыўнай вайны ў іерархіі сусветнага глабальнага кіравання знаходзяцца над цэнтрамі інфармацыйнай вайны, бо іх прадмет – стратэгіі сусветнага развіцця, у той час як галоўнай задачай СМІ становіцца інфармацыйна-камунікацыйнае абслугоўванне інтарэсаў гэтых цэнтраў.

Кагнітыўнае хакерства накіравана на маніпуляцыю ўспрыманнем карыстальніка, каб можна было ажыццявіць атаку. Кагнітыўная вайна можа неўзаметку хавацца з тэлесерыяле, рамане, песні. Яна кадуецца ў словах і людзях. Аўтар тэхналогіі – Франсуа дзю Клюзель, былы французскі афіцэр, які ў 2013 годзе дапамог стварыць Цэнтр інавацый НАТА (iHub).

Цэнтр дыслакаваны ў Норфалскай базе, штат Вірджынія. iHub атрымлівае фінансаванне ад Саюзнага камандавання па трансфармацыі (АСТ), якое з'яўляецца адным з двух стратэгічных камандаванняў на чале структуры вайсковага кіравання НАТА. Сутнасць тэхналогіі складаецца ў сістэмным уздзеянні на прытомнасць людзей, выява іх думак. Згодна з новай канцэпцыяй НАТА, задача кагнітыўнай вайны – «узлом асобы» з дапамогай выкарыстання «уразлівасцяў чалавечага мозгу» для наступнага ўжывання «сацыяльнага інжынірынгу» з мэтай перафарматавання чалавека. Карацей – фарміраванне новай асобы з іншымі каштоўнаснымі арыенцірамі, мараллю і разуменнем дабра і зла.

Унутры сеткі нават рэклама ўцягнутая ў сістэмнае ўздзеянне. Праз яе адсочваюцца інтарэсы канкрэтнага чалавека. Затым варта мэтанакіраванае ўздзеянне на яго прытомнасць з улікам асобасных запытаў і прыярытэтаў.

Масавы збор дадзеных заходнімі спецслужбамі пацверджаны Эвадром Сноўдэнам, былым супрацоўнікам ЦРУ, які раскрыў інфармацыю аб праграме сачэння спецслужбаў за амерыканцамі і замежнымі грамадзянамі з дапамогай тэлефона і інтэрнэту – PRISM.

У доўгатэрміновай перспектыве (ад аднаго да некалькіх дзясяткаў гадоў) гэта перазагрузка гістарычнай самасвядомасці, сістэмы адукацыі і

выхавання, базавых сэнсаў і мэт грамадства. У тым ліку перапісванне гісторыі, разбурэнне традыцый, укладаў, веры (рэлігіі) і базавых каштоўнасцей. У сярэднетэрміновай перспектыве – рэалізацыя ўздзеянне на нормы паводзін, падрыў даверу да ўлады, раскол грамадства.

Фарміраванне "пятай калоны". Абедзве тэхналогіі выкарыстоўваюць інфармацыйны і псіхаэмацыйны складнікі. Інфармацыйны складнік прадугледжвае змену зместу ведаў, фактаў і звестак. Гэта значыць дэзінфармаванне, падмену паняццяў. Аб'ектамі ўздзеяння з'яўляюцца: навіны, аналітычныя і сацыялагічныя даныя, праграмы навучання ў вышэйшых навучальных установах і школе.

Псіхаэмацыйны складнік прымяняе маніпуляцыю свядомасцю, настроямі і эмоцыямі, калі індывідууму, групам людзей і грамадству ў цэлым апасродкавана ўкараняюцца патрэбныя настроі, ацэнкі, меркаванні аб чым-небудзь, аб кім-небудзь, і ўсё гэта прымаецца людзьмі неўсвядомлена, без разумення сутнасці. Кагнітыўная вайна паглынула інфармацыйныя войны.

Экзістэнцыйныя пагрозы

Экзістэнцыйная пагроза – гэта небяспека, якая можа сур'ёзна паставіць пад пагрозу існаванне і развіццё якой-небудзь сутнасці, няхай гэта будзе індывід, супольнасць ці нават увесь чалавечы род. Уздзеянне экзістэнцыйнай пагрозы можа быць множным і ахопліваць самыя розныя сферы жыцця.

Адным з асноўных уплываў, які можа мець экзістэнцыйная пагроза на існаванне, з'яўляецца страта сэнсу жыцця. Калі чалавек ці супольнасць сутыкаюцца з пагрозай, якая пастаўляе пад пытанне іх існаванне і будучыня, яны пачынаюць задумвацца аб тым, ці мае жыццё сэнс. Зніжэнне матывацыі, апатыя, дэпрэсія – усе гэтыя з'явы могуць быць следствам экзістэнцыйнай пагрозы.

Акрамя таго, экзістэнцыйная пагроза можа аказаць уплыў на псіхалагічны стан чалавека ці супольнасці. Адчуванне сталай небяспекі і

страху можа выклікаць трывожнасць, нервовасць і падвышаную напружанасць. У такім стане псіхіка чалавека ці групы людзей можа не здольная эфектыўна функцыянаваць, што прыводзіць да пагаршэння жыццёвых умоў і якасці жыцця.

