**Приложение № 1**

В тендерную комиссию

ЗАО «ФИНКА Банк»

от «\_\_\_\_»\_\_\_\_\_\_\_\_\_202\_ г.

номер тел. Участника

электронный адрес

**ЗАЯВКА**

**на участие в тендере**

Изучив тендерные документы на \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, мы, нижеподписавшиеся, предлагаем осуществить поставку вышеуказанной услуги/товара, в соответствии с указанными тендерными документами.

В случае если наше предложение будет принято, берем на себя обязательство осуществить поставку услуги/товара --------------------------------------------------\_ указанной в тендерных документах.

Мы подтверждаем наше согласие, считать данное тендерное предложение действительным в течение \_\_\_\_\_\_ (\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_) календарных дней с даты указанной, в тендерных документах и обязуемся рассматривать его как обязательное для нас.

Мы выражаем свое согласие/ несогласие открыть расчетный счет в ЗАО ФИНКА Банк

 Согласен

 Не согласен

Мы признаем за вами все ваши права, указанные в тендерных документах. Мы понимаем, что вы не обязаны принять тендерную заявку с наименьшей стоимостью или вообще какую-либо из заявок, полученных вами.

Дата: число \_\_\_\_\_\_\_\_\_\_\_ месяц \_\_\_\_\_\_\_\_\_\_\_\_ 202\_ г.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 ( Подпись) (Должность)

**Приложение № 2**

В тендерную комиссию

ЗАО «ФИНКА Банк»

**Анкета Участника тендера**

| **№ п/п** | **Наименование** | **Сведения об Участнике тендера (заполняется Участником тендера)** |
| --- | --- | --- |
|  | Организационно-правовая форма и фирменное наименование Участника  |  |
|  | ИНН Участника  |  |
|  | Юридический адрес |  |
|  | Фактический адрес |  |
|  | Филиалы: перечислить наименования и фактические адреса |  |
|  | Телефоны Участника  |  |
|  | Адрес электронной почты Участника  |  |
|  | Фамилия, имя и отчество, дата рождения руководителя Участника, имеющего право подписи согласно учредительным документам, с указанием должности и контактного телефона |  |
|  | Фамилия, имя и отчество ответственного лица Участника Запроса предложений с указанием должности и контактного телефона |  |

\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись, М.П.)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(фамилия, имя, отчество подписавшего, должность)

*Участники должны заполнить приведенную выше таблицу по всем позициям.*

*В случае отсутствия каких-либо данных указать «нет».*

**Приложение № 3**

В тендерную комиссию

ЗАО «ФИНКА Банк»

**Техническое задание**

1. В случае досрочного расторжении Полиса по инициативе Страховщика, сторонами производится финансовый взаиморасчет и Страхощик возвращает Банку полную разницу суммы страховой премии без никаких удержаний.
2. Требуется застраховать комплексные банковские риски, а также риски от электронных и компьютерных преступлений ЗАО «ФИНКА Банк» согласно категориям, приведенным ниже:

