АГЕНЦИЈА ЗА БАНКАРСТВО РЕПУБЛИКЕ СРПСКЕ

УПУТСТВО
ЗА ИЗВЈЕШТАВАЊЕ О
УПРАВЉАЊУ ИНФОРМАЦИОНИМ СИСТЕМИМА У БАНКАМА

Бања Лука, фебруар 2021. године

Увод

Упутство за извјештавање о управљању информационим системима у банкама доноси се на основу члана 5. став 1. тачка б, члана 22. став 1. тачка ђ. и члана 37. Закона о Агенцији за банкарство Републике Српске ("Службени гласник Републике Српске" број 59/13 и 04/17), члана 6. став 1. тачка б. и члана 22. став 4. тачка л. Статута Агенције за банкарство Републике Српске ("Службени гласник Републике Српске" број 63/17), те члана 32. став 1. Одлуке о управљању информационим системима у банкама ("Службени гласник Републике Српске" број 116/17).

I ОПШТЕ ОДРЕДБЕ

Предмет

Члан 1.

Овим упутством прописује се извјештавање, садржај и начин попуњавања, као и динамика достављања извјештајних образаца које је банка дужна да доставља Агенцији за банкарство Републике Српске (у даљем тексту: Агенција).

Структура и правила

Члан 2.

(1) У складу са чланом 32. став 1. Одлуке о управљању информационим системима у банкама, банка је дужна да Агенцији доставља сљедеће извјештаје:

1) Извјештај Општи подаци на следећим обрасцима:
   1. ОП.1 - Општи подаци о организационој структури,
   2. ОП.2 - Општи подаци о одговорним особама,
   3. ОП.3 - Општи подаци о флуктуацији кадрова,
   4. ОП.4 - Општи подаци о ванјским ИТ сарадницима,
   5. ОП.5 - Општи подаци о интерној ревизији информационог система.
2) Извјештај Општи подаци о информационом систему на следећим обрасцима:
   1. ИС.1 - Инфраструктура система,
   2. ИС.2 - Сервери,
   3. ИС.3 - Мрежни уређаји,
   4. ИС.4 - Радне станице,
   5. ИС.5 - Банкомати,
   6. ИС.6 - Системи без подршке произвођача,
   7. ИС.7 - Удаљени приступ информационом систему.
3) Извјештај Стратегија и оперативни планови информационог система на обрасцу СОП - Стратешки и оперативни циљеви.
4) Извјештај Управљање ризицима информационог система на обрасцу УРИС - План мјера за поступање са процијењеним ризицима информационог система.
5) Извјештај Безбједност информационог система на обрасцу ПЕН - Резултати пенетрационих тестирања/ тестова рањивости.
6) Извјештај Интерна ревизија информационог система на следећим обрасцима:
   1. ИТР.1 - Преглед планираних и обављених ревизија информационог система,
   2. ИТР.2 - Преглед препорука/налога.
7) Извјештај Буџет за информациони систем и технологије на следећим обрасцима:
   1. БИС.1 - ИКТ буџет,
   2. БИС.2 - Fintech буџет.
8) Извјештај Значајне промјене у информационом систему банке на обрасцу ПИС - Значајне промјене у информационом систему.
9) Извјештај Преглед инцидената у информационом систему банке на следећим обрасцима:
   1. ПИ.1 - Категоризација инцидената,
   2. ПИ.2 - Преглед инцидената по пословним процесима,
   3. ПИ.3 - Преглед оперативних инцидената,

4. ПИ.4 - Сајбер инциденти,
5. ПИ.5 - Електронско банкарство и картично пословање - могуће злоупотребе.

10) Извјештај Електронско банкарство на сљедећим обрасцима:
1. ЕБ.1 - Обим електронског банкарства,
2. ЕБ.2 - Елементи аутентификације и ауторизације у електронском банкарству.

11) Извјештај Картично пословање на сљедећим обрасцима:
1. КП.1 - Обим картичног пословања,
2. КП.2 - Број POS и ATM уређаја.

12) Извјештај Употреба нових технологија (FinTech) на обрасцу ФТ - Обим кориштења нових технологија (FinTech).

13) Извјештај План опоравка информационог система на сљедећим обрасцима:
1. ПОИС.1 - Основни подаци о тестирању плана опоравка информационог система,
2. ПОИС.2 - Сценарији за тестирање,
3. ПОИС.3 - Преглед тестираних пословних процеса,
4. ПОИС.4 - Остали подаци.