Таксама экзістэнцыйная пагроза можа прывесці да сацыяльнага разладу і канфліктаў. Калі людзі адчуваюць небяспеку і страх за сваё жыццё, яны могуць праяўляць агрэсію і жорсткасць у адносінах да іншых людзей, нервовасць і падвышаную напружанасць. У такім стане псіхіка чалавека ці групы людзей можа не здольная эфектыўна функцыянаваць, што прыводзіць да пагаршэння жыццёвых умоў і якасці жыцця.

Яшчэ адным уплывам экзістэнцыйнай пагрозы на існаванне з'яўляецца змена каштоўнасцяў і прыярытэтаў. Калі ставіцца пад пагрозу само жыццё, людзі пачынаюць пераацэньваць свае каштоўнасці і арыенціры. Матэрыяльныя даброты і індывідуальныя дасягненні могуць саступаць месца каханню, сям'і, духоўным і маральным каштоўнасцям.

У цэлым экзістэнцыйная пагроза аказвае сур'ёзны ўплыў на існаванне і развіццё чалавецтва. Яна можа выклікаць страту сэнсу жыцця, трывожнасць, сацыяльны разлад і змяненне каштоўнасцей. Таму важна прымаць усе магчымыя меры для прадухілення і ўстаранення падобных пагроз, каб забяспечыць стабільнасць і дабрабыт нашай сучаснай цывілізацыі.

У наш час, чалавецтва сутыкаецца з шэрагам экзістэнцыйных пагроз, якія могуць нанесці сур'ёзную шкоду яго існаванню і развіццю. Гэтыя пагрозы з'яўляюцца глабальнымі і паўсюднымі, а іх наступствы могуць мець доўгатэрміновыя і катастрафічныя наступствы.

Адной з галоўных пагроз з'яўляецца змена клімату. Рост тэмпературы на Зямлі ў выніку выкідаў парніковых газаў у атмасферу вядзе да глабальнага пацяплення. Гэта выклікае разнастайныя наступствы, такія як змена пагодных умоў, павышэнне ўзроўню мораў і акіянаў, засухі і паводкі. Усё гэта негатыўна ўплывае на прыродныя экасістэмы і прыводзіць да страты

біяразнастайнасці, што ў канчатковым выніку можа прывесці да незваротнага разбурэння экасістэм і скарачэння рэсурсаў планеты.

Яшчэ адной сур'ёзнай пагрозай з'яўляецца ядзерная вайна. Наяўнасць ядзернай зброі ў многіх краінах свету стварае рэальную верагоднасць яе выкарыстання. Ядзерны канфлікт можа прывесці да масавага знішчэння і страты жыццяў, у тым ліку вельмі верагодную «ядзерную зіму», якая патэнцыйна можа выклікаць кліматычныя змены і голад у маштабе ўсёй планеты.

Інфармацыйныя тэхналогіі і штучны інтэлект таксама ўяўляюць пагрозы для чалавецтва. Сучасныя тэхналогіі могуць быць скарыстаны для стварэння кібератак, маніпуляцыі інфармацыяй і кантролю над грамадствам. Развіццё штучнага інтэлекту можа стварыць сітуацыю, дзе машыны стануць больш разумнымі і магутнымі, чым людзі, што патэнцыйна пагражае існаванню чалавецтва.

І, нарэшце, глабальныя эпідэміі і пандэміі з'яўляюцца іншымі пагрозамі для чалавецтва. Успышкі новых і небяспечных інфекцыйных захворванняў могуць распаўсюджвацца ў маштабах усёй планеты, выклікаючы значныя страты ў жыццях і наносячы ўдар ахове здароўя і эканоміцы.

Каб супрацьстаяць гэтым пагрозам, неабходна развіваць глабальнае супрацоўніцтва і прымаць калектыўныя захады. Узмацненне міжнароднай каардынацыі і ўзаемадзеяння можа дапамагчы ў прадухіленні і кіраванні экзістэнцыяльнымі пагрозамі, забяспечваючы выжыванне і дабрабыт для ўсяго чалавецтва.

Экзістэнцыйная пагроза: важнасць прадухілення

Экзістэнцыйная пагроза ўяўляе сабой небяспеку, якая можа прывесці да знішчэння чалавецтва або сур'ёзнага ўрону для яго існавання і развіцця. Яна ўключае ў сябе розныя віды пагроз, такія як ядзерная вайна, глабальнае пацяпленне, пандэміі, штучны інтэлект, касмічныя стыхійныя бедствы і

іншыя. Прадухіленне экзістэнцыйнай пагрозы мае вялікае значэнне для забеспячэння бяспекі і дабрабыту чалавецтва.

Задача прадухілення заключаецца ў тым, каб прыняць меры і распрацаваць стратэгіі, якія дазволяць пазбегнуць наступлення пагрозы або мінімізаваць яе ўздзеянне ў выпадку ўзнікнення. Важнасць прадухілення экзістэнцыйнай пагрозы заключаецца ў наступным:

Захаванне жыцця і дабрабыту чалавецтва: Прадухіленне экзістэнцыйнай пагрозы дазваляе захаваць жыцці людзей і забяспечыць ім неабходныя ўмовы для развіцця і працвітання.

Захаванне цывілізацыі і культуры: Прадухіленне пагрозы дапамагае захаваць каштоўнасці і дасягненні чалавечай цывілізацыі, а таксама захаваць культурную спадчыну пакаленняў.

Абарона экалагічнай сістэмы: Прадухіленне экзістэнцыйнай пагрозы дазваляе захаваць прыродныя рэсурсы і біялагічную разнастайнасць, забяспечваючы ўстойлівае развіццё планеты.