|  |  |
| --- | --- |
| **Категория** | **Страховое покрытие** |
| ***Нечестность сотрудников*** | Убытки, возникающие исключительно и в прямой связи с нечестными или мошенническими действиями Сотрудников, действовавшим в одиночку или в сговоре с иными лицами, независимо от места действий, с намерением нанести убыток Застрахованному или извлечь необоснованную личную финансовую выгоду в собственных интересах. Страховой полис покрывает убыток, понесенный и обнаруженный во время действия страхового полиса, а также обнаруженный в течение не более 1 (одного) года после прекращения действия страхового полиса, но понесенный в период действия страхового полиса.Убытки, возникающие вследствии разглашения сотрудниками конфиденциальной информации третьих лиц являющейся владельцем конфиденциальной информации (коммерческой тайны). |
| ***Помещения*** | Убытки вследствие утраты Имущества (включая материальные ценности-наличность), из Помещений по причине:(i) Кражи/Грабеж, хищений, совершенной личностями, присутствующими или незаконно проникшими в Помещение, или(ii) таинственного, необъяснимого исчезновения, или(iii) повреждений, разрушений или перемещения, также(iv) затопы, пожары, землетрясения, наводнения или др. стихийные бедствия |
| ***Перевозки*** | Утраты или повреждения любого Имущества (в том числе и денежная наличность и другие материальные ценности), по любой причине независимо от места происшествия и от вида транспорта во время перевозки/перемещения находящегося на попечении любого Сотрудника или на попечении любой Охранной Компании во время их транспортировки. А также угроза жизни и здоровью ответственных лиц Банка\водителей Банка учавствующих при перевозке\инкассации денежной наличности и других материальных ценностей Банка.  |
| ***Поддельные Ценные бумаги и платежные/кассовые документы*** | Убытки вследствие поддельной Подписи или иного Мошеннического Изменения любой ценной бумаги, Чека, Переводных Векселей, Банковской Тратты, Банковского Акцепта или Депозитного Сертификата, любых платежных кассовых документов, Договоров выданных Застрахованным,Убытки вследствие поддельной Подписи или иного Мошеннического Изменения любого РасходногоОрдера, Векселя, доверенности, договора и любого иного документа предусмотренного законодательством КР подлежащих оплате у Застрахованного и Застрахованным. |
| ***Фальшивые Денежные Знаки*** | Убыток вследствие добросовестного получения Застрахованным в ходе обычной хозяйственной деятельности любых фальшивых денежных знаков или монет, выпущенных в обращение или якобы выпущенных в обращение как законное платежное средство в любой Стране. (при мошенничестве со стороны кассира замена годных банкнот на фальшивые банкноты и их обнаружении в хранилище или кассе банка, при фальшивых банкнот высокого качества и не обнаружении их аппаратами-детекторами фальшивых банкнот –обнаружение при сдаче в другом банке или клиент обнаружил или следственные органы.) |
| ***Офисы и содержимое*** | Убытки вследствие повреждения помещений Застрахованного, напрямую вызванного кражей или попыткой кражи, или повреждения интерьера таких помещений вследствие случаев вандализма или умышленно нанесенного повреждения, а также вследствие повреждения содержимого внутри помещений, напрямую вызванного кражей или попыткой кражи, или случаями хулиганства, или умышленно нанесенного повреждения. |
| ***Компьютерные системы,*** ***включая Автоматизированные Банковские Системы (АБС)*** | Если Банк осуществил денежный перевод, оплатил или поставил какие-либо средства или имущество, получил кредит, дебетовал счет или осуществил любой другой вид выплат в результате1. мошеннического ввода электронных данных непосредственно в:
2. компьютерные системы Банка,; или
3. компьютерные системы сервисной (процессинговой) компании; или
4. электронную систему перевода средств; или
5. систему электронной связи с клиентами; или
6. мошеннического изменения или порчи электронных данных, хранящихся или использующихся в любой из вышеупомянутых систем, или во время передачи данных по системам электронной связи в компьютерную систему Банка или сервисной (процессинговой) компании; или
7. мошеннического ввода данных в компьютерную систему Банка через систему банковского обслуживания посредством телефонной связи. При условии, что мошеннические действия координировались или были совершены лицом, которое намеревалось причинить ущерб Банку, либо получить финансовую выгоду для себя или в пользу любого другого лица. Убытки вследствие утраты или повреждения компьютерной техники, сети, АБС и электронных оборудований от любых возможных [аварий](https://ru.wikipedia.org/wiki/%D0%90%D0%B2%D0%B0%D1%80%D0%B8%D1%8F).
 |
| ***Программное обеспечение*** | В случае если Банк осуществил денежный перевод, оплатил или поставил какие-либо средства или имущество, получил кредит, дебетовал счет или осуществил любой другой вид выплат в результате мошеннической разработки нового или модернизации существующего программного обеспечения (ПО). При этом, мошеннические действия по разработке ПО были совершены лицом, намеревавшимся причинить ущерб Банку или приобрести финансовую выгоду для себя или для другого лица. Ущерб или гибель программных обеспечений, а также убытки от перерыва в производственной (коммерческой) деятельности в результате террористического акта, хакерских атак, отмывания денег и возможных аварий. |
| ***Электронные данные и носители*** | Убытки, понесенные Банком от ущерба, причиненного электронным данным и носителям, вследствие:1. умышленной порчи или попытки порчи каким-либо лицом или сотрудником электронных данных и носителей, которые являются собственностью Банка или за которые он несет юридическую ответственность в случае потери или повреждения:
* в период хранения электронных данных в автоматизированной системе Банка или компьютерной системе Сервисной (процессинговой) компании;
* во время записи электронных данных на носители в пределах офисов или помещений Банка:
* в период перевозки или хранения вне офиса Банка носителей электронных данных лицом, назначенным Банком в качестве своего курьера (или лицом, временно действующим в качестве курьера или хранителя вследствие невозможности для основного курьера выполнить поручение), при этом носители электронных данных считаются находящимися в перевозке или на хранении с момента их получения курьером и до момента доставки получателю или его агенту;
1. повреждения или уничтожения электронных данных и носителей в результате:
* кражи, грабежа,форс-мажорных/непреодолимой силы обстоятельств, воровства со стороны курьера (хранителя);
* исчезновения по неустановленной компетентными органами причине носителя электронных данных, которые находились на хранении в офисе Банка или любых иных помещениях, или у лица, назначенного Банком в качестве своего курьера (или у лица, временно действующего в качестве курьера или хранителя вследствие невозможности для основного курьера выполнить поручение), при этом носители электронных данных считаются находящимися в перевозке или на хранении с момента их получения курьером и до момента доставки получателю или его агенту.
 |
| ***Компьютерные вирусы*** | 1. Если Банк перевел, осуществил денежный перевод или поставил какие-либо средства, либо имущество, получил кредит, дебетовал счет или осуществил любую другую выплату, что явилось прямым следствием воздействия компьютерного вируса на компьютерную систему Банка или компьютерную систему сервисной компании.
2. Если электронные данные Банка, хранящиеся в памяти его компьютерной системы или компьютерной системы сервисной компании, утеряны в результате их уничтожения, шифрования или попытки уничтожения компьютерным вирусом.
 |
| ***Электронные и телефаксные системы связи*** | Если Банк перевел, оплатил или поставил какие-либо средства или собственность, открыл кредит, дебетовал счет или осуществил любую другую выплату на основании направленного ему поручения или подтверждения на осуществление перевода, платежа, доставки или получения средств/имущества, которое было передано или выглядело как переданное1. по системе электронной связи, или
2. посредством телефаксной, телексной или иной аналогичной телетайпной системы связи связи