(2) Форма извјештајних образаца из става 1. овог члана утврђена је и објављена на званичној интернет страници Агенције.

II СТРУКТУРА ИЗВЈЕШТАЈНИХ ОБРАЗАЦА

Извјештај Општи подаци

Члан 3.

(1) Извјештај Општи подаци садржи основне податке о броју запослених у банци, организационој јединици за управљање информационим системом и организационој јединици за безбједност информационог система, флуктуацији кадрова у овим организационим јединицама, те ванъским ИТ сарадницима и интерној ревизији информационог система.

(2) Извјештај Општи подаци доставља се на пет извјештајних образаца:
1) ОП.1 - Општи подаци о организационој структури,
2) ОП.2 - Општи подаци о одговорним особама,
3) ОП.3 - Општи подаци о флуктуацији кадрова,
4) ОП.4 - Општи подаци о ванъским ИТ сарадницима,
5) ОП.5 - Општи подаци о интерној ревизији информационог система.

(3) Извјештајни образац ОП.1 - Општи подаци о организационој структури садржи податке о броју запослених у банци, организационој јединици за управљање информационим системом и организационој јединици за безбједност информационог система, те називима ових организационих јединица. Број запослених у јединици за безбједност информационог система се односи искључиво на запослене који се баве безбједношћу информационог система, не односи се уопштено на безбједност банке, као што је физичка безбједност и сл.

(4) Извјештајни образац ОП.2 - Општи подаци о одговорним особама садржи податке о лицима одговорним за управљање и безбједност информационог система (члан управе надлежан за управљање информационим системом, члан управе надлежан за безбједност информационог система, руководилац организационе јединице за управљање информационим системом и лице одговорно за безбједност информационог система). Потребно је попунити следеће податке: име и презиме, назив радног мјеста, стручна спрема и датум почетка обављања функције.

(5) Извјештајни образац ОП.3 - Општи подаци о флуктуацији кадрова садржи податке о запосленима који су у извјештајном периоду започели, прекинули радни однос или промијенили радно мјесто унутар организационих јединица за информациони систем или безбједност информационог система. Потребно је попунити следеће податке: име и презиме, назив радног мјеста, занимање, врста промјене и датум промјене. У колони Врста промјене изабрати једну од понуђених опција: одлазак, долазак или промјена унутар банке. Уколико се ради о промјени унутар банке колона Назив радног мјеста попуњава се на следећи начин: назив новог радног мјеста (назив старог радног мјеста).

(6) Извјештајни образац ОП.4 - Општи подаци о ванъским ИТ сарадницима садржи податке о свим сарадницима (правна и физичка лица) који пружају услуге из области информационих технологија. Потребно је попунити следеће податке: назив правног или физичког лица, опис послова, датум почетка обављања услуге, датум потписивања уговора и период трајања уговора (исказан у мјесецима).

(7) Извјештајни образац ОП.5 - Општи подаци о интерној ревизији информационог система садржи податке о лицима која обављају интерну ревизију ИС. Уколико је банка екстернализовала интерну ревизију информационог система потребно је навести назив пружаоца услуга. За лица која обављају ревизију информационог система потребно је навести име и презиме, занимање, сертификат релевантан за обављање ревизије, те период ангажовања (датум од – датум до).

Извјештај Општи подаци о информационом систему банке

Члан 4.

(1) Извјештај Општи подаци о информационом систему банке садржи најзначајније податке о информационом систему који се односе на: инфраструктуру, сервере, мрежне уређаје, радне станице и банкомате, те правна и физичка лица којима је одобрен приступ информационом систему банке и податке о системима којима је истекла подршка произвођача или истиче у наредној години.

(2) Извјештај Општи подаци о информационом систему банке доставља се на седам извјештајних образаца:
1) ИС.1 - Инфраструктура система,
2) ИС.2 - Сервери,
3) ИС.3 - Мрежни уређаји,
4) ИС.4 - Радне станице,
5) ИС.5 - Банкомати,
6) ИС.6 - Системи без подршке произвођача,
7) ИС.7 - Удаљени приступ.

(3) Извјештајни образац ИС.1 - Инфраструктура система садржи податке о броју рачунарских центара који се налазе у банци (власништво банке) и изван банке (уколико се ради о екстернализацији те су у власништву пружаоца услуга), укључујући резервни рачунарски центар, податке о броју критичних/кључних ИТ система (утврђени у оквиру анализе утицаја на пословање) и апликација које подржавају критичне/кључне пословне процесе. Потребно је одвојено навести број апликација и помоћних алата развијених у MS Excel-у, MS Access-у и сличним алатима, које користе крајњи корисници (нпр. радне табеле/прорачуни у MS Excel-у,...) и при том подржавају критичне/кључне пословне процесе, укључујући и извјештавање.

