|  |  |  |  |
| --- | --- | --- | --- |
| **Микрокредит ташкилотлари, ломбардлар ва ипотекани қайта молиялаштириш ташкилотларининг ахборот тизимларида ахборот хавфсизлигига доир минимал талаблар тўғрисидаги НИЗОМ**  **(АВ 30.06.2020 й руйхатга олинган №3260)**    Ўзбекистон Республикасининг “Ўзбекистон Республикасининг Марказий банки тўғрисида”ги қонунга мувофиқ Ўзбекистон Республикаси Марказий банки Бошқаруви **қарор қилади:**  1.Микрокредит ташкилотлари, ломбардлар ва ипотекани қайта молиялаштириш ташкилотларининг ахборот тизимларида ахборот хавфсизлигига доир минимал талаблар тўғрисидаги низом иловага мувофиқ тасдиқлансин.  2. Мазкур қарор расмий эълон қилинган кундан эътиборан уч ойдан кейин кучга киради.   |  |  | | --- | --- | | Марказий банк раиси М.Нурмуратов |  |   **Микрокредит ташкилотлари, ломбардлар ва ипотекани қайта молиялаштириш ташкилотларининг ахборот тизимларида ахборот хавфсизлигига доир минимал талаблар тўғрисидаги**  **НИЗОМ**  Мазкур Низом «Ўзбекистон Республикасининг Марказий банки тўғрисида»ги Ўзбекистон Республикасининг қонунига мувофиқ микрокредит ташкилотлари, ломбардлар ва ипотекани қайта молиялаштириш ташкилотларининг (бундан буён матнда нобанк кредит ташкилотлари деб юритилади) ахборот тизимларида ахборот хавфсизлигига доир минимал талабларини белгилайди.  **1-боб. Умумий қоидалар**  1. Мазкур Низомда қуйидаги асосий тушунчалардан фойдаланилади:  **антивирус ҳимояси** — антивирус дастурлари ёрдамида компьютер вируслари таъсирининг олдини олиш, вирусларни топиш ва зарарсизлантиришга қаратилган чора-тадбирлар мажмуи;  **аутентификация килиш**— фойдаланувчи, дастур, қурилма ёки маълумотларнинг ҳақиқийлигини тасдиқлаш тартиб-таомили;  **авторизация килиш** — фойдаланиш ҳудудлари асосида фойдаланиш имкониятини тақдим этиш;  **ахборот тизими** — ахборотни тўплаш, сақлаш, излаш, унга ишлов бериш ҳамда ундан фойдаланиш имконини берадиган, ташкилий жиҳатдан тартибга солинган жами ахборот ресурслари, ахборот технологиялари ва алоқа воситалари;  **ахборот хавфсизлиги** — ахборот муносабатларининг субъектларига номақбул зиёнларни келтириши мумкин бўлган табиий ёки сунъий хусусиятли, тасодифий ёки қасддан қилинган таъсирлардан ахборот ва таъминлаб турадиган инфратузилманинг муҳофаза қилинганлиги;  **ахборот хавфсизлиги нохуш ҳодисаси** — ахборот хавфсизлигининг ягона воқеаси ёки бир қатор нохуш ёхуд кутилмаган воқеалари бўлиб, ушбу воқеалар туфайли ахборотнинг ошкор бўлиши ва ахборот хавфсизлигига таҳдидлар эҳтимоли юзага келиши;  **идентификация**— фойдаланувчининг шахсни, унга тизим билан ишлашда ҳуқуқ ва имтиёзларнинг маълум тўпламини бериш мақсадида аниқлаш;  **тармоқлараро экран** — автоматлаштирилган тизимга келиб тушадиган ва (ёки) тизимдан чиқиб кетадиган ахборотнинг назорат қилинишини амалга оширадиган дастур ва (ёки) дастурий восита;  **шахсга доир маълумотлар** — муайян жисмоний шахсга тааллуқли бўлган ёки уни идентификация қилиш имконини берадиган, электрон тарзда, қоғозда ва (ёки) бошқа моддий жисмда қайд этилган ахборот.  2. Нобанк кредит ташкилотлари мазкур Низом талаблари асосида, ўз фаолиятларининг хусусиятларидан келиб чиқиб, ахборот тизимлари ва ахборот ресурсларидаги ахборотнинг хавфсизлигини таъминлашлари хамда ахборот хавфсизлиги бўйича ички тартиб ва қоидаларини ишлаб чиқишлари лозим.  **2-боб. Нобанк кредит ташкилотларининг ахборот хавфсизлигига доир минимал талаблари**  3. Нобанк кредит ташкилотлари ўз фаолиятининг барқарорлигини таъминлаши ва ахборот хавфсизлигига таҳдидларни олдини олишлари учун, ахборот тизимлари ва ахборот ресурсларидаги ахборотнинг хавфсизлигини таъминлашлари, юзага келиши мумкин бўлган ахборот хавфсизлиги нохуш ҳодисаларини аниқлашлари, уларнинг олдини олишлари ва нохуш ҳодисаларнинг юзага келиш эҳтимолини бартараф этиш чораларини кўришлари лозим.  