# Приложение № 11

**ЗАЯВЛЕНИЕ О КОМПРОМЕТАЦИИ**

|  |  |  |  |
| --- | --- | --- | --- |
| **Клиент** | |  | |
| *указывается наименование организации, включая организационно-правовую форму / ФИО индивидуального предпринимателя / физического лица, занимающегося частной практикой* | | | |
| в лице | |  | |
| действующий на основании | | |  |
| ИНН | | |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  |  |  |  |  |  |  |  |  |  |  |  | | |
| **НАСТОЯЩИМ ЗАЯВЛЕНИЕМ КЛИЕНТ** | | | |
| 1. **Уведомляет** о наступлении события, связанного с Компрометацией или подозрением на Компрометацию: | | | |
|  | Ключа ЭП, указать идентификатор Ключа проверки ЭП[[1]](#footnote-1) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | |
|  | Ключа PayControl | | |
|  | Ключевого носителя (USB-токена) | | |
|  | Мобильного устройства (при использовании Ключа PayControl) | | |
|  | Пароля | | |
|  | Устройства подтверждения | | |
|  | Иное \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | |
| в отношении **Уполномоченного лица** | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ФИО (полностью)**  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | **СНИЛС \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | **е-mail и телефон для направления Логина и Пароля**[[2]](#footnote-2) | **\_\_\_\_\_\_\_\_\_@\_\_\_\_\_\_\_\_\_\_** |
| **+7 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |

|  |
| --- |
| 1. **Просит заблокировать скомпрометированные Ключ ЭП /Ключ PayControl/устройство, указанные в п. 1 настоящего Заявления** |

|  |
| --- |
| 1. **Просит для возобновления работы в Системе ДБО выдать Уполномоченному лицу / принять от Уполномоченного лица (при необходимости):**   *В случае если у Уполномоченного лица (УЛ) несколько типов полномочий, заявление дополняется дополнительным блоком* |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Полномочия** | | **Дополнительно** | | **Вариант защиты Системы и подтверждения исполнения документов**  **(нужное отметить)** | | |
|  | **группа 1** |  | **выдать USB-токен Банка** | **Способ** | **Обязательное подтверждение исполнения платежного документа**[[3]](#footnote-3)**:** | **Дополнительно для входа в Систему**[[4]](#footnote-4)**:** |
|  | **группа 2** |  | **принять USB-токен Клиента** | **SMS-сообщение на номер +7 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |  |  |
|  | **просмотр** |  | **выдать Устройство подтверждения**[[5]](#footnote-5) |
| **Устройство подтверждения**5 |  |  |
|  | **акцепт (визирование)**[[6]](#footnote-6) |  | **выдать Ключи инициализации PayControl** |

**Клиент подтверждает достоверность сведений, содержащихся в настоящем Заявлении о компрометации.**

**ПОДПИСЬ КЛИЕНТА**

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| подпись |  |  | дата |

МП

**ОТМЕТКИ БАНКА**

|  |  |  |
| --- | --- | --- |
| Настоящее Заявление принято\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Дата | | |
|  |  |  |
| Подпись |  | фамилия, инициалы |

1. Поле заполняется, если Уполномоченное лицо имеет несколько Ключей ЭП. Данные об идентификаторе Ключа проверки ЭП доступны Клиенту в разделе «Безопасность» / «Запросы на новый сертификат» Системы «ДБО «BS-Client CORREQTS»/ в разделе «Электронные подписи» Системы iBank или на бумажном экземпляре бланка Ключа проверки ЭП в поле «Идентификатор ключа». [↑](#footnote-ref-1)
2. Для «ДБО BS-Client (CORREQTS)». [↑](#footnote-ref-2)
3. При выборе PayControl подтверждение платежа осуществляется в мобильном приложении PayControl [↑](#footnote-ref-3)
4. Не применяется при использовании Мобильного приложения Банка [↑](#footnote-ref-4)
5. Разрешено использование устройств: ключ OTP eToken Pass Event (в системе «ДБО BS-Client (CORREQTS)») и МАС-токен BIFIT (в системе «iBank») [↑](#footnote-ref-5)
6. Предоставляется уполномоченному лицу в случае указания порядка приема электронных платежных документов «с визирующей подписью. [↑](#footnote-ref-6)