(4) Извјештајни образац ИС.2 - Сервери садржи податке о свим серверима који подржавају критичне/ кључне пословне процесе, укључујући и сервере који се налазе код пружаоца услуга и на резервној локацији. За сваки сервер навести: назив (ознака сервера у информационом систему банке), намјену (нпр. апликативни сервер кључне банкарске апликације, бекап сервер,...), врсту (физички/виртуални), назив и верзију оперативног система, локацију на којој се налази (примарни или резервни рачунарски центар/град/ознака држава).

(5) Извјештајни образац ИС.3 – Мрежни уређаји садржи податке о свим мрежним уређајима који подржавају критичне/ кључне пословне процесе, укључујући и уређаје који се налазе код пружаоца услуга и на резервној локацији. Уређаје груписати по врсти, моделу, произвођачу, оперативном систему/фирмверу који користи и локацији (банка или пружалац услуге), те унијети број уређаја у колону Количина. У колони Локација се уноси назив пружаоца услуга, уколико се уређај налази код пружаоца услуга, у супротном се подразумијева да се уређај налази унутар банке и ова колона се не попуњава.

(6) Извјештајни образац ИС.4 – Радне станице садржи податке о укупном броју радних станица у употреби, груписане према оперативном систему који се на њима користи.

(7) Извјештајни образац ИС.5 – Банкомати садржи податке о броју банкомата који су груписани према произвођачу, оперативном систему и софтверу који је се користи за рад банкомата, те

чињеници да ли је банкомат у власништву банке или пружаоца услуга, да ли је екстернализована услуга одржавања и/или надзора банкомата. Уколико је нека од наведених услуга екстернализована навести назив пружаоца услуга.

(8) Извјештајни образац ИС.6 – Системи без подршке произвођача садржи податке о свим системима (нпр. оперативни системи, системи за управљање базама података, мрежни оперативни систем, ...) којима је истекла подршка произвођача или истиче у наредној години. За сваки систем навести датум истека подршке, број и врсту уређаја (сервер, мрежни уређај, радна станица, банкомат,...) на којима се користи, те планирани датум замјене.

(9) Извјештајни образац ИС.7 - Удаљени приступ садржи податке о свим ванјским компанијама и сарадницима којима је одобрен удаљени приступ информационом систему банке, врсти приступа (site to site или client to site) и типу примјењене енкрипцију. За ванјске компаније потребно је навести број запослених који имају приступ информационом систему банке, те да ли је овај приступ персонализован.

Извјештај Стратегија информационог система и оперативни планови

Члан 5.

(1) Извјештај Стратегија информационог система и оперативни планови садржи податке о стратешким циљевима банке и повезаним стратешким циљевима информационог система, те активностима предвиђеним годишњим оперативним плановима.

(2) Доставља се на извјештајном обрасцу СОП - Стратешки и оперативни циљеви. Извјештајни образац СОП садржи податке о свим активностима у извјештајној и наредној пословној години, које подржавају реализацију стратешких циљева банке и информационог система. За сваку активност поребно је унијети планиране временске рокове и реализоване, који представљају стварни почетак, односно завршетак активности, те статус активности на дан достављања извјештајног обрасца.

Извјештај Управљање ризицима информационог система

Члан 6.

(1) Извјештај Управљање ризицима информационог система садржи резултате годишње процјене ризика информационог система за извјештајну годину у складу са чланом 10. Одлуке о управљању информационим системима у банкама. Доставља се на извјештајном обрасцу УРИС - План мјера за поступање са ризицима информационог система.

(2) Извјештајни образац УРИС - План мјера за ублажавање ризика информационог система садржи податке о свим идентификованим ризицима информационог система. За сваки ризик се наводи кратак опис ризика, ниво ризика, начин третирања, приједлог мјера, те иницијални рок за примјену мјера. Уколико се продужи рок за имплементацију мјера у колону Продужење рока унијети датум новог рока.