Бяспека глабальнай супольнасці: Прадухіленне пагрозы спрыяе забеспячэнню бяспекі ўсіх краін і народаў, бо негатыўныя наступствы экзістэнцыйнай пагрозы могуць распаўсюдзіцца на глабальным узроўні.

Для эфектыўнага прадухілення экзістэнцыйнай пагрозы неабходна сумеснае намаганне і супрацоўніцтва ўсіх удзельнікаў міжнароднай супольнасці. Важна распрацаваць і рэалізаваць міжнародныя стратэгіі і палітыкі, а таксама праводзіць даследаванні і распрацоўкі ў галіне навукі, тэхналогій і інавацый, каб выяўляць і аналізаваць патэнцыйныя пагрозы, распрацоўваць эфектыўныя меры прадухілення і рэагаваць на ўзніклыя пагрозы хутка і эфектыўна.

Такім чынам, прадухіленне экзістэнцыйнай пагрозы з'яўляецца неад'емнай часткай бяспекі чалавецтва і яго будучага развіцця. Яно патрабуе сумесных намаганняў і доўгатэрміновых стратэгій для забеспячэння захавання жыцця, захавання цывілізацыі і культуры, аховы прыроды і забеспячэння бяспекі на глабальным узроўні.

Роля навукі ў выяўленні і рашэнні пагроз

Навука адыгрывае ключавую ролю ў выяўленні і вырашэнні экзістэнцыйных пагроз, якія ўяўляюць небяспеку для існавання і развіцця чалавецтва. З дапамогай навуковага метаду даследчыкі выяўляюць і аналізуюць розныя віды пагроз, каб распрацаваць эфектыўныя стратэгіі і рашэнні для іх прадухілення або змякчэння.

Адным з ключавых аспектаў ролі навукі ў выяўленні пагроз з'яўляецца даследаванне і аналіз даных. Навукоўцы збіраюць і аналізуюць інфармацыю аб розных аспектах экзістэнцыйных пагроз, у тым ліку іх прыроду, верагоднасць узнікнення і патэнцыйныя наступствы. Гэтыя дадзеныя дазваляюць лепш зразумець пагрозы і вызначыць меры па іх пераадоленні.

Навука адыгрывае важнейшую ролю ў распрацоўцы новых тэхналогій і інавацый, якія могуць быць выкарыстаны для выяўлення і вырашэння пагроз. Інжынеры, вучоныя-тэхнолагі і іншыя спецыялісты працуюць над стварэннем новых сродкаў дэтэктавання і вырашэння пагроз, такіх як сістэмы ранняга папярэджання, інтэлектуальныя аналітычныя інструменты і многае іншае. Гэтыя тэхналогіі дапамагаюць выявіць і аналізаваць пагрозы больш эфектыўна і аператыўна, што садзейнічае іх больш эфектыўнаму вырашэнню.

Акрамя таго, навука адыгрывае важную ролю ў адукацыі і інфармаванні грамадскасці аб экзістэнцыйных пагрозах. Навукоўцы, камунікацыйныя спецыялісты і журналісты выконваюць ролю тлумачальнікаў і інфарматараў, дапамагаючы людзям лепш зразумець і ўсвядоміць пагрозы, з якімі сутыкаецца чалавецтва, і падахвочваючы да прыняцця неабходных мер па іх прадухіленні і зніжэнні рызык.

У цэлым навука з'яўляецца ключавым інструментам пры выяўленні і вырашэнні экзістэнцыйных пагроз. Даследаванні, аналіз дадзеных, распрацоўка тэхналогій і адукацыя гуляюць абавязковую ролю ў пошуку і прымяненні рашэнняў, якія дапамогуць засцерагчы існаванне і развіццё чалавецтва.

Асноўная прычына з'яўлення лічбавых сістэм – неабходнасць інтэнсіфікацыі рашэння задач і важнасць аптымізацыі сацыяльных адносін, звязаных з рашэннем гэтых задач. Перадумовамі для стварэння лічбавых сістэм з'яўляецца залішняя магчымасць лічбавых сістэм, якая можа быць прадстаўлена ў той ці іншай форме для рашэння іншых задач.

Лічбавыя платформы

Платформа – гэта пляцоўка, якая дае іншым магчымасці. Адна з ключавых функцый платформы – прадастаўленне камерцыйных, камунікатыўных, маркетынгавых, інвестыцыйных магчымасцяў дзвюм або больш катэгорый суб'ектаў рынку. У адрозненні ад замкнёнай экасістэмы (самадастатковай і самаўдасканальванай) платформа – гэта рэсурс і магчымасць для карыстальнікаў-нерэзідэнтаў.

Анлайн-платформа – лічбавы сэрвіс «акна магчымасцяў», які палягчае ўзаемадзеянне паміж двума ці больш асобнымі, але ўзаемазалежнымі карыстальнікамі (няхай гэта будзе фірмы або асобныя асобы), якія ўзаемадзейнічаюць праз сэрвіс праз Інтэрнэт

Платформа, дзякуючы сваім камунікатыўным, тэхніка-тэхналагічным, арганізацыйным, маркетынгавым магчымасцям, спрыяе:

- камунікацыі (сацыяльная функцыі),
- навуковаму развіццю, рэалізацыі ідэй (навуковая платформа),
- лепшаму знаходжанню, пошуку, інфармаванню (камунікатыўная),
- прасоўванні і папулярызацыі (маркетынгавая)
- заробак (эканамічная). Вось пералік функцый "платформы".

