БАНКОВСКИЙ ПРОЦЕССИНГОВЫЙ ЦЕНТР

# ЗРОБІМ БЕЗНАЯЎНЫЯ АПЕРАЦЫІ БЯСПЕЧНЫМІ

## Банкаўскі працэсінгавы цэнтр аб бяспечным выкарыстанні плацежных картак

**Плацяжы з дапамогай банкаўскай карткі сталі звыклай справай кожнага дня для большасці жыхароў нашай краіны. На 9,5 мільёна беларусаў прыпадае больш за 15 мільёнаў банкаўскіх картак, і іх колькасць няўхільна расце.**

ААТ «Банкаўскі працэсінгавы цэнтр» ужо амаль 17 гадоў аказвае банкам краіны паслугі па тэхналагічнай і інфармацыйнай падтрымцы безнаяўных разлікаў па плацежных картках. За гэтыя гады сфера безнаяўных разлікаў у Рэспубліцы Беларусь і маштабы дзейнасці прадпрыемства значна змяніліся. Вельмі наглядна гэтыя змены дэманструе дынаміка паказчыкаў з першых гадоў работы прадпрыемства і іх значэнні за апошні год.

**ААТ «Банкаўскі працэсінгавы цэнтр» у лічбах**

| | 2003 год | 2018 год |
|---|---|---|
| Банкаўскія карткі | 761,7 тыс. | 9 434 тыс. |
| Фінансавыя аперацыі | 2,23 млн/ месяц | 113 млн/ месяц |
| Арганізацыі гандлю і сэрвісу | 558 | 71 451 |
| Плацежныя тэрміналы | 3 148 | 122 109 |
| Банкаматы | 350 | 2 446 |
| Інфакіёскі | 53 | 2 512 |

Для трымальнікаў картак дзейнасць Банкаўскага працэсінгавага цэнтра больш вядомая па выпадках форс-мажору, калі картка заблакавана ці згублена і трэба звяртацца ў кругласутачную службу падтрымкі.

Разам з тым нараўне з аказаннем паслуг працэсінгу (сукупнасці аперацый па апрацоўцы інфармацыі, якая выкарыстоўваецца пры здзяйсненні плацежных аперацый) вельмі важным для прадпрыемства з'яўляецца дзейнасць па забеспячэнні надзейнасці і бяспечнасці правядзення разлікаў. Прадпрыемства на пастаяннай аснове ажыццяўляе маніторынг аперацый з плацежнымі карткамі банкаў-кліентаў з мэтай выяўлення і папярэджання махлярскіх аперацый.

З актыўным развіццём сферы безнаяўных плацяжоў і з'яўленнем новых тэхналогій аплаты, якія паскараюць і спрашчаюць працэс аплаты тавараў і паслуг, павялічваецца і інтарэс махляроў да магчымасцяў пакарыстацца рэквізітамі картак у карыслівых мэтах.

Эксперты Банкаўскага працэсінгавага цэнтра адзначаюць павелічэнне колькасці махлярскіх аперацый з выкарыстаннем рэквізітаў картак побач з памяншэннем выпадкаў ажыццяўлення махлярскіх аперацый з выкарыстаннем падробленых картак.

Такія паводзіны махляроў тлумачацца развіццём ва ўсім свеце сацыяльнай інжынерыі, ростам кіберзлачыннасці, сферы інтэрнэт-камерцыі, а таксама імкненнем зламыснікаў схаваць махлярскія аперацыі на невялікія сумы пад выглядам легітымных аперацый трымальніка, што ў сваю чаргу павышае прывабнасць атрымання «хуткіх і лёгкіх» даходаў.

Па выніках 2018 года колькасць махлярскіх аперацый па картках банкаў, якія абслугоўваюцца ў Банкаўскім працэсінгавым цэнтры, па тыпе махлярства размеркавалася наступным чынам:

95 працэнтаў махлярскіх аперацый прыпадае на махлярства з выкарыстаннем рэквізітаў картак;

3 працэнты незаконных аперацый з банкаўскімі плацежнымі карткамі прыпадае на аперацыі па падробленых картках;

2 працэнты прыпадае на махлярскія аперацыі па згубленых ці скрадзеных картках.

У канцы 2018 года павялічылася колькасць махлярскіх аперацый з выкарыстаннем рэквізітаў картак з прымяненнем тэхналогіі 3D Secure, што выклікана ўсплёскам фішынгу (махлярства, мэтай якога з'яўляецца атрыманне доступу да лагінаў і пароляў) з прымяненнем сацыяльнай інжынерыі ў адносінах да даверлівых і бесклапотных грамадзян, якія выдаюць махлярам усе неабходныя для ажыццяўлення плацяжоў ці пераводаў рэквізіты, уключаючы даныя для доступу да сістэм дыстанцыйнага банкаўскага абслугоўвання і паролі 3D Secure.

