

ОРГАНИЗАЦИОННЫЕ МЕРЫ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОЙ РАБОТЫ В СИСТЕМЕ FAKTURA.RU

1. Требования по защите от вредоносного кода:

1.1. К средствам защиты от вредоносного кода относятся средства, используемые для:

- выявления и обезвреживания вредоносного кода (антивирусы);
- межсетевого экранирования рабочего места или корпоративной сети;
- Web-фильтрации;
- обнаружения и предотвращения вторжений;
- контроля выполнения приложений.

2. Для обеспечения надлежащей защиты от вредоносного кода Клиент обязан:

- обеспечить непрерывное использование средств защиты от вредоносного кода;
- обеспечить периодический контроль целостности системного, прикладного и специального программного обеспечения;

- ежедневно осуществлять проверку рабочего места на наличие вредоносного кода;

обеспечить регулярное обновление средств защиты от вредоносного кода, обновление прикладного программного обеспечения, установку пакетов обновления безопасности операционной системы;

- использовать лицензионное программное обеспечение;

использовать для работы в Системе учетную запись, не входящую в группу «Локальные администраторы» или аналогичную группу пользователей;

- на мобильном устройстве (смартфоне) не повышать полномочия до пользователя root;

осуществлять вход в Систему с рабочего места используемого исключительно для подключения к Системе;

ограничивать по времени доступ ответственных лиц к ПЭП и/или телефону, на который приходят СМС – подтверждения платежей;

- контролировать суммы переводов, реквизиты получателей.

1. Для защиты ПЭП необходимо:

1.1. Для входа в Систему вводить логин и пароль только на сайте Системы, убеждаться в подлинности сайта Системы до ввода реквизитов доступа.

1.2. Никогда и ни при каких обстоятельствах не сообщать никому свои логины, пароли, СМС/Push коды.

1.3. Обязательно сверять текст СМС-сообщений, содержащий пароль, с деталями выполняемой операции. Если в СМС указан пароль для платежа, который вы не совершали или его предлагают ввести/назвать, чтобы отменить якобы ошибочно проведенный по счету платеж, ни в коем случае не вводить его и не сообщать его никому, в том числе сотрудникам Банка.

1.4. В случае утери мобильного телефона, на который приходят разовые пароли, немедленно заблокировать соответствующую SIM-карту у оператора сотовой связи.

1.5. Записать контактный телефон Банка в адресную книгу или запомнить его. В случае если в личном кабинете Системы вы обнаружите телефон, отличный от записанного, в особенности, если вас будут призывать позвонить по этому телефону для уточнения информации, либо по другому поводу, будьте бдительны и немедленно позвоните в Банк по ранее записанному вами телефону.

1.6. Устанавливать мобильные приложения Системы только из авторизованных магазинов. Использовать антивирусное программное обеспечение для смартфона.

1.7. Избегать регистрации номера мобильного телефона, на который приходят СМС-сообщения с разовым паролем, в социальных сетях и других открытых источниках.

2. Общие правила безопасности, применяющиеся для защиты любых данных, хранящихся на компьютере:

2.1. Использовать только компьютеры с лицензионным программным обеспечением, установленным и запущенным антивирусным программным обеспечением и персональным межсетевым экраном, своевременно обновлять антивирусные базы. Регулярно проводить полную проверку компьютера на предмет наличия вредоносного кода, своевременно обновлять лицензионную операционную систему и браузеры.

2.2. Проверять действительность сертификата веб-сайта Системы. При вводе личной информации, помнить, что любой веб-адрес в адресной строке Интернет-банка должен начинаться с «https». Если в адресе не указано «https», это значит, что вы находитесь на незащищенном веб-сайте, и вводить данные нельзя.

2.3. Использовать виртуальную клавиатуру для ввода пароля.

2.4. Быть внимательным: в случае возникновения подозрений на мошенничество необходимо максимально быстро сообщить о своих подозрениях в Банк с целью оперативного блокирования доступа к вашей учетной записи в Системе.

2.5. При работе с электронной почтой не открывать письма и вложения к ним, полученные от неизвестных отправителей, не переходить по содержащимся в таких письмах ссылкам.

2.6. Не работать с правами администратора при отсутствии необходимости. В повседневной практике входить в систему как пользователь, не имеющий прав администратора.

2.7. Включить системный аудит событий, регистрирующий возникающие ошибки, вход пользователей и запуск программ, периодически просматривать журнал и реагировать на ошибки.

2.8. Запретить в межсетевом экране соединения по неиспользуемым протоколам.

2.9. Не давать разрешения неизвестным программам выходить в Интернет.

2.10. При работе в Интернете не соглашаться на установку каких-либо дополнительных программ от недоверенных издателей.