Разнавіднасці лічбавых платформ

Гандлёвая анлайн-платформа – гэта толькі прыватны выпадак лічбавых платформаў. Ёсць фінтэх-платформы, ёсць платформы развіцця інаватыкі, стартап-платформы, навучальныя платформы.

Маркетплэйс – вузка спецыялізаваная лічбавая платформа, на якой прапануюцца розныя бясшвоўна інтэграваныя або натуральна дапаўняюць адзін аднаго прадукты і паслугі, якія пакрываюць максімальна шырокі спектр патрэб аднаго профілю кліента.

Лічбавыя экасістэмы

Гэта справядліва для прыродных, тэхнагенных ці лічбавых сістэм. Людзі, як і выкарыстоўваны імі комплекс розных лічбавых мабільных і лічбавых стацыянарных прылад, а таксама лічбавых прылад рэальнага свету, развітыя магчымасці і ўзаемна інтэграваныя сэрвісы, імі якія прадстаўляюцца, утворыць лічбавую экасістэму. У першую чаргу, калі гавораць аб экасістэмах, маюць на ўвазе:

Закрытыя сістэмы (самадастаткавыя, устойлівыя і самаўдасканальваемыя), у якіх ствараецца мікраклімат, які спрыяе развіццю ўсяго, які знаходзіцца ў сістэме.

Сумеснае існаванне;

Сумеснае выкарыстанне і аднаўленне рэсурсаў;

Мэта ўсяго, што ўтварае сістэму дваякая: сумесна паляпшаць экасістэму і здабываць не супярэчную развіццю экасістэмы, персанальную, групавую і калектыўную выгаду.

Людзі выкарыстоўваюць лічбавыя прыкладанне каб замовіць прадукты дадому, і тут жа, расплачваюцца за набытыя тавары ў дадатку банка, фармуючы выгаду тым, хто арганізуе такія сэрвісы. Рэгіструюцца на рэйс авіякампаніі ў інтэрнэце, а атрымліваюць білеты або пацвярджаюць рэгістрацыю на рэйс у стацыянарным лічбавым тэрмінале аэрапорта, тым самым, беручы частку функцый адзінай сістэмы на сябе, чым спрашчаюць працу арганізатарам сэрвісу.

Зарэгістраваць кампанію можна на лічбавым сэрвісе "Лічбавага ўрада", там жа можна скарыстацца і сотнямі іншых паслуг, што робіць лагічным узаемаадносіны і спрашчае працэсы. Доступ да гісторыі ўзаемаадносін з

пакупніком можна атрымаць праз мабільнае прыкладанне CRM, тамака жа прасачыць стадыі адпрацоўкі бягучага кантракту і атрымаць прагноз плацяжоў, у выпадку рэгулярных і працяглых узаемаадносін. Архітэктура лічбавай экасістэмы ўяўляе сабой:

- серверную інфраструктуру: вылічальныя прылады, віртуальныя серверы, праграмы і алгарытмы, рэсурсы для захоўвання, каманду распрацоўшчыкаў і інжынераў, менеджмент і кліенцкія службы.
- кліенцкую інфраструктуру: прылада доступу з датчыкамі і інтэрфейсам карыстальніка;
- даныя: банкі даных, алгарытмы работы з дадзенымі.

Лічбавая архітэктура – гэта лічбавае асяроддзе, элементамі якога з'яўляюцца ўдзельнікі (рэзідэнты) і мноства лічбавых сэрвісаў, якія выконваюць задачы рознага ўзроўню, доступ да якіх ажыццяўляецца рэзідэнтам пад адзіным уліковым запісам.

Рэзідэнты выкарыстоўваюць рэсурсы «архітэктуры» і магчымасці для атрымання персанальных і калектыўных выгод, а таксама для сумеснага ўдасканалення экасістэмы.

Банкі + Паслугі + Гандаль = Мабільнасць

Мабільны доступ да магчымасцяў і паслуг – адлюстраванне сусветнай тэндэнцыі. Крыху раней, акном у мабільны свет былі смартфоны. Сёння лічбавыя гіганты ствараюць свае экасістэмы, калі не выходзячы з прыкладання, можна скарыстацца вялікай колькасцю сэрвісаў – пазнаць, вывучыць, абраць, аплаціць і атрымаць тое, што лепш задавальняе запатрабаванне.

Apple, Xiaomi стварылі сваю ўласную анлайн – экасістэму, базавы прадукт якой – мабільная прылада і прыкладанні, якія працуюць на ім.

Такія кампаніі, як Google, Яндэкс, МТС стварылі свае лічбавыя экасістэмы вакол базавага прадукта – лічбавая інфармацыя;

Amazon, падгледзеў патрэбнасці спажыўцоў, падвойваючы лічбавыя і аналагавыя тавары;

Сбер утварыў лічбавую экасістэмы, абапіраючыся на банкаўскую паслугу – як аснову ўзаемаадносін са спажыўцамі. Інфармацыя аб іх патрэбнасці, якая аналізуецца па характары плацяжоў і аплатных тавараў і паслуг, стала прычынай стварэння лічбавых сэрвісаў.

Дзяржаўная праграма "Лічбавы Урад" – экасістэма доступу да тысяч дзяржаўных паслуг, якімі можна скарыстацца не наведваючы офісы дзяржаўных структур, а адзіная інфармацыйная прастора, якая існуе ўнутры экасістэмы дазволіла пазбавіць людзей ад бясконцай колькасці папяровых даведак, праверак і пераправерак, ад недакладнасці і страты дадзеных.