непосредственно в компьютерную систему или на телекоммуникационный терминал Банка, и подделанного под отправленное клиентом Банка, автоматизированной клиринговой организацией, офисом Банка или другим финансовым институтом, но которое на самом деле не было отправлено ни клиентом Банка, ни автоматизированной клиринговой организацией, ни офисом Банка, ни каким-либо другим финансовым институтом, или было мошеннически изменено во время физической перевозки носителей электронных данных к Банку либо во время электронной передачи поручения по коммуникационным системам , в том числе спутниковой, в автоматизированную систему или на телекоммуникационный терминал Банка. |
| ***Электронные переводы, включая SWIFT, Клиринг, Гросс и другие*** | Убытки, понесенные Банком от электронных переводов денежных средств в результате мошеннических действий, если Клиент Банка, автоматизированная клиринговая организация или другая финансовая организация перевела, оплатила или поставила какие-либо средства или собственность, выдала кредит, дебетовала счета или осуществила любую другую выплату, на основании:1. полученного мошеннического поручения или подтверждения на осуществление перевода, платежа, доставки или получения средств либо имущества, которое было передано непосредственно в автоматизированную систему или на телекоммуникационный терминал Клиента, автоматизированной клиринговой организации или другой финансовой организации, якобы от имени Банка:
* по системе электронной связи;
* посредством проверенной телефаксной, телексной или иной аналогичной телетайпной системы связи связи, посредством услуги Банк-клиент;
1. полученного от Банка поручения или подтверждения на осуществление перевода, платежа, доставки или получения средств / имущества, в которое были внесены изменения с целью мошенничества во время пересылки электронных данных, либо во время передачи поручения по системе электронной связи, в том числе и спутниковой, в автоматизированную систему или на телекоммуникационной терминал Клиента, автоматизированной клиринговой организации или другой финансовой организации.