Стабільна высокі ўзровень колькасці кампраметацыі даных трымальнікаў картак з дапамогай шкоднага праграмнага забеспячэння, а таксама на разнастайных сайтах з сумнеўнай рэпутацыяй.

Летась лідарамі па выкарыстанні падробленых картак у банкаматах былі краіны Азіі: 64 працэнты — Індыя, 28 — Інданезія. Два працэнты прыпадае на долю ЗША і шэсць працэнтаў, што засталіся, — на Расійскую Федэрацыю, Дамініканскую Рэспубліку і Тайвань.

А ў топ-спіс краін, у якіх карткі беларускіх банкаў падвяргаліся скімінгу (крадзеж даных карткі для наступнага вырабу падробнай), уваходзяць Расійская Федэрацыя, Украіна, Турцыя, Італія, Вялікабрытанія, Балгарыя. У Санкт-Пецярбургу скімінгу падвяргаліся 68 працэнтаў ад агульнай колькасці картак, па якіх прайшлі махлярскія аперацыі з выкарыстаннем падробленых картак у 2018 годзе.

Дзякуючы рабоце, што пастаянна праводзіцца Банкаўскім працэсінгавым цэнтрам сумесна з банкамі і плацежнымі сістэмамі па мінімізацыі ўзроўню махлярства з выкарыстаннем банкаўскіх плацежных картак, колькасць махлярскіх аперацый ва ўстройствах банкаў, падключаных да прадпрыемства, у 2018 годзе знізілася на 13 працэнтаў.

Разам з тым і ад паводзін саміх трымальнікаў карткі залежыць бяспечнасць безнаяўных аперацый.

Банкаўскі працэсінгавы цэнтр напамінае асноўныя правілы па бяспечным выкарыстанні банкаўскіх плацежных картак.

Выкананне гэтых правілаў звядзе да мінімуму рызыку стаць ахвярай махляра.

### Выконвайце асноўныя правілы карыстання карткай

Ніколі не ўказвайце свой ПІН-код на адваротным боку карткі і не захоўвайце яго разам з карткай.

Ніколі не ўводзьце даныя сваёй банкаўскай плацежнай карткі (нумар, тэрмін дзеяння, трохзначны код бяспекі CVV2/CVC2 на адваротным боку карткі, банкаўскі код пацвярджэння аперацыі з СМС-паведамлення) на неправераных сайтах, якія выклікаюць у вас падазрэнне.

### Завядзіце асобную картку для здзяйснення аперацый у сетцы Інтэрнэт і для паездак за мяжу

Для здзяйснення плацежных аперацый у сетцы Інтэрнэт завядзіце картку да асобнага рахунку, які вы будзеце папаўняць на неабходную суму для ажыццяўлення пэўнага плацяжу непасрэдна перад яго ажыццяўленнем.

Тым, хто плануе паездку ў іншую краіну (асабліва ў гарады павышанай рызыкі, такія як Санкт-Пецярбург, Адэса і Кіеў), рэкамендуем заводзіць асобную картку (абавязкова перавыпускайце картку пасля наведвання краін з сумнеўнай рэпутацыяй), а знаходзячыся ў ёй, карыстацца банкаматамі, размешчанымі непасрэдна ў аддзяленнях банкаў; ажыццяўляць пакупкі з дапамогай карткі толькі ў буйных магазінах, пры гэтым не выпускаць яе з поля зроку.

**Устанавіце ліміты (абмежаванні) на правядзенне аперацый па картцы,** гэта дазволіць знізіць страты ад махлярства ў выпадку крадзяжу/страты карткі ці кампраметацыі яе рэквізітаў.

### Падключыце паслугу дадатковай аўтэнтыфікацыі 3D Secure і СМС-інфармавання

Пры здзяйсненні пэўнай плацежнай аперацыі ў сетцы Інтэрнэт на нумар вашага мабільнага тэлефона будзе прыходзіць спецыяльны код, які трэба ўвесці, каб правесці гэтую аперацыю.

Памятайце аб тым, што **ніколі не варта нікому паведамляць пароль 3D Secure альбо сеансавыя ключы.**

Гэтыя паролі можна выкарыстоўваць толькі для пацвярджэння аперацыі ў сетцы Інтэрнэт, якая праводзіцца непасрэдна вамі.

Падключэнне **СМС-інфармавання дазволіць вам** не толькі **кантраляваць рух грашовых сродкаў** па рахунку, але і **аператыўна рэагаваць** на спробы здзяйснення махлярскіх аперацый.