4. Нобанк кредит ташкилотлари ахборот хавфсизлигига доир қуйидаги минимал талабларни бажаришлари лозим:  антивирус дастури билан ахборот муҳофазасини таъминлаш;  амалга оширилган туловларга оид маълумотларни электрон тарзда қонун хужжатларида белгиланган муддатларда сақлаш;  махфий ва шахсга доир маълумотлардан қонунга зид равишда фойдаланиш ва маълумотларни ноқонуний ошкор этилишини олдини олиш;  техник носозликлар вақтида ахборот тизимларининг узлуксиз фаолиятини таъминлаш, шу жумладан тизимларда қўлланилган дастур ва маълумотлар нусхаларини сақлаш;  телекомунникация тармоги оркали ахборот алмашинувидаги тулов маълумотларини мухофазалаш;  маълумотларга ишлов берувчи компьютер ва серверларнинг ахборот муҳофазасини таъминлаш, узлуксиз электр таъминоти манбаи курилмалари (UPS) билан жиҳозлаш;  қўриқлаш, ёнғиндан огоҳ этиш ва ташвишдан хабар бериш, видеокузатув ҳамда ўт ўчириш тизимларини жорий қилиш;  ахборот тизимлари маълумотлари йиғиладиган ва уларга ишлов бериладиган ҳудудларга (хоналарга) бегона шахсларнинг рухсатсиз (назоратсиз) киришининг олдини олиш, ушбу ҳудудлар видеокузатув тизими орқали назоратга олинган бўлиши ва видеокузатув маълумотларининг сакланишини таъминлаш;  тулов ва махфий маълумотларнинг электрон нусхалари сакланишида ахборот хавфсизлигини таъминлаш;  масофадан хизмат кўрсатишда мижозни идентификация, аутентификация ва авторизация килиш;  телекоммуникация тармоғи орқали ахборот алмашинувида ёки масофадан хизмат кўрсатишда тизимга киришда идентификация ва кўп факторли аутентификация килиш ҳамда тармокка киришдаги маълумотларни (сана, вақт, IP манзил ва бошқа идентификация маълумотлари) электрон баённомаларда қайд этиб бориш;  масофадан хизмат кўрсатиш билан боғлиқ бўлган ахборот тизимларидаги ўзгаришлар юзасидан мижозларни ўз вақтида хабардор килиш;  телекоммуникация тармоқларида тўловларни криптографик усуллар (электрон рақамли имзо ва шифрлаш) билан муҳофазалаш;  нобанк кредит ташкилоти худудида Wi-Fi зоналари ташкил этилса, Wi-Fi тармоги оркали юзага келиши мумкин булган ахборот хатарларининг олдини олиш;  нобанк кредит ташкилотларнинг Узбекистон Республикаси Марказий банки билан ахборот алмашинувида ахборот муҳофазасини таъминлаш, ахборот алмашинувини икки томонлама имзоланган тегишли технологик йўриқнома талаблари асосида амалга ошириш;  ахборот тизимларининг ахборот хавфсизлиги таваккалчиликларини камайтириш чораларини кўриш;  ахборот тизимлари қурилмалари ва дастурларининг иш холатини назорат килиб бориш;  ахборот хавфсизлиги билан боғлиқ нохуш ҳодисаларни бартараф этиш режаларини ишлаб чиқиш.  **3-боб. Ахборот хавфсизлигини ташкиллаштириш**  5. Нобанк кредит ташкилотлари ўзларининг ахборот тизимларининг ахборот хавфсизлигини таъминлаш мақсадида ахборот хавфсизлигига маъсул ходим тайинлаши лозим.  6. Ахборот хавфсизлигига маъсул ходим вазифаларига қуйидагилар киради:  ахборот тизимлари ва ахборот ресурсларининг ахборот муҳофазасини ташкил этиш ва таъминлаш;  иш жараёнида ходимларга маълум бўлган махфий ва шахсга доир маълумотларни сир сақлаш мажбурияти ва жавобгарликлари тўғрисида тушунтириш ишларини олиб бориш;  антивирус муҳофазасини ташкил этиш ва назоратини юритиш;  электрон тўлов маълумотларининг нусхаларини сақланишини ташкил этиш;  ахборот тизимларига ўзгартиришлар киритилишини назорат килиш;  фойдаланувчиларнинг ахборот ресурсларида ишлаш ҳуқуқларини ва чегараларини белгилаш;  ахборот тизимларига киришни назорат қилиш;  ахборот тизимларида электрон тўловлар билан боғлиқ ноқонуний хатти-ҳаракатларнинг олдини олиш чораларини кўриш;  ахборот тизимлари ва ахборот ресурсларидан рухсатсиз фойдаланишни чеклаш;  веб-ресурслар (маълумотлар базаси) ва бошқа ахборот ресурсларини ахборот хавфсизлиги хатарларидан сақлаш;  электрон маълумотларнинг рухсатсиз киритилиши, ўзгартирилиши, ўчириб ташланиши, кўчириб олиниши ва фойдаланилиши имкониятини тўлиқ бартараф қилиш;  компьютер ва бошқа ҳисоблаш воситалари носоз ҳолатга келганида, иш узлуксизлигини таъминлаш мақсадида, тизимнинг захира тикланиш режасини ишлаб чиқиш;  юзага келиши мумкин бўлган ахборот хавфсизлиги нохуш ҳодисаларини бартараф этилишини таъминлаш;  ахборот хавфсизлиги хатарларини камайтириш ва олдини олиш чораларини кўриш;  махфий ва шахсга доир маълумотлардан қонунга зид равишда фойдаланиш хавфларини бартараф этиш;  ҳисоблаш техникаларига рухсатсиз жисмонан таъсир ўтказишини олдини олиш;  ахборот хавфсизлигини таъминлаш юзасидан ички меъёрий ҳужжатларни ишлаб чиқиш;  ахборот хавфсизлиги талабларининг бажарилишини назорат қилиш.  **4-боб. Ахборот муҳофазаси дастурлари ва ускуналари**  7. Нобанк кредит ташкилотларининг ахборот муҳофазасини таъминловчи барча ахборот дастурлари лицензияланган бўлиши керак.  8. Нобанк кредит ташкилотларининг ахборот муҳофазаси дастурлари ва ускуналари қуйидагиларни амалга ошириши лозим:  тармоқ муҳофазасини таъминлаши, шу жумладан, локал ҳисоблаш тармоғига рухсатсиз киришларни олдини олишни;  тўловларнинг амалга оширилиши электрон рақамли имзо билан тасдиқланиши;  тулов маълумотларини узоқ муддат сақлаши, заҳиралаш ва қайта тиклашни таъминлаши;  ахборотни шакллантириш, узатиш, саклаш, улардан фойдаланиш ва уларга ишлов бериш жараёнларида маълумотларни муҳофазалаши;  ахборот алмашинуви жараёнида ахборотни муҳофаза қилиши;  ахборот тизимларидаги маълумотларнинг махфийлигини таъминлаши;  фойдаланувчиларнинг тизимга кириш ва чиқиш бўйича ҳаракатлари қайд этиши;  фавқулодда ҳолатларда тизимнинг хавфсизлигини ва узилишларсиз фаолиятини таъминлаши.  9. Нобанк кредит ташкилотлари ўзларидаги тўловлар тўғрисидаги маълумотларнинг ҳимоя қилинишида Ўзбекистон Республикасининг “Тўловлар ва тўлов тизимлари тўғрисида”ги Конунида белгиланган талаб ва тартибларга  риоя этишлари зарур.  10. Нобанк кредит ташкилотлари содир булган нохуш ҳодиса тугрисида Узбекистон Республикаси Марказий банкига зудлик билан ёзма ёки электрон шаклда хабар бериши лозим.  **5-боб. Якуний қоида**  11. Мазкур Низом талабларининг бузилишида айбдор бўлган шахслар қонун ҳужжатларида белгиланган тартибда жавобгар бўлади. | **Переведен на русский язык (не официально)**  **ПОЛОЖЕНИЕ «О минимальных требованиях к информационной безопасности в информационных системах микрокредитных организаций, ломбардов и организаций рефинансирования ипотеки»**  (Мин.Юст №3260 от 30.06.2020 г)  В соответствии с Законом Республики Узбекистан «О Центральном банке Республики Узбекистан» Правление Центрального банка Республики Узбекистан **принимает решение:**  1. Утвердить Положение о минимальных требованиях к информационной безопасности в информационных системах микрокредитных организаций, ломбардов и организаций рефинансирования ипотеки согласно приложению.  2. Данное решение вступает в силу через три месяца после его официального опубликования.  Председатель Центрального банка М.Нурмуратов  **ПОЛОЖЕНИЕ «О минимальных требованиях к информационной безопасности в информационных системах микрокредитных организаций, ломбардов и организаций рефинансирования ипотеки»**  В соответствии с Законом Республики Узбекистан «О Центральном банке Республики Узбекистан» настоящим Положением устанавливаются минимальные требования к информационной безопасности в информационных системах микрокредитных организаций, ломбардов и организаций по рефинансированию ипотеки (далее по тексту – небанковские кредитные организации).  **Глава 1. Основные правила**  1.