 Убытки, понесенные банком вследствие: 1. кражи токенов аутентификации, сертификата ключа проверки ЭПЦ,
2. ведения бизнеса с несанкционированным контрагентом,
3. компрометации системы аутентификации организации,
4. компрометации достоверных резервных данных,
5. компрометации учетных данных пользователя,
6. удаления журналов операций и следов преступлений,
7. избыточного количества потенциальных векторов атак,
8. выполнения вредоносного кода,
9. взлома, подбора или другой компьютерной компрометации паролей,
10. кражи паролей,
11. форс-мажорных/непреодолимой силы обстоятельств,финансирования террористической деятельности/отмывания денег,
12. операции с электронными деньгами,
13. несанкционированного физического доступа.

Убытки, понесенные банком в случаях, когда:1. Злоумышленники компрометируют учетные данные системного администратора корпоративной службы каталогов Active Directory, что позволяет злоумышленникам получить доступ ко всем учетным данным, хранящимся в каталоге,
2. Злоумышленники подвергают опасности поддерживаемую ИТ-инфраструктуру (например, сервер сканирования, сервер исправлений), расположенной в общей ИТ-среде, для кражи системных учетных данных и последующего доступа к локальной инфраструктуре SWIFT,
3. Злоумышленники получают административный доступ к ПК оператора, что позволяет получить доступ к локальной базе данных учетных записей и повторно использовать сохраненные хэш-коды для доступа к другим системам,
4. Оператор щелкает на вредоносную ссылку в сообщении электронной почты, неумышленно загружая вредоносные программы, которые наносят ущерб локальному компьютеру.
5. Злоумышленник, имеющий сетевой доступ к зоне безопасности, нарушает целостность транзакций, переданных между интерфейсом обмена сообщениями и коммуникационным интерфейсом,
6. Злоумышленник, имеющий сетевой доступ к зоне безопасности, может наблюдать за незащищенным трафиком между локальными компонентами SWIFT и записывать конфиденциальные транзакции.
7. Злоумышленник использует известную и неустраненную уязвимость, чтобы получить доступ к серверу, на котором размещено связанное со SWIFT приложение,
8. Для доступа к интерфейсу администрирования сетевого брандмауэра злоумышленник использует имя пользователя и пароль по умолчанию, или применяет метод подбора пароля;
9. Злоумышленник использует уязвимость, связанную с неиспользуемым сетевым протоколом (например, telnet), чтобы получить доступ к серверу SWIFT,
10. Злоумышленник, расположенный между бэк-офисом и интерфейсом обмена сообщениями, вводит неудостоверенные транзакции,
11. Злоумышленник создает атаку типа "незаконный посредник", чтобы изменить расчётные счета получателей действующих транзакции SWIFT,
12. Злоумышленник, расположенный между бэк-офисом и интерфейсом обмена сообщениями, может отслеживать незашифрованный трафик и записывать конфиденциальные транзакции,
13. Злоумышленник перехватывает транзакцию, отправленную между браузером и веб-приложением, изменяет ее содержимое и пересылает его веб-приложению.
14. Аутсорсинговый провайдер не проводит надлежащего отделения систем SWIFT от других систем с низкой степенью защиты, что приводит к распространению вируса во всех средах и нарушению целостности систем SWIFT,
15. Аутсорсинговый провайдер не обеспечивает надлежащего контроля доступа, в результате чего неуполномоченный сотрудник получает доступ к интерфейсу обмена сообщениями SWIFT,
 |
| ***ПОС-терминалы, находящиеся в кассах банков/в торгово-сервисных предприятиях от похищений и повреждений.*** | Убытки, понесенные банком вследствие: 1. получение контроля над ПОС-терминалом и проведение операций с использованием украденных данных или фальшивых карт, и последующей наличкой в кассе банка;
2. кража или поломка ПОС-терминала
 |
| ***Платежные карты*** | Убытки, понесенные банком вследствие: 1. ограбление держателя карты при получении, внесении или переводе им денежных средств;
2. получение держателем карты денежных средств под принуждением со стороны преступника;
3. копирование магнитной полосы карты (скимминг и пр.);
4. блокирование карты в считывающем устройстве (ридере) с целью незаконного изъятия;
5. незаметная подмена или присвоение карты после выполнения операции на банкомате или ПОС-терминале;
6. установка фальшивых банкоматов;
7. кибератака, при которой информация о реквизитах карты присваивается путем незаконного доступа в систему банкоматов или к каналам связи;
8. заражение компьютера или телефона/планшета держателя карты с целью получения данных;
9. потеря владельцем карты денежных средств при использовании платежной карты третьми лицами после ее кражи/потери
 |
| ***Процессинг платежей принятых через платежные терминалы:*** | Убытки, понесенные банком вследствие: 1. кража или акт вандализма физического характера на терминальных устройствах;
2. кража терминала с целью подключения его к сети и «прокатывание» платежей в свою пользу;
3. мошеннический доступ к системам «электронных денег»;
4. заражение компьютерными «вирусами» и «троянами», что, в случае получения злоумышленником контроля над терминалом, может позволить ему проводить незаконные платежи, создавать новых получателей платежей, подменять «иконки» на сенсорном экране терминала, удалять или добавлять записи, накапливающиеся в файле терминала для «офлайн-платежей», а также подменять логи валидатора и чекового принтера (или, с недавнего времени, контрольно-кассовой техники);
5. атака на трафик GPRS-модема;
6. атака на серверную часть программного обеспечения (или шлюзы платежных систем, поставщиков услуг), к которым подключаются терминалы на хранимые ключи электронно-цифровой подписи, и на сопутствующую информацию (логи, адреса и другая информация об агентах, поставщиков используемая позже для "фишинга"), и на хранилище обновлений к программному обеспечению (и заражение их вирусами);
7. получение несанкционированного доступа к счетам банка через терминальные устройства
8. Злоумышленник использует известную и неустраненную уязвимость, чтобы получить доступ к серверу, на котором размещен процессинг.
 |
| ***Другое*** | Убытки, понесенные банком вследствие: 1. кража конфиденциальной информации банковских карт клиентов (скимминг/шимминг);
2. кража банковской карты путем ее механической блокировки в картридере банкомата («ливанская петля»);
3. кража наличных денег клиента путем захвата и удержания банкнот в устройстве выдачи банкомата;
4. ложная отмена банковской или платежной операции;
5. установка подложных банкоматов («банкоматов-клонов»);
6. создание «сайтов-клонов» кредитных организаций, а также «сайта-клона» официального сайта банка;
7. создание мошеннических страниц в социальных сетях с использованием логотипа и названия банка, приведшие к убыткам банка
8. рассылка на сотовые телефоны держателей банковских карт сообщений от имени банка о блокировке банковской карты;
9. получение несанкционированного доступа к счетам банка через терминальные устройства/мобильные/электронные кошельки/любые другие каналы дистанционного банкинга
10. государственной политики.
 |