Сёння мы назіраем этап бурнага развіцця экасістэм, доступ да якіх ужо ажыццяўляецца не толькі з мабільных тэлефонаў, але і з разумных прыстасаванняў з інтуітыўным кіраваннем і з дапамогай галасавога кіравання. Аднак, пакуль яшчэ, нават з пункту гледжання IT, не гаворачы ўжо аб маркетынгу, такія экасістэмы маюць толькі малую ўзгодненасць.

Наступны этап – важны этап узгаднення прылад экасістэм: распрацоўкі стандартаў, пратаколаў доступу, бяспекі доступу, але ўжо сёння лічбавыя экасістэмы – прадмет цікавасці маркетынгу. Віды лічбавых экасістэм

Гарызантальная. Розныя сэрвісы ці продаж розных тавараў рознымі незалежнымі пастаўшчыкамі. Прыклад: маркетплэйсы.

Вертыкальная. Сэрвісы ў рамках жыццёвага цыкла прадукта, паслядоўнага выканання прац. Прыклад: аўтасалон – ад пакупкі аўта, праз планавыя сэрвісы і да ўтылізацыі або праграмы «трэйд-ін»;

Змешаная. Сімбіёз гарызантальнай і вертыкальнай мадэлі. Продаж уласных прадуктаў + прапанова дадатковых паслуг ад партнёраў. Прыклад: Экасістэма Сбер або ў аўтасэрвісе: крама + сэрвіс + іншыя паслугі (крэдыт, лізінг, тэхдапамога на дарозе, эвакуацыя).

Маркетынг экасістэм

Мэты кампаній таксама павінны зведаць змены – максімізацыя прыбытку ўжо не павінна разглядацца як самамэта, прыбытак выступае як сродак для развіцця. Асноўнымі мэтамі кампаніі становяцца атрыманне выгод з развіцця грамадства і максімальнага задавальнення яго патрэб. Прычым гэтыя мэты будуць рэалізоўвацца паралельна, без пераважання адной над другой. Лічбавая экасістэма дапамагае:

- спажыўцам – арыентавацца ў лічбавым свеце і падтрымлівае на ўсіх этапах яго жыццёвага цыклу,
- кампаніі – здабываць выгаду, не руйнуючы грамадства і адносіны ў ім і ад сінэргіі накіраваных да захавання і развіццю іншых удзельнікаў рынкавага працэсу
- рынку – развівацца паступальна, перашкаджаючы дэструктыўным крокам асобных удзельнікаў рынкавага працэсу;
- грамадству – выбудоўваць гарманічныя адносіны, накіраваныя на карысць кожнаму.

У цэнтры маркетынгавай экасістэмы – чалавек. Выяўленыя запатрабаванні дазваляюць ствараць лічбавыя сэрвісы і прадукты, якія дапамагаюць і забяспечваюць існуючыя запатрабаванні спажыўцоў: ежа, транспарт, пражыванне, здароўе, праца і забаўка. Маркетынг бізнэсу, інтэграваны ў маркетынг экасістэмы.

У цэнтры інфраструктуры лічбавай экасістэмы – лічбавы банкаўскі сэрвіс, які збірае асноўны паток карыстальнікаў, фінансы і вывучае інтарэсы карыстальнікаў, вытворцаў выгод і фінансавых інстытутаў.

Лічбавая экасістэма працуе на некалькі рынкавых сегментаў, мяркуе скразны доступ да інфармацыі і кругласутачны сэрвіс – гэта новая парадыгма маркетынгу. Традыцыйна маркетынг разглядаў спажыўцоў, канкурэнтаў і дзелавых партнёраў у межах адной галіны і рыначнага сегмента.

Аднак, рынкавыя тэндэнцыі ідуць следам за лічбавай трансфармацыяй і мабільнасцю чалавека: новыя звычкі і тыпы спажывання, новыя лічбавыя тавары і лічбавыя інструменты камунікацыі – усё гэта патрабуе іншага падыходу да рынкавай дзейнасці – маркетынгу лічбавых мабільных экасістэм. Змены рынкавыя вядуць да змены ў арганізацыйнай структуры кампаній – кампаніі стануць пераважна дэцэнтралізаванымі. Колькасць іерархічных узроўняў будзе зведзена да мінімуму, месца аддзелаў і дэпартаментаў зоймуць каманды і працоўныя групы.

Асаблівасці маркетынгу лічбавых экасістэм

- канкурэнцыя не ў сегменце рынку, а за чалавека-спажыўца, у якім бы сегменце ён не знаходзіўся;
- прыбытак не ад магчымасці кампаніі і не ў якія-небудзь традыцыйных для кампаніі відах дзейнасці, а прыбытак ад узаемаадносін са спажыўцом;
- маркетынг адносін – гэта не перацягнуць спажыўца на свой бок, а прайсці за чалавекам туды, у тыя рынкавыя сегменты, дзе ён з'яўляецца спажыўцом;
- следствам гэтага з'яўляецца не пагоня за прыбытковасцю здзелак з канкрэтным спажыўцом, а за павелічэнне колькасці продажаў гэтаму спажыўцу, якія прыпадаюць на розныя рынкавыя нішы і сегменты;
- аналіз дадзеных карыстацкай базы, а не маркетынгавая актыўнасць - вось крыніца ведаў аб спажыўцах;
- сфармуляваныя спажыўцу, у рамках экасістэмы, таргетаваныя прапановы тавараў і паслуг іх розных рынкавых сегментаў зніжаюць выдаткі на прыцягненне;
- адзіныя для экасістэмы прынцыпы прасоўвання сярод спажыўцоў ідэй і прадуктаў;
- унутрысістэмнае стымуляванне спажыўцоў карыстацца ўсімі сэрвісамі платформы;
- брэнд – рэальны актыў і сіла лічбавых экасістэм.

