Утверждено
Решением Правления
АО «Таганрогбанк»

(протокол № 47 от 20.09.2021 г.)

РЕКОМЕНДАЦИИ И ТРЕБОВАНИЯ
клиентам АО «Таганрогбанк» по обеспечению информационной безопасности

Введено с 20.09.2021 года
приказом № 190 от 20.09.2021 г.

Таганрог
2021

1. Общие положения

1.1. Данные рекомендации разработаны на основании:
- — Пункта 7 «Положения Банка России от 17 апреля 2019 года № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента»;
- — «Методическими рекомендациями по усилению кредитными организациями информационной работы с клиентами в целях противодействия несанкционированным операциям» от 19 февраля 2021г. №3-МР;
- — «Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденной приказом ФАПСИ от 13 февраля 2001 года №152;
- — «Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации» (Положение ПКЗ-2005), утвержденное Приказом ФСБ России от 9 февраля 2005г. №66;
- — Эксплуатационной и технической документации на систему дистанционного банковского обслуживания «iBank 2» и используемые в процессе осуществления услуг средства защиты информации.

1.2. Информационная безопасность автоматизированных рабочих мест Клиентов (далее по тексту — АРМ) должна обеспечиваться с использованием комплексных мер и средств.

2. Обязательные требования по обеспечению информационной безопасности

2.1. АО «Таганрогбанк» ниже приводит требования к применению Клиентами с целью обеспечения информационной безопасности:
- 2.1.1. Используйте лицензионные операционные системы.
- 2.1.2. Используйте лицензионное программное обеспечение.
- 2.1.3. Используйте лицензионное антивирусное программное обеспечение.
- 2.1.4. Регулярно устанавливайте рекомендуемые разработчиком операционных систем и программного обеспечения обновления безопасности.
- 2.1.5. Регулярно обновляйте базы данных и сигнатуры антивирусного программного обеспечения.
- 2.1.6. Используйте сложные пароли (минимальное количество символов — 8, строчные и заглавные буквы, цифры, спецсимволы).
- 2.1.7. Регулярно, не реже одного раза в 90 дней, производите смену пароля.
- 2.1.8. Не передавайте устройства аутентификации (носители ключей, токены) и банковские карты третьим лицам.
- 2.1.9. Не передавайте учётные данные (логин, пароль, код из SMS, кодовое слово, номер карты, срок действия карты, ПИН и т. п.) третьим лицам.
- 2.1.10. Не храните учётные данные и данные банковских карт в открытом виде.
- 2.1.11. Не используйте устаревшие версии операционных систем, более не поддерживаемые разработчиком.

3. Общие рекомендации по обеспечению информационной безопасности

3.1. Разграничьте полномочия пользователей АРМ (в том числе с использованием разных учётных записей с разными правами пользователей, родительский контроль и т. п.).

3.2. Ограничьте использование внешних накопителей информации (USB, FLASH, HDD, CD и т. п.).

3.3. Устанавливайте стороннее программное обеспечение только из доверенных источников (официальный сайт разработчика, личный кабинет и т.п.).

3.4. Перед установкой того или иного программного продукта, выполняйте проверку антивирусом установочного пакета (.exe, .msi и др.).
3.5. В случае распространения установочных файлов в сжатом виде (в виде архива .zip, .rar и др.) проводите обязательную проверку антивирусными средствами.
3.6. Не открывайте архивы и не запускайте установку программного обеспечения без полной уверенности в отсутствии вредоносного кода!
3.7. Выходите из системы (с сайта, личного кабинета) по окончании работы (закрывайте сессию пользователя!).
3.8. Немедленно прекратите работу с системой и отключите АРМ в случае обнаружения подозрительной активности, а также незамедлительно сообщите в Банк о возможной компрометации учётных данных.
3.9. Проверяйте адрес системы дистанционного банковского обслуживания в адресной строке браузера (адрес должен начинаться с HTTPS и слева от адреса должен отображаться соответствующий символ, как правило, — зелёный замок).
3.10. Контролируйте дату и время последнего входа в систему.

4. Рекомендации юридическим лицам

4.1. Используйте систему дистанционного банковского обслуживания на отдельном персональном компьютере.
4.2. Используйте пароль на BIOS/загрузчик АРМ.
4.3. Установите запрет загрузки АРМ