(3) У колону Ниво ризика се уноси оцјена 1 до 4, при чему оцјена 1 представља најнижи ниво ризика, а оцјена 4 највиши ниво ризика. Уколико се оцјене нивоа ризика према интерној методологији банке разликују од претходно наведених, потребно је да банка изврши адекватно мапирање у наведене оцјене. Уколико је банка у процесу процјене ризика утврдила да ризик није прихватљив, за тај ризик у колону Приједлог мјера уноси кратак опис одабраних мјера. У колону Статус се уноси статус реализације одабраних мјера на последњи дан извјештајног периода (1-отворен, 2- у току, 3-затворен). Ако су мјере реализоване попунити колону Датум имплементације мјера.

Извјештај Безбједност информационог система

Члан 7.

(1) Извјештај Безбједност информационог система садржи податке о резултатима пенетрационих тестирања/провјера рањивости. Доставља се на извјештајном обрасцу ПЕН - Резултати проведних пенетрационих тестирања/тестова рањивости.

(2) Извјештајни образац ПЕН - Резултати проведних пенетрационих тестирања/тестова рањивости садржи податке о свим идентификованим рањивостима у извјештајном периоду, као и

рањивостима које су утврђене претходним тестирањима, а нису још отклоњене. За сваку идентификовану рањивост уносе се подаци о тестирању: јединствена ознака и назив, врста тестирања (интерни тест уколико је проведен од стране банке или екстерни тест од стране ангажоване фирме), назив лица или фирме која је провела тестирање, период тестирања, затим кратак опис, ниво ризика (низак, средњи, висок и критичан), начин третирања ризика, опис мјера за отклањање, иницијални рок за отклањање и статус на последњи дан извјештајног квартала. Уколико је продужен рок за имплементацију мјера унијети нови рок (колона Продужење рока). За рањивости које су отклоњене унијети Датум имплементације мјера.

Извјештај Интерна ревизија информационог система

Члан 8.

(1) Извјештај Интерна ревизија информационог система садржи податке о планираним и обављеним интерним ревизијама информационог система у извјештајном периоду, као и препорукама/налазима издатим у току обављених ревизија.

(2) Извјештај Интерна ревизија информационог система доставља се на следећим обрасцима:
1) ИТР.1 - Преглед планираних и обављених ревизија информационог система,
2) ИТР.2 - Преглед препорука/налога.

(3) Извјештајни образац ИТР.1 - Преглед планираних и обављених ревизија информационог система садржи податке о планираним и обављеним интерним ревизијама информационог система у извјештајном периоду. За сваку ревизију уноси се јединствена ознака, која се досљедно користи на извјештајном обрасцу ИТР. 2 и период трајања ревизије. Уколико ревизија није завршена у извјештајном периоду колона Крај се не попуњава. Потребно је назначити које области информационог система су предмет ревизије у извјештајном периоду. За све области информационог система обавезно се наводи ревизијски циклус у складу са методологијом банке (да ли се ревизија обавља сваке године, једном у двије или једном у три године) и пословна годину у којој је та област последњи пут ревидирана, иако нису предмет ревизије у извјештајном периоду.

(4) Извјештајни образац ИТР.2 - Преглед препорука/налога садржи податке о свим препорукама/налозима који су издати у извјештајном периоду или су издати у претходним ревизијама (интерна ИТ ревизија, спољна ревизија информационог система, ревизија од стране регулатора), а још нису извршени. За сваку препоруку/ налог уносе се подаци о ревизији (јединствена ознака и врста ревизије), датум издавања, кратак опис, ниво ризика, приједлог мјера за отклањање утврђених незаконитости и неправилности те недостатака и слабости утврђених током обављања ревизије и рок за имплементацију мјера. За препоруке/налоге који су издати током претходних ревизија уноси се статус извршења мјера и информације о статусу извршења мјере (колона Праћење извршења мјера), те уколико је продужен рок за имплементацију мјера уноси се нови рок (колона Продужење рока). За мјере које су имплементиране уноси се датум имплементације мјера. У колону Ниво ризика се уноси оцјена 1 до 4, при чему оцјена 1 представља најнижи ниво ризика, а оцјена 4 највиши ниво ризика. Уколико се оцјене нивоа ризика према интерној методологији банке разликују од претходно наведених, потребно је да банка изврши адекватно мапирање у наведене оцјене.

Извјештај Буџет за информациони систем и технологије

Члан 9.

(1) Извјештај Буџет за информациони систем и технологије садржи податке податке о планираним и реализованим буџетима за информационо-комуникационе технологије и Fintech.

(2) Извјештај Буџет за информациони систем и технологије доставља се на следећим обрасцима:
1) БИС.1 - ИКТ буџет,
2) БИС.2 - Fintech буџет.

