Система ДБО – как обезопасить себя?

Статистика от ЦБ

- В 2022 г. у юридических лиц - клиентов Российских банков **без согласия** было проведено **4,84 тыс. операций на общую сумму 807,67 млн руб.**, т.е. средняя сумма одной операции составила 166,91 тыс. руб.[1]
- Доля возмещенных (возвращенных) средств (от объема) по операциям без согласия клиентов (далее – ОБС) через канал дистанционного банковского обслуживания (ДБО) юридических лиц за III квартал 2022 года составила **всего 4,6%** [2]

ОБС со счетов юридических лиц имеют характерный признак – большие суммы каждой операции в отдельности.

При проведении подобной операции со счетов юридических лиц злоумышленники для успешного ее осуществления в лучшем случае имитируют модель типичных для деятельности юридического лица операций, а в худшем – **ограничены только количеством денежных средств на банковском счете юридического лица.**

Т.е. совокупно операции, совершенные без согласия клиентов по каналам ДБО юридических лиц, характеризуются **значительными суммами и малым процентом возмещения**.

Кто может пострадать от финансовых мошенников?

Пострадать от действий финансовых мошенников может любой человек, независимо от его возраста и статуса. Тем не менее опрос Банка России позволил сформировать среднестатистический портрет клиента банка, наиболее уязвимого для обмана:

- Возраст от 25 до 44 лет.
- Проживает в городе.
- Работающий мужчина со средним уровнем дохода и средним образованием.
- Активно пользуется банковскими онлайн-сервисами. [1]

Как происходят операции без согласия по каналам ДБО?

Можно выделить 2 основных пути:

1. Злоумышленники **путем обмана или злоупотребления доверием** с использованием «социальной инженерии» **убеждают Клиента выполнить действия**, которые приводят к совершению операции без согласия[3].

Пример:

«На рынке действует организация «Ромашка», которая занимается поставкой цветов. Компания существует давно и зарекомендовала себя в качестве надёжного контрагента. Мошенники регистрируют фирму-однодневку с таким же названием. Возможно, даже дублируют сайт компании, и выходят на заказчиков. С заказчиком заключают договор, высылают счёт и реквизиты. ИНН указан реально существующей на рынке организации, а расчётный счёт принадлежит мошенникам.

Заказчик проверяет компанию по ИНН и убеждается в её реальности. Если он не сверит расчётный счёт, который прислали аферисты, с реальным, подозрений не возникнет. Даже если заказчик сверит счета и найдёт расхождения, это вряд ли его смутит, ведь у крупной компании может быть несколько расчётных счетов. В итоге деньги уходят злоумышленникам».

2. Злоумышленники путем **использования зараженных ресурсов** (фишинговых сайтов или рассылок по электронной почте с вредоносными вложениями) и **эксплуатации уязвимостей программного обеспечения на компьютере Клиента получают к нему доступ и возможность удаленного управления**, что приводит к совершению операции без согласия.

1 ЦБ – Обзор операций, совершенных без согласия клиентов финансовых организаций https://cbr.ru/analytics/ib/operations_survey_2022/
2 ЦБ – Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств за III квартал 2022 года https://cbr.ru/analytics/ib/review_3q_2022/
3 В значении, используемом в Федеральном законе от 27.06.2011 N 161-ФЗ (ред. от 28.12.2022) "О национальной платежной системе"
4 Кибергигиена – это образ мышления и привычки с фокусом на безопасность, помогающие пользователям и организациям снизить количество нарушений в интернете.
5 https://www.sevnb.ru/public/files/dbo/2022/dbo_rules.pdf
6 не является публичной офертой, Банк не осуществляет продажу, тиражирование, разработку, предоставление во временное пользование указанного ПО

Пример:

«Клиент скачал из Интернета программу для редактирования фотографий, но она содержала в себе вредоносный код и позволяла злоумышленникам подключаться к компьютеру Клиента без его ведома. Злоумышленники в течение некоторого времени следили за работой Клиента в ДБО и узнали его пароль и пинкод. В момент, когда Клиент подключил токен к компьютеру и вошел в ДБО, на компьютере Клиента отобразился "синий экран смерти" с сообщением, что сейчас осуществляется сохранение информации об ошибке. В момент "сохранения информации" к компьютеру удаленно подключился злоумышленник и создал в уже открытом интерфейсе ДБО мошеннический платеж».

Как можно обезопасить себя от операций без согласия?

☑ Прежде всего через повышение уровня финансовой грамотности и формирование кибергигиены [4]

☑ **Корректно настройте и используйте технические средства для работы с системой ДБО**

- ☐ используйте только лицензионное ПО фирм-изготовителей
- ☐ исключите возможность удаленного управления и администрирования компьютера
- ☐ правом установки и настройки должен обладать только уполномоченный сотрудник (администратор) - всем остальным пользователям необходимо назначить минимально возможные права
- ☐ используйте антивирусное программное обеспечение
- ☐ регулярно устанавливайте пакеты обновления безопасности ОС (Service Packs, Hot fix и т.п.) и ПО, обновляйте антивирусные базы
- ☐ при подключении к общедоступным сетям связи используйте дополнительные методы и средства защиты (например: межсетевой экран, VPN и т.п.)

Все требования к рабочему месту системы ДБО и организации работы с ней, которые помогут снизить риск осуществления ОБС, подробно описаны в Правилах использования СКЗИ и ЭП (Приложение 1 к Правилам «Дистанционного банковского обслуживании по счетам юридических лиц и индивидуальных предпринимателей» [5])

☑ **Установите ограничения на максимальную сумму, перечень возможных получателей, временной период, перечень устройств для работы в ДБО.** Для этого заполните Заявление на установку ограничений в Системе дистанционного банковского обслуживания (ДБО) (Приложение 4 к Правилам «Дистанционного банковского обслуживании по счетам юридических лиц и индивидуальных предпринимателей» [5])

☑ **Подключите услугу оперативного информирования о расходных операциях**. Для этого заполните Заявление на подключение услуги оперативного информирования о расходных операциях (Приложение 3 к Правилам «Дистанционного банковского обслуживании по счетам юридических лиц и индивидуальных предпринимателей» [5])

☑ **Посетите fincult.info** — информационно-просветительский ресурс, созданный Центральным банком Российской Федерации. Его цель — формирование финансовой культуры граждан.

Сколько стоит безопасность?

Практика показывает, стоимость внедрения рекомендованных мероприятий по соблюдению кибергигиены несоизмерима с Вашими возможными потерями.

На 1 рабочее место [6]

Антивирус **2 346 ₽**
VPN **6 043 ₽**
Сканер уязвимостей **5 500 ₽**

<

Средняя сумма одной мошеннической операции [1]

166 910 ₽

1 ЦБ – Обзор операций, совершенных без согласия клиентов финансовых организаций https://cbr.ru/analytics/ib/operations_survey_2022/
2 ЦБ – Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств за III квартал 2022 года https://cbr.ru/analytics/ib/review_3q_2022/
3 В значении, используемом в Федеральном законе от 27.06.2011 N 161-ФЗ (ред. от 28.12.2022) "О национальной платежной системе"
4 Кибергигиена – это образ мышления и привычки с фокусом на безопасность, помогающие пользователям и организациям снизить количество нарушений в интернете.
5 https://www.sevnb.ru/public/files/dbo/2022/dbo_rules.pdf
6 не является публичной офертой, Банк не осуществляет продажу, тиражирование, разработку, предоставление во временное пользование указанного ПО