Участник тендера вправе дополнить коммерческое предложение любыми предложениями, которые являются по мнению участника преимуществом.

Ценновое предложение участников тендера в иностранной валюте, для принятия решения конвертируется в национальную валюту по официальному курсу валют НБКР. При заключении договора с банком требуется открытие счета в банке ЗАО «ФИНКА Банк».

**Приложение № 4**

В тендерную комиссию

ЗАО «ФИНКА Банк»

«\_\_\_\_» \_\_\_\_\_\_\_\_\_ 202\_\_г.\_\_\_\_\_\_\_\_

Настоящим, на ваш запрос относительно информации о судебных исках, сообщаем следующее.

 По состоянию на \_\_\_\_\_\_\_\_\_\_\_\_ 202\_\_ года ОсОО / ЧП «\_\_\_\_\_\_\_\_\_\_\_\_» выступает/не выступает ответчиком/истцом по \_\_\_\_\_\_\_\_\_\_\_\_ (количество) судебным делам (в случае вовлеченности в судебные тяжбы, предоставить подробную информацию относительно участников и суммы иска).

ОсОО / ЧП «\_\_\_\_\_\_\_\_\_\_\_\_» подтверждает, что вышеприведенная информация является достоверной и полной.

ОсОО / ЧП «\_\_\_\_\_\_\_\_\_\_\_\_» признает, что в случае преднамеренных искажений и упущений, это может послужить основанием для дисквалификации из участия в тендере.

С уважением,