(3) Извјештајни образац БИС.1 - ИКТ буџет садржи податке о планираним и реализованом трошковима/инвестицијама за извјештајну годину, као и за наредну годину. Ставке су груписане у пет категорија (лиценце, софтвер, хардвер, комуникационе линије, остало). За сваку ставку потребно је навести краћи опис, врсту (трошак/инвестиција), назив и ЈИБ пружаоца

услуге/добављача (уколико је примјењиво). Колоне Интерно се попуњавају уколико се ради о интерним плаћањима унутар банке.

(4) Извјештајни образац БИС.*2* – FinTech буџет садржи податке о буџету за сва Fintech рјешења која банка користи или развија и планира користити у наредној пословној години. У табелу се уноси назив Fintech рјешења, краћи опис, врста напредне технологије на којој се заснива, пословни процес у којем се користи, статус (имплементирано, тестна фаза, развојна фаза, у плану) и датум имплементације. Уколико банка не развија самостално Fintech рјешење потребно је попунити колоне Назив пружаоца услуге/добављача и Врста односа са пружаоцем услуга.

Извјештај Значајне промјене у информационом систему банке

Члан 10.

(1) Извјештај Значајне промјене у информационом систему банке садржи податке о свим значајним измјенама у информационом систему (нпр. замјена кључних мрежних уређаја, измјене на кључним пословним апликацијама, миграција примарног или резервног рачунарског центра,...) у извјештајном периоду. Доставља се на извјештајном обрасцу ПИС - Значајне промјену у информационом систему.

(2) Извјештајни образац ПИС - Значајне промјену у информационом систему садржи податке о дијелу информационог система на који се односи промјена (нпр. главна банкарска апликација, систем за подршку картичном пословању, фајервол, рачунарски центар, резервна локација,...), кратак опис измјене, разлог за измјену (закон, регулатор, налог ревизора, унапређење, инцидент, грешка у раду,...), начин провођења промјене (интерно/екстерно) и статус (завршена, у току, отказана) на последњи дан извјештајног периода.

Извјештај Преглед инцидената у информационом систему банке

Члан 11.

(1) Извјештај Преглед инцидената у информационом систему банке садржи податке о категоризацији инцидената према интерној методологији банке, те броју инцидента и догађаја који су се десили у раду информационог система у извјештајном периоду, а нису класификовани као инцидент.

(2) Извјештај Преглед инцидената у информационом систему доставља се на следећим обрасцима:
1) ПИ.1 - Категоризација инцидената,
2) ПИ.2 - Преглед инцидената по пословним процесима,
3) ПИ.3 - Преглед оперативних инцидената,
4) ПИ.4 - Сајбер инциденти,
5) ПИ.5 - Електронско банкарство и картично пословање - могуће злоупотребе.

(3) Извјештајни образац ПИ.1 - Категоризација инцидената садржи податке о дефинисаним нивоима инцидената. Ниво I означава инциденте највишег ризика, а ниво IV најнижег. Уколико се категоризација инцидената према интерној методологији банке разликује од претходно наведеног, потребно је да банка изврши адекватно мапирање у наведене нивое. За сваку категорију потребно је навести очекивано вријеме рјешавања инцидента.

(4) Извјештајни образац ПИ.2 - Преглед инцидената по пословним процесима садржи податке о броју инцидената и догађаја који нису класификовани као инцидент и њиховог утицаја на ИТ сегмент/пословни процес који је наведен у табели, при том треба назначити да ли се ради о критичном/кључном сегменту и да ли је ИТ подршка или сам сегмент екстернализован. Уколико се инцидент/догађај десио у ИТ сегменту који није наведен у табели, подаци се уносе у ред "друге пословне апликације", уз навођење пословног процеса на који је инцидент утицао. У колони Утицај на репутациони ризик назначити ДА уколико је бар један инцидент у оквиру тог ИТ сегмента утицао на репутациони ризик, те навести број инцидената.

(5) Извјештајни образац ПИ.3 - Преглед оперативних инцидената садржи податке о броју оперативних инцидената и догађаја који нису класификовани као инцидент према дефинисаним категоријама (грешке у процесима, системске грешке, људске грешке, екстерни догађаји,

критични/кључни пословни процеси). У образац је потребно укључити и број инцидената који су забиљежени код пружаоца услуга.