Рынкавыя перспектывы лічбавых экасістэм

Цяпер экасістэмы з'яўляюцца адным з трэндаў развіцця высокатэхналагічнага бізнес-ландшафту. Пакуль яны пераважна працуюць у кампаніях высокіх тэхналогій, банкаўскага сектара, гандлі і тэлекамунікацыйным асяроддзі. Аднак перспектывы ў гэтай галіне вялізныя.

Гэта дэвелаперскія кампаніі, тураператары, авіякампаніі, гандлёвыя сеткі, аўтадылеры, кампаніі індустрыі забаў і інш. Фарміраванне экасістэм павінна кардынальным чынам пераўтварыць эканамічныя рэаліі. Гаворка ні ў якім разе не аб прэярытэце лічбавай экакомікі перад, скажам, энергетыкай. Любыя экасістэмы развіваюцца толькі тады, калі ў іх развейваецца ўсё прапарцыйна і гарманічна. Адно няўхільна – кампетэнтнасць (не лічбавыя дадзеныя, а ўменне прымяняць веды) становіцца асобным таварам.

Капіталізацыя ведаў і інфармацыі, здольнасці развіцця і ўкараненні тэхналогій, канкурэнтаздольнасць, прымянення новых спосабаў збыту прадукцыі, аператыўнасць прыняцця і рэалізацыі рыначных рашэнняў – гэта перадумовы паспяховага маркетынгу лічбавых экасістэм.

Бяспека IT-ландшафту

IT-ландшафт аб'ядноўвае ўсе інфармацыйныя сістэмы прадпрыемства. Яе арганізацыя звычайна адбываецца ў некалькі этапаў: распрацоўка, укараненне, тэсціраванне, увод у эксплуатацыю і далейшая падтрымка.

Перад укараненнем будучай IT-інфраструктуры выконваюцца наступныя этапы: аналіз бізнес-працэсаў арганізацыі аўдыт IT-інфраструктуры аналіз даступных рашэнняў разлік неабходнага бюджэту Вынікам этапа планавання IT-інфраструктуры з'яўляецца зацверджаная мэтавая архітэктура, якая адпавядае патрэбам бізнесу як з пункту гледжання эфектыўнасці, так і па эканамічных паказчыках.

Па зацверджаным тэхнічным заданні выканаўца пачынае рэалізацыю праекта. У залежнасці ад маштабаў праекта можа спатрэбіцца:

- падбор і настройка абсталявання і праграмнага забеспячэння;

- настройка службаў, падключэнне сэрвісаў, стварэнне карыстальнікаў;
- размеркаванне па групах бяспекі;
- вызначэнне, настройка і ўстаноўка правоў доступу ў адпаведнасці з распрацаванымі і зацверджанымі рэгламентамі;
- ўстаноўка і настройка сродкаў абароны інфармацыі;
- настройка неабходных інтэграцый, правядзенне тэсціравання, стварэнне рэгламентаў абслугоўвання і інструкцый.

Пасля ўкаранення тэхнічныя спецыялісты сочаць за станам IT-інфраструктуры. Яны праводзяць планава-прафілактычныя работы з абсталяваннем і праграмным забеспячэннем, а таксама аналізуюць зваротную сувязь ад усіх карыстальнікаў. У працэсе эксплуатацыі IT-інфраструктуры ў арганізацыі з часам узнікаюць новыя бізнес-працэсы, арганізацыя развіваецца і разам з гэтым узнікае патрэбнасць у аптымізацыі IT-інфраструктуры.

Аптымізацыя прадугледжвае любыя змены IT-інфраструктуры. Яны могуць быць злучаны з наступнымі працэсамі:

- нарошчванне магутнасцяў у сувязі з развіццём арганізацыі (набыццё кампутараў, сервераў, ліцэнзій) укараненне новых сістэм, службаў і сэрвісаў у дзейсную інфраструктуру ў сувязі са зменамі запатрабаванняў бізнэсу (CRM , ERP, дакументаабарот);
- укараненне сродкаў абароны інфармацыі ў сувязі са зменамі заканадаўства або з'яўленнем новых напрамкаў бізнесу (неабходнасць забяспечваць захаванасць персанальных дадзеных);
- аптымізацыя хуткадзейнасці ў сувязі з павелічэннем карыстальнікаў і сэрвісаў.

Для якаснай аптымізацыі IT-інфраструктуры неабходна наймаць супрацоўнікаў у штат. І тут, як і ў любой бізнес-сферы, галоўную ролю будзе адыгрываць рэнтабельнасць мер. Прычым у выпадку ўцечкі дадзеных варта ўлічваць не толькі фінансавыя страты, але і іміджавыя, якія часам могуць быць больш сур'ёзнымі, чым фінансавыя. Знайсці рашэнне дапаможа кансультацыя кваліфікаваных адмыслоўцаў.

