

Краткая памятка для юридических лиц: Действия при инциденте информационной безопасности

Что такое инцидент ИБ? Событие, угрожающее безопасности данных, платежей, денег на счетах или вызывающее странное поведение компьютера.

Тревожные сигналы: фишинговое письмо, самопроизвольные платежи, ошибка в Клиент-банк (Web), неясное списание средств, неконтролируемая работа системы (самодвижущийся курсор мыши или открывающиеся окна и действия на экране).

1. Выявление инцидента

- **Сбор информации** Запишите (на бумаге или в телефоне):
 - Дату и время.
 - Сумму и номер платёжного документа.
 - Краткое описание (например, ошибка в платежке, неясное списание, письмо от мошенников).
- Сохраните доказательства: сделайте скриншоты или сохраните сообщения об ошибках.

2. Уведомление и изоляция

- **Отключите USB носитель ключа ЭЦП** от компьютера.
- **Уведомление банка** Позвоните своему менеджеру или в Контакт-центр (см. раздел 5) для рекомендаций.
- **Немедленная блокировка** По инструкциям банка (через менеджера или Контакт-центр) заблокируйте счета, карты и ДБО.
- При утечке данных клиентов/контрагентов уведомите **свое руководство** в течение 1 часа.
- Проверьте наличие резервных копий данных (например, экспорт платежей из Клиент-банк (Web)).
- Отключите устройство от интернета (выдерните кабель, выключите Wi-Fi), но не выключайте компьютер.
- Ограничьте доступ к системе (запретите сотрудникам вход).

3. Реагирование

- При пропаже денег или данных, либо при обнаружении попытки подобного действия, обратитесь в **милицию** в течение 1–2 часов. Подайте заявление, укажите: время, сумма, доказательства (скриншоты).
- Перед возобновлением работы: обновите антивирус, смените пароли, проверьте и при необходимости перевыпустите ключ ЭЦП.

4. Уведомления

- **Срочно** уведомите (**НЦЗПД**) **Национальный центр защиты персональных данных Республики Беларусь** при утечке персональных данных в течение 24 часов (Закон № 99-З, 07.05.2021). Укажите описание утечки. Контакты: см. раздел 5.
- Сообщите клиентам и контрагентам, если их данные затронуты. Не разглашайте детали без согласования.

5. Контакты

- **Банк:** Номер менеджера _____, Контакт-центра **147** или Центр поддержки пользователей **(017) 309-04-04** (проверьте на сайте банка или в договоре).
- **НЦЗПД:** cpd.by
- **Милиция:** 102.

6. Профилактика

- Установите антивирус.
- Ознакомьтесь с полезной информацией на сайте банка в разделе Безопасная работа в системах ДБО - <https://belarusbank.by/o-banke/safe-dbo/>
- Регулярно проверяйте системы на слабые места.

7. После инцидента

- Подтвердите у банка и НЦЗПД (если уведомляли), что инцидент решен.
- Проверьте активность счетов после инцидента.
- Распечатайте эту памятку как чек-лист (выделите срочные шаги красным).