(6) Извјештајни образац ПИ.4 - Преглед сајбер инцидената садржи податке о броју инцидената из домена безбједности информационог система, према дефинисаним категоријама (малициозни код, неовлашћено прикупљање података, покушај упада у ИКТ систем, упади, доступност, превара, остало) и врстама напада/пријетњи. У образац је потребно унијети и број детектованих покушаја за одређену врсту напада/пријетњи, с тим да ако се ради о великом броју детектованих покушаја банка може унијети оквиран број.

(7) За потребе попуњавања извјештајних образаца ПИ.2, ПИ.3 и ПИ.4 користити следеће напомене:
Број и износ обухваћених трансакција се рачуна на основу свих трансакција на које инцидент директно или индиректно утиче или ће вјероватно утицати, као и свих трансакција које се неће моћи иницирати или обрадити, трансакција са промијењеним садржајем поруке о плаћању и оних које су иниције са намјером преваре. Код израчунавања броја и износа обухваћених трансакција потребно је посматрати дневне просјеке трансакција извршених истим услугама које су погођене инцидентом, при чему претходна година служи као референтно раздобље за израчунавање.
Обухваћени клијенти су сви клијенти који имају уговор са банком којим им се одобрава коришћење погођене услуге и који су претрпјели или ће вјероватно претрпјети посљедице инцидента. Банка треба на основу претходних активности процијенти број клијената који су се можда користили услугом током трајања инцидента.
Код израчунавања **времена прекида рада процеса** посматра се прекид или значајно смањена доступност било које активности или ИКТ система у оквиру погођеног пословног процеса, који ће онемогућити приступ услузи, иницирање и/или извршавање услуге. При том се узима у обзир временско раздобље у којем је услуга иначе доступна клијентима , ако је то релевантно и примјењиво за погођену услугу (нпр. електронско банкарство 24 сата, шалтерско пословање у централи 10 сати, шалтерско пословање у агеције 8 сати, ...) Ако банка не може да утврди када је почело раздобље прекида услуге, вријеме прекида се рачуна од тренутка у којем је прекид рада откривен. Укупно вријеме прекида рада одређеног пословног процеса представља укупно вријеме прекида обављања или смањене доступности одређеног пословног процеса/ИТ сегмента узрокованих забиљеженим инцидентима.
Укупан износ губитка проузрокован инцидентима за одређени пословни процес представља збир свих финансијских губитака због прекида рада ИТ система или значајно смањене доступности ИТ система који подржавају тај пословни процес.

(8) Извјештајни образац ПИ.5 - Електронско банкарство и картично пословање - могуће злоупотребе садржи податке о броју инцидената који су се догодили у извјештајном периоду а односе се на могуће злоупотребе система електронског банкарства и картичног пословања усљед слабости информационог система нпр. посљедица хакерских напада и слично. Потребно је унијети податке о неуобичајеним трансакцијама у зависности од статуса:
- статус отворен за неуобичајене трансакције које још нису извршене, а сумња се на злоупотребу система,
- статус извршена за трансакције које су извршене и потврђене да се ради о злоупотреби система,
- статус одбијен за неуобичајене трансакције које су правовремено блокиране, те нису извршене,
- статус неријешено за неуобичајене трансакције за које се сумња да се ради о злоупотреби система и анализа је још у току,
- статус неусаглашене за неуобичајене трансакције које су извршене, али не постоји усаглашен став банке и корисника да се ради о злоупотрби система.

Извјештај Електронско банкарство

Члан 12.

(1) Извјештај Електронско банкарство садржи податке о обиму електронског банкарства (интернет и мобилно банкарство), као и начинима аутентификације клијената.

(2) Извјештај Електронско банкарство доставља се на следећим обрасцима:

1) ЕБ.1 - Обим електронског банкарства и
2) ЕБ.2 - Елементи аутентификације и ауторизације у електронском банкарству.

(3) Извјештајни образац ЕБ.1 - Обим електронског банкарства садржи податке о обиму (број клијената, број и износ трансакција) електронског банкарства за правна и физичка лица у односу на укупан платни промет банке у извјештајном периоду. У колону Број клијената уноси се број клијената банке, те број клијената интернет и мобилног банкарства, за правна и физичка лица на последњи дан извјештајног периода. Број и износ извршених трансакција се уноси за унутрашњи платни промет (УПП) и ино платни промет (ИПП), гдје се износ уноси у хиљадама (000) КМ.