В этом Положении используются следующие основные понятия:  **антивирусная защита** - комплекс мер, направленных на предотвращение воздействия компьютерных вирусов, обнаружение и нейтрализацию вирусов с использованием антивирусного программного обеспечения;  **аутентификация** - процедура проверки подлинности пользователя, приложения, устройства или данных;  **авторизация** - предоставление доступа на основе областей использования;  **информационная система** - совокупные организованные информационные ресурсы, информационные технологии и средства связи, позволяющие собирать, хранить, искать, обрабатывать и использовать информацию;  **информационная безопасность** - защита информации и инфраструктуры, которая предоставляет информацию от естественных или искусственных, случайных или преднамеренных воздействий, которые могут нанести чрезмерный вред субъектам информационных отношений;  **инцидент информационной безопасности** - единичное событие информационной безопасности или серия неблагоприятных или неожиданных событий, которые могут привести к раскрытию информации и возможной угрозе информационной безопасности;  **идентификация** - идентификация пользователя с целью предоставления ему определенного набора прав и привилегий при работе с системой;  **межсетевой экран** - программный и (или) программный инструмент, который контролирует информацию, которая входит и (или) покидает автоматизированную систему;  **персональные данные** - информация, записанная в электронном виде, на бумаге и (или) в другом материальном виде, которая принадлежит конкретному лицу или позволяет его идентифицировать.  2.В соответствии с требованиями настоящего положения небанковские кредитные организации, исходя из специфики своей деятельности, должны обеспечивать безопасность информации в информационных системах и информационных ресурсах, а также разрабатывать внутренние процедуры и правила обеспечения информационной безопасности.  **Глава 2. Минимальные требования к информационной безопасности небанковских кредитных организаций**  3. В целях обеспечения устойчивости своей деятельности и предотвращения угроз информационной безопасности небанковские кредитные организации должны обеспечивать безопасность информации в информационных системах и информационных ресурсах, выявлять потенциальные инциденты информационной безопасности, предотвращать их и принимать меры по устранению возможности потенциальных инцидентов.  4. Небанковские кредитные организации должны соответствовать следующим минимальным требованиям информационной безопасности:  обеспечение защиты информации с помощью антивирусного программного обеспечения;  электронное хранение платежной информации в течение срока, установленного законодательством;  предотвращение противозаконного использования конфиденциальной и личной информации и предотвращение незаконного раскрытия информации;  обеспечение бесперебойной работы информационных систем в случае технических сбоев, включая хранение копий программного обеспечения и данных, используемых в системе;  защита платежных данных при обмене информацией через телекоммуникационную сеть  обеспечение защиты информации компьютеров и серверов обработки данных и оснащение их источником бесперебойного питания (ИБП);  внедрение систем охранной безопасности, пожарной сигнализации и систем видеонаблюдения и пожаротушения;  предотвращать несанкционированный доступ к областям (комнатам), где собираются и обрабатываются данные информационных систем, обеспечить, что эти области контролировались системами видеонаблюдения и обеспечивали хранения данных видеонаблюдения;  обеспечение информационной безопасности при хранении электронных копий платежной и конфиденциальной информации;  при дистанционным обслуживании клиентов проводить идентификацию, аутентификацию и авторизацию;  Регистрация в электронных протоколах всех операций сети (дата, время, IP-адрес и другая идентификационная информация), выполнение процессов идентификации и многофакторной аутентификации при доступе к системе при обмене информацией или при оказании удаленных услугах через телекоммуникационную сеть:  своевременное информирование пользователей об изменениях в информационных системах, связанных с оказанием удаленных услуг;  защита платежной информации в телекоммуникационных сетях криптографическими методами (электронная цифровая подпись и шифрование);    предотвращение информационных рисков, которые могут возникнуть через сеть Wi-Fi, если на территории небанковской