### Не ажыццяўляйце ўвод пароля 3D Secure, калі адсутнічае бяспечнае злучэнне па пратаколе https

У апошні час усё большую папулярнасць набывае спосаб крадзяжу даных пры дапамозе выкарыстання вэб-рэсурсаў, якія цалкам імітуюць рэсурсы вядомых банкаў, плацежных сістэм альбо іншых ведамстваў, што выклікаюць давер у карыстальнікаў. Гэта так званыя фішынгавыя сайты — махлярскія вэб-рэсурсы, што выманьваюць рэквізіты банкаўскіх плацежных картак.

### Аплачвайце толькі на надзейных сайтах

Правядзіце праверку сайта, загадзя вывучыўшы водгукі карыстальнікаў інтэрнэт-рэсурсу, які вас цікавіць.

*З актыўным развіццём сферы безнаяўных плацяжоў і з'яўленнем новых тэхналогій, якія паскараюць і спрашчаюць працэс аплаты тавараў і паслуг, павялічваецца і інтарэс махляроў да магчымасцяў пакарыстацца рэквізітамі картак у карыслівых мэтах.*

Не ўводзьце даныя карткі на сайтах, што прапануюць паўдзельнічаць у разнастайных акцыях з наступнай выплатай грашовых прызоў. Настойваюць на пераводзе на рахунак? Падумайце двойчы!

Любая просьба перавесці грашовыя сродкі для атрымання выйгрышу павінна насцярожыць вас.

З «акна», якое з'явілася (усплыло) на экране ноўтбука ці тэлефона, вы даведаліся, што выйгралі прыз?

Падумайце, а ці не выйгралі вы вірус?

### Будзьце пільнымі са званкамі, што прапануюць вам фінансавыя інвестыцыі

Калі вам тэлефануюць і прапануюць інвеставаць з высокім даходам у акцыі, аблігацыі, крыптавалюту, каштоўныя металы, то будзьце пільныя, адхіляйце званкі з такімі прапановамі.

Запытайце незалежнай фінансавай парады, перш чым аддаваць свае сродкі. Вывучыце інфармацыю ў інтэрнэце.

І пры неабходнасці звярніцеся ў міліцыю.

**У апошні час пачасціліся выпадкі вішынгу** (разнавіднасць тэлефоннага махлярства) з мэтай выманьвання ў трымальнікаў банкаўскіх плацежных картак асабістай інфармацыі, нумара карткі, логіна і пароля ад сістэм дыстанцыйнага банкаўскага абслугоўвання, СМС-кодаў і іншага.

Зламыснікі могуць называць сябе работнікамі банка альбо Службы сэрвісу кліентаў ААТ «Банкаўскі працэсінгавы цэнтр», выкарыстоўваць закрытыя тэлефонныя нумары альбо праграмы-ананімайзеры, што падмяняюць нумары тэлефонаў на рэальныя нумары, размешчаныя на афіцыйных рэсурсах арганізацый.

ААТ «Банкаўскі працэсінгавы цэнтр» напамінае, што пры тэлефанаванні **работнікі банка альбо Службы сэрвісу кліентаў ніколі не запытваюць інфармацыю пра поўны нумар банкаўскай плацежнай карткі, тэрмін дзеяння, CVC/CVV-код, паролі 3D Secure, аднаразовыя пацвярджальныя коды.**

**Ні ў якім разе не паведамляйце інфармацыю аб рэквізітах банкаўскай карткі, логінах і паролях, СМС-кодах, сеансавых ключах да інтэрнэт-банкінгу і мабільных праграм.**

У выпадку з'яўлення званкоў з просьбамі ўдакладніць вашы даныя неадкладна звярніцеся ў банк на нумары тэлефонаў, што ўказаны на афіцыйным сайце.

Пры звяртанні сяброў праз сацыяльныя сеткі з просьбай аб дапамозе ў пераводзе грашовых сродкаў на картку альбо аплаце мабільнай сувязі, білетаў і да т. п. пераканайцеся, што асоба, якая звярнулася праз старонку ў сацыяльнай сетцы, з'яўляецца менавіта тым, за каго сябе выдае.

*Давайце разам зробім безнаяўныя аперацыі больш бяспечнымі!*

### Карыстайцеся інтэрнэт-банкінгам толькі на абароненым камп'ютары з абмежаваным фізічным доступам да яго пабочных асоб

Калі вы выкарыстоўваеце агульнадаступныя камп'ютары, памятайце аб вялікай верагоднасці таго, што даныя вашай плацежнай карткі могуць быць скрадзены падчас пакупак у інтэрнэце.

На такіх камп'ютарах можа быць усталявана праграмнае забеспячэнне для крадзяжу інфармацыі (кейлогеры), якое фіксуе ўсе націсканні на клавішы, у тым ліку нумар вашай карткі і рэгістрацыйныя звесткі.