(4) Извјештајни образац ЕБ.2 - Елементи аутентификације и ауторизације у електронском банкарству садржи податке о свим могућим начинима аутентификације и ауторизације клијената у систему електронског банкарства, на последњи дан извјештајног периода. За све системе електронског банкарства који су доступни клијентима банке потребно је навести назив система, врсту електронског банкарства (1-интернет банкарство/ 2-мобилно банкарство), те врсту клијената којима је систем намијењен (1-физичка лица/ 2-правна лица). Уколико се ради о екстернализацији потребно је попунити колону Назив пружаоца услуга. За сваки систем потребно је навести број клијената у зависности од начина аутентификације (комбинација елемента у колонама Елемент аутентификације 1 и Елемент аутентификације 2). У табели су наведени најчешће коришћени елементи, те уколико системи које је банка имплементирала дозвољавају и неке друге елементе аутентификације потребно их је унијети. Такође за сваки систем, уколико је примјењиво, потребно је изабрати елемент ауторизације (колона Елементи ауторизације), те број клијената који користи овај елемент ауторизације.

Извјештај Картично пословање

Члан 13.

(1) Извјештај Картично пословање садржи податке о обиму картичног пословања и броју активних POS и ATM уређаја.

(2) Извјеш Извјештај Картично пословање доставља се на следећим обрасцима:
1) КП.1 - Обим картичног пословања и
2) КП.2 - Број POS и ATM уређаја.

(3) Извјештајни образац КП.1 – Обим картичног пословања садржи податке о обиму картичног пословања за правна и физичка лица, броју картица по врстама на последњи дан извјештајног периода, те износу извршених трансакција у извјештајном периоду у зависности од начина обављања трансакције. У колону Број картица уноси се податак о укупном броју картица према бренду/врсти картице на последњи дан извјештајног периода, као и износ извршених трансакција у колону Износ трансакција у односу на врсту картице и начин обављања трансакције у извјештајном периоду. Износ трансакција се уноси у хиљадама (000) КМ. У случају да банка издаје и друге врсте картица број картица и износ извршених трансакција уноси под Остало.

(4) Извјештајни образац КП.2 - Број POS и ATM уређаја садржи податке о укупном броју POS и ATM уређаја на последњи дан извјештајног периода који се налазе у објектима у банци (колона Број уређаја у банци), као и изван банке (колона Број уређаја изван банке).

Извјештај Употреба нових технологија

Члан 14.

(1) Извјештај Употреба нових технологија (FinTech) садржи податке о обиму кориштења нових технологија (FinTech) у извјештајном периоду. Извјештај се доставља на извјештајном обрасцу ФТ - Обим кориштења нових технологија (FinTech).

(2) Извјештајни образац ФТ - Обим кориштења нових технологија (FinTech) садржи податке о свим FinTech рјешењима које банка користи. За свако FinTech рјешење уноси се назив, врста напредне технологије на којој се заснива, кратак опис, пословни процеси у којима се користи, те уколико је примјењиво број и износ трансакција остварених коришћењем наведеног рјешења у извјештајном периоду. Износ трансакција се уноси у хиљадама (000) КМ.

Извјештај План опоравка информационог система

Члан 15.

(1) Извјештај План опоравка информационог система садржи податке о тестирању плана опоравка информационог система, сценаријима за тестирање, пословним процесима који су обухваћени тетсирањем и другим подацима у извјештајном периоду.

(2) Извјештај План опоравка информационог система доставља се на следећим обрасцима:
1) ПОИС.1 - Основни подаци о тестирању плана опоравка информационог система,
2) ПОИС.2 - Сценарио тестирања,
3) ПОИС.3 - Тестирани пословни процеси и
4) ПОИС.4 - Остали подаци о опоравку информационог система.

(3) Извјештајни образац ПОИС.1 - Основни подаци о тестирању плана опоравка информационог система садржи податке о тестирању плана опоравка информационог система. У извјештајном обрасцу је потребно изабрати или уписати одговоре о обављеном тестирању као што су: датум тестирања, начин тестирања (симулација или стварни рад банке са резервног рачунарског центра, као и број обухваћених пословних процеса), врста резервне локације, укљученост централе, организационих дијелова и пословних процеса у тестирање, укљученост запослених банке и пружаоца услуге у тестирање и др.

(4) Извјештајни образац ПОИС.2 - Сценарији тестирања садржи податке о сценарију који је кориштен приликом тестирања плана опоравка информационог система. За наведене сценарије потребно је унијети одговор да ли су кориштени или не током предметног тестирања. У случају да је банка користила неки други сценарио за тестирање, који није наведен у табели, исти је потребно додатно унијети. У колону Датум последњег тестирања сценарија уноси се датум последњег тестирања за сваки од наведених сценарија.