кредитной организации создаются зоны Wi-Fi;  обеспечение информационной безопасности при обмене информацией между небанковскими кредитными организациями и Центральным банком Республики Узбекистан в соответствии с требованиями соответствующих двусторонних технологических положений;  принять меры по снижению рисков информационной безопасности информационных систем;  мониторинг работы информационных систем устройств и программ;  разработать планы по устранению инцидентов, связанных с информационной безопасностью  **Глава 3 Организация информационной безопасности**  5. Небанковские кредитные организации должны назначить ответственного сотрудника по информационной безопасности, для обеспечения информационной безопасности.  6. В обязанности ответственного сотрудника по информационной безопасности входит:  организация и обеспечение защиты информации информационных систем и информационных ресурсов;  проведение разъяснительной работы об ответственности работников сохранять конфиденциальную и личную информацию ставшую известной ими в процессе работы;  организация и контроль антивирусной защиты;  организация хранения копий данных электронных платежей;  контроль за изменениями в информационных системах;  определение прав и ограничений пользователей на работу с информационными ресурсами;  контроль доступа к информационным системам;  принять меры по предотвращению незаконных действий, связанных с электронными платежами в информационных системах;  ограничение несанкционированного доступа к информационным системам и информационным ресурсам;  защита веб-ресурсов (баз данных) и других информационных ресурсов от рисков информационной безопасности;  полное исключение возможности несанкционированного ввода, изменения, удаления, копирования и использования электронных данных;  разработка плана восстановления системы резервного копирования для обеспечения непрерывности работы в случае выхода из строя компьютеров и других вычислительных устройств;  обеспечение устранения возможных инцидентов информационной безопасности;  принять меры по снижению или предотвращению рисков информационной безопасности;  принять меры по устранению рисков незаконного использования конфиденциальной и личной информации;  принять меры по предотвращению несанкционированного физического воздействия на вычислительную технику;  разработка внутреннего нормативного документа по информационной безопасности;  контроль за соблюдением требований информационной безопасности.  **Глава 4 Программы и оборудование информационной безопасности**  7. Все информационные программы, обеспечивающие информационную безопасность небанковских кредитных организаций, должны быть лицензированы.  8. Программы информационной безопасности и оборудование небанковских кредитных организаций должны:  обеспечить защиту сети, в том числе предотвращение несанкционированного доступа к локальной сети;  подтверждение платежей электронной цифровой подписью;  обеспечение долгосрочного хранения, резервного копирования и восстановление платежной информации;  защита данных в процессе формирования, передачи, хранения, использования и обработки информации;  защита информации в процессе обмена информацией  обеспечение конфиденциальности информации в системе;  записывать действия пользователей по входу и выходу из системы;  обеспечить безопасность и бесперебойную работу системы в случае чрезвычайных ситуаций.  9. При защите своей платежной информации небанковские кредитные организации должны соблюдать требования и процедуры, установленные Законом Республики Узбекистан «О платежах и платежных системах».  10. Небанковские кредитные организации в случае инцидента должны немедленно уведомить Центральный банк Республики Узбекистан в письменной или электронной форме.  **Глава 5 Окончательное правило**  11. Лица, виновные в нарушении требований настоящих Правил, несут ответственность в порядке, установленном законом. |