Літаратура

1. Абалкин, Л.И. Экономическая безопасность России: угрозы и их отражение / Л.И. Абалкин // Вопросы экономики. – 1994. – № 12 – С. 3 – 14;

2. Бахтеев, Д. В. Искусственный интеллект в следственной деятельности: задачи и проблемы / Д.В. Бахтеев // Российский следователь. – 2020. – N 9. – С. 3 – 6

3. Викторов, А.Ш. Введение в социологию безопасности / А.Ш. Викторов. – М.: Канон+, РООИ «Реабилитация», 2008. – 568 с.

4. Диев, В. С. Философская парадигма риска / В.С. Диев // ЭКО. 2008. № 11. с. 27-39.

5. Джафарли, В. Ф. Криминология кибербезопасности: в 5 томах / В. Ф. Джафарли; под ред. С. Я. Лебедева. – Москва: Проспект, 2021. – Том 1. Криминологическая кибербезопасность: теоретические, правовые и технологические основы. – 285 с.

6. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам. – М.: Горячая линия – Телеком, 2019 – 560 с.

7. Кузнецов, В.Н. Социология безопасности / В.Н. Кузнецов. – М.: Книга и бизнес, 2003. – 880 с.

8. Ларин, В. Безопасность развития и развитие безопасности / В. Ларин // Свободная мысль. – 2008. № 7. С. 40–43.

9. Личность преступника: характеристика, предупреждение формирования и криминализация: в 2 ч. / В.А. Ананич [и др.]; под общ. ред. В.А. Ананича; учреждение образования «Акад. М-ва внутр. Дел Респ. Беларусь. – Минск: Академия МВД, 2022. Ч. 1: общенаучные и теоретико-правовые основы изучения личности преступника. – 324 с.

10. Лойка, А.І. Філасофія кагнітыуных тэхналогій / А.І. Лойка. – Мінск: БНТУ, 2022 – 190 с.

11. Лойка, А.І. Філасофія лічбавай антрапалогіі / А.І. Лойка. – Мінск: БНТУ, 2023 – 210 с.

12. Лойко, А.И. Философия дизайна: цифровые технологии / А.И. Лойко. – Минск: БНТУ, 2023 – 119 с. https://rep.bntu.by/handle/data/126474

13. Лойко, А.И. Философия информации / А.И. Лойко. – Минск: БНТУ, 2021 – 372 с. https://rep.bntu.by/handle/data/106984

14. Лойко, А.И. Философия сознания / А.И. Лойко. – Минск: БНТУ, 2022 – 348 с. https://rep.bntu.by/handle/data/109344

15. Лойко, А.И. Философия цифровых технологий / А.И. Лойко. – Минск: БНТУ, 2022 – 207 с. https://rep.bntu.by/handle/data/109829

16. Лойко, А.И. Философия цифровой экономики / А.И. Лойко. – Минск: БНТУ, 2023 – 196 с. https://rep.bntu.by/handle/data/126237

17. Лойко, Л.Е. Коммуникативное действие в пространстве сетевой экономики и управления: Ю. Хабермас о социальной динамике / Л.Е. Лойко // Социальное пространство интернета: перспективы экономсоциологических исследований. – Минск: Право и экономика, 2014. – С. 190-192.

18. Лойко, Л.Е. Информационные системы и современные требования конфиденциальности / Л.Е. Лойко, А.И. Лойко // Информационные технологии в технических и социально-экономических системах. Сборник материалов научно-теоретической конференции. Минск, 22 апреля 2015 г. – Минск: РИВШ, 2015. – С. 363-365.

19. Лойко, Л.Е. Философская рефлексия трансформаций жизненного мира молодежи в информационном пространстве: социальные сети и сетевые сообщества / Л.Е. Лойко // Философское знание и вызовы цивилизационного развития. – Минск: Право и экономика, 2016. – 521 с. – С. 297-298.

20. Лойко, Л.Е. Аддитивные и информационные технологии в эволюции общества / Л.Е. Лойко, А.И. Лойко // Информационные технологии в технических, правовых, политических и социально-экономических системах. – Минск: РИВШ, 2017. – С. 330-331.

21. Лойко, Л.Е. Историческая память и информационные технологии / Л.Е. Лойко, А.И. Лойко // Информационные технологии в технических, экономических и социально-политических системах.– Минск: БНТУ, 2018.

22. Лойко, Л.Е. Философско-психологический аспект анализа достоверности информации в ходе процессуальных действий / Л.Е. Лойко // Проблемы борьбы с преступностью и подготовки кадров для правоохранительных органов. – Минск: УО «Академия МВД Республики Беларусь», 2019. – С. 335-336.

23. Лойко, Л.Е. Право и правосознание в эпоху неопределенности / Л.Е. Лойко // Глобальные риски цифровой эпохи и образы будущего. – М: Издательский центр РГУ нефти и газа (НИУ) имени И.М. Губкина, 2019. – С. 22.

24. Лойко, Л.Е. Модели социальной коммуникации в пространстве цифровой реальности / Л.Е. Лойко / Thesaurus: зборнік навуковых прац.– Вып. VII. Лічбавы свет. – Магілеу: Магілеускі інстытут МУС, 2020. – С. 100-109.

25. Лойко, Л.Е. Цифровизация систем социальной коммуникации: технологические и психологические компоненты / Л.Е. Лойко // Информационное общество: пределы и риски – прошлое, настоящее, будущее. – М: Издательский центр РГУ нефти и газа (НИУ) имени И.М. Губкина, 2020. – С. 241.