(5) Извјештајни образац ПОИС.3 - Тестирани пословни процеси садржи податке о појединачним пословним процесима и ИКТ системима који су укључени у тестирање плана опоравка информационог система. У извјештајном обрасцу је потребно дати одговоре који је пословни процес или ИКТ систем био укључен у тестирање плана опоравка информационог система, те да ли је исти критичан/кључан.. За сваки пословни процес или ИКТ систем уноси се податак о захтијеваном RTO и RPO (који је банка дефинисала у оквиру анализе утицаја на пословање - BIA), као и остварени RTO током обављеног тестирања. У случају да је банка током тестирања укључила пословни процесе или ИКТ системе, који нису наведени у табели потребно их је додатно унијети.

(6) Извјештајни образац ПОИС.4 - Остали подаци садржи остале податке о тестирању плана опоравка информационог система. У извјештајном обрасцу је потребно изабрати или уписати одговоре као што су: подаци о физичким локацијама рачунарских центара (примарни, резервни, локални,...), укљученост ресурса са примарне локације током тестирања плана опоравка информационог система, периодичност опоравка резервних копија података неопходних за опоравак критичних/кључних пословних процеса, те начин преноса података између примарне и резервне локације и др.

III РОКОВИ ЗА ИЗВЈЕШТАВАЊЕ

Динамика достављања извјештаја

Члан 16.

(1) Банка је дужна да годишње, а најкасније до 5. марта наредне године за претходну годину, доставља Агенцији сљедеће извјештајне обрасце:
1) ОП.1 - Општи подаци о организационој структури,
2) ОП.2 - Општи подаци о одговорним особама,
3) ОП.5 - Општи подаци и интерној ревизији информационог система,
4) ИС.1 - Инфраструктура система,
5) ИС.2 - Сервери,
6) ИС.3 - Мрежни уређаји,

7) ИС.4 - Радне станице,
8) ИС.5 - Банкомати,
9) ИС.6 - Системи без подршке,
10) ИС.7 - Удаљени приступ информационом систему,
11) СОП - Стратешки и оперативни циљеви,
12) БИС.1 - ИКТ буџет,
13) БИС.2 - FinTech буџет,
14) ЕБ.2 - Елементи аутентификације и ауторизације у електронском банкарству,
15) КП.1 - Обим картичног пословања,
16) КП.2 - Број POS и АТМ уређаја,
17) ФТ - Обим коришћења нових технологија (FinTech),
18) ПОИС.1 - Основни подаци о тестирању плана опоравка информационог система,
19) ПОИС.2 - Сценарији тестирања,
20) ПОИС.3 - Тестирани пословни процеси,
21) ПОИС.4 - Остали подаци о тестирању.

(2) Банка је дужна да квартално, а најкасније 30 дана након посљедњег дан извјештајног квартала, доставља Агенцији сљедеће извјештајне обрасце:
1) ОП.3 - Општи подаци о флуктуацији кадрова,
2) ОП.4 - Општи подаци о ванјским ИТ сарадницима
3) УРИС - План мјера за поступање са ризицима информационог система,
4) ПЕН - Резултати пенетрационих тестирања/тестова рањивости,
5) ИТР.1 - Преглед планираних и обављених ревизија информационог система,
6) ИТР.2 - Преглед препорука/налога,
7) ПИС - Значајне промјене у информационом систему,
8) ПИ.1 - Категоризација инцидената,
9) ПИ.2 - Преглед инцидената по пословним процесима,
10) ПИ.3 - Преглед оперативних инцидената,
11) ПИ.4 - Сајбер инциденти,
12) ПИ.5 - Електронско банкарство и картично пословање - могуће злоупотребе,
13) ЕБ.1 - Обим електронског банкарства.

(3) Банка је дужна да извјештаје из овог упутства електронским путем доставља Агенцији, у формату и на начин који су прописани овим упутством.

IV ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Ступање на снагу

Члан 17.

(1) Ово упутство ступа на снагу осмог дана од дана објављивања у "Службеном гласнику Републике Српске".

(2) Овим упутством ставља се ван снаге Упутство за извјештавање о управљању информационим системима у банкама број: Д-2/18 од 24.01.2018. године.

(3) Банка је дужна прве извјештаје из члана 16. став 1. и 2. са стањем на дан 31.12.2020. године доставити до 31.03.2021. године.

Број: Д-6/21

Дана, 19.02.2021. год.

Директор

Раде Растока