Акрамя таго, **не выкарыстоўвайце адкрытыя сеткі Wi-Fi пры выкананні плацежных аперацый у інтэрнэце, у тым ліку не заходзьце ў інтэрнэт-банкінг,** нават калі вы карыстаецеся сваім персанальным камп'ютарам ці мабільным тэлефонам.

Да агульнадаступнай сеткі могуць таксама падключацца зламыснікі і перахопліваць інфармацыю падчас яе перадачы.

### Не адкрывайце камп'ютарныя файлы ці спасылкі, атрыманыя з ненадзейных крыніц

Не націскайце на падазроныя спасылкі, атрыманыя з пісем электроннай пошты і сацыяльных сетак, асабліва ад незнаёмых адпраўшчыкаў.

### Не ўсталёўвайце на мабільныя прылады праграмы з сумнеўных крыніц

Спампоўвайце праграмы толькі з афіцыйных магазінаў (PlayMarket, WindowsPhoneStore, AppStore) і тых крыніц, у надзейнасці якіх вы пераканаены.

Пры спампоўванні праграмы з неафіцыйных крыніц праверце перад загрузкай наяўнасць негатыўных водгукаў аб праграме, памылак друку ў апісанні, а таксама звярніце ўвагу на звесткі, якія неабходна перадаць пры ўсталяванні праграмы.

### Выкарыстоўвайце апошнія версіі браўзераў. Абнаўляйце антывіруснае ПЗ

Каб быць упэўненым, што ваш камп'ютар або мабільнае прыстасаванне бяспечныя для выканання плацежных аперацый у інтэрнэце, своечасова абнаўляйце браўзеры, а таксама ўсталюйце на вашы прылады аўтарытэтнае антывіруснае праграмнае забеспячэнне.

Заўсёды інфармуйце аб спробах махлярства праваахоўныя органы, нават калі вы не сталі ахвярай падману.

ААТ «Банкаўскі працэсінгавы цэнтр» пастаянна ажыццяўляе пошук і распрацоўку дадатковых мер бяспекі ў адпаведнасці з міжнароднымі стандартамі, сочыць за тэндэнцыямі ў сферы безнаяўных плацяжоў, а таксама рэгулярна абнаўляе рэкамендацыі па бяспечным выкарыстанні банкаўскіх плацежных картак.

Давайце разам зробім безнаяўныя аперацыі больш бяспечнымі!

**Інфармацыя і здымкі атрыманы ад ААТ «Банкаўскі працэсінгавы цэнтр».**

УНП 190381773

## Расказваем пра ААТ «Банкаўскі працэсінгавы цэнтр»

Банкаўскі працэсінгавы цэнтр пачаў сваю работу ў Мінску ў 2002 годзе.

Ён створаны шэрагам буйных банкаў і прамысловых прадпрыемстваў Рэспублікі Беларусь з мэтай шырокага ўкаранення ў краіне безнаяўных разлікаў з выкарыстаннем банкаўскіх плацежных картак і развіцця інфраструктуры абслугоўвання трымальнікаў картак.

ААТ «Банкаўскі працэсінгавы цэнтр» аказвае комплекс паслуг па працэсінгу аперацый з банкаўскімі плацежнымі карткамі, у тым ліку аўтарызацыю картачных аперацый, вядзенне ідэнтыфікацыйных баз даных картак, банкаматаў і тэрміналаў, персаналізацыю картак, працэсінг і кірынг аперацый з карткамі плацежных сістэм, што дзейнічаюць на тэрыторыі Рэспублікі Беларусь, а таксама падключэнне і абслугоўванне банкаматаў і тэрміналаў у пунктах продажу.

Усе паслугі, што прапаноўваюцца, сертыфікаваны на поўную адпаведнасць патрабаванням і правілам плацежных сістэм.

ААТ «Банкаўскі працэсінгавы цэнтр» — спецыялізаваны цэнтр па інфармацыйна-тэхналагічным забеспячэнні безнаяўных разлікаў з выкарыстаннем банкаўскіх картак айчыннай плацежнай сістэмы БЕЛКАРТ і міжнародных сістэм VISA International і MasterCard WorldWide, UnionPay, American Express, што дзейнічаюць на тэрыторыі Рэспублікі Беларусь.

Апаратна-праграмны комплекс і вытворчыя памяшканні прадпрыемства адпавядаюць тэхналагічным патрабаванням і правілам бяспекі пры ажыццяўленні фінансавых транзакцый, якія прад'яўляюцца плацёжнымі сістэмамі да працэсінгавых цэнтраў.

Кадравая палітыка цэнтра будуецца ў адпаведнасці са стратэгіяй развіцця прадпрыемства і накіравана на прыцягненне і ўтрыманне высокакваліфікаванага персаналу, на фарміраванне адзінай каманды.