26. Лойко, Л.Е. Межкультурная коммуникация, историческая память и социиальные сети / Л.Е. Лойко // Thesaurus: зб. навук. пр. / Магілёўскі інстытут МУС. – Магілёў, 2021. – Вып. 8: Міжкультурная камунікацыя. – С. 111–121.

27. Лойко, Л.Е. Актуальные проблемы борьбы с психологией манипулятивных практик / Л.Е. Лойко // Проблемы борьбы с преступностью и подготовки кадров для правоохранительных органов. – Минск: УО «Академия МВД Республики Беларусь», 2021. – С. 330-331.

28. Лойко, Л.Е. Правовые компоненты национальной безопасности / Л.Е. Лойко // Современная политическая наука о траекториях развития государства, бизнеса и гражданского общества. – Минск, БГЭУ, 2021. – С. 35–38.

29. Лойко, Л.Е. Историческая ответственность, право и практики сетевых медиакоммуникаций / Л.Е. Лойко // Tempus et Memoria – 2021 – Т. 2 – № 1 – С. 12–17.

30. Лойко, Л.Е. Информационные технологии и правовые аспекты национальной безопасности / Л.Е. Лойко // Большая Евразия: Развитие, безопасность, сотрудничество. Ежегодник. Вып. 5. Ч. 1. – М.: ИНИОН РАН, 2022. – С. 215-217.

31. Лойко, Л.Е. Коммуникация в условиях короновирусной пандемии: цифровая доминанта / Л.Е. Лойко / Thesaurus: зборнік навуковых прац – Вып. X. Камунікацыя у эпоху постпандэміі. – Магілеу: Магілеускі інстытут МУС, 2022. – С. 92–98.

32. Лойко, Л.Е. Философия права в условиях цифровых трансформаций / Л.Е. Лойко // Современная политическая наука о траекториях развития государства, бизнеса и гражданского общества. – Минск: БГЭУ, 2023 – С. 311.

33. Нестеров, С. В. Безопасность как философско-правовая категория / С.В. Нестеров // Юридическая наука. Рязань, 2013, № 1. с. 11-13.

34. Ницевич, В.Ф. Национальная безопасность: теоретические основы, механизм обеспечения, региональная составляющая / В.Ф. Ницевич. – Орел: ОРАГС, 2000. – 324 с.

35. Проблемы борьбы с преступностью в условиях цифровизации: теория и практика: сборник статей XVIII Международной научно-практической конференции «Уголовно-процессуальные и криминалистические чтения на Алтае». — Вып. XVI / Министерство науки и высшего образования РФ, Алтайский государственный университет; отв. ред. С. И. Давыдов, В. В. Поляков. — Барнаул : Изд-во Алт. ун-та, 2020. — 276 с.

36. Проблемы правовой и технической защиты информации: сб. науч. ст. / АлтГУ; редкол.: В. В. Поляков (гл. ред.) [и др.]. - Барнаул: Изд-во АлтГУ. - Вып. 8. - 2020. - 128 с.

37. Рыбалкин, Н.Н. Философия безопасности / Н.Н. Рыбалкин. – М.: Московский психолого–социальный институт, 2006. – 296 с.

38. Связи с общественностью и медиавоздействие: учебное пособие / С.В. Масленченко, Е.Н. Мисун; Л.Е. Лойко, И.В. Ермолинский, Л.М. Беленкова; под общ. ред. С.В. Масленченко; учреждение образования

«Акад. М-ва внутр. дел Респ. Беларусь». – Минск: Академия МВД, 2018. – 153 с.

39. Стенькина, Е.Н. Кибербезопасность как основной фактор национальной и международной безопасности в отрасли экономики: тенденции, базовые понятия и термины / Е.Н. Стенькина. – Владивосток: Первое экономическое издательство, 2021 – 258 с.

40. Сушина, Т.Е. Перспективы и риски использования искусственного интеллекта в уголовном судопроизводстве / Т.Е. Сушина, А.А. Собенин // Российский следователь. - 2020. - N 6. - С. 21 - 25.

41. Трансформация права в цифровую эпоху: монография / АлтГУ; под ред. А. А. Васильева. - Барнаул: Изд-во АлтГУ, 2020. - 432 с.

42. Уголовно-процессуальные и криминалистические чтения на Алтае: Вып. XIV / Министерство науки и высшего образования РФ, Алтайский государственный университет; отв. ред. С. И. Давыдов, В. В. Поляков. – Барнаул: Изд-во Алтайского ун-та, 2017. – 118 с.

43. Уголовно-процессуальные и криминалистические чтения на Алтае: Вып. XV / Министерство науки и высшего образования РФ, Алтайский государственный университет; отв. ред. С. И. Давыдов, В. В. Поляков. – Барнаул : Изд-во Алт. ун-та, 2018. – 228 с.

44. Умрихина, Е. И. Безопасность как философско-правовая категория / Е.И. Умрихина // Философия права. Ростов-на-Дону: Изд-во Рост. юрид. ин-та МВД России, 2010, № 4. С. 53-56.

45. Экстремизм и терроризм в киберпространстве: угрозы миру и безопасности человечества: сб. материалов по итогам III Всерос. студенческой науч.-практ. оч.-заоч. видеоконф. / АлтГУ, Юрид. ин-т, Каф. уголовного права и криминологии, Регион. антитеррорист. науч.-метод. центр; ред.: В. А. Мазуров, М. А. Стародубцева. - Барнаул: Изд-во АлтГУ, 2020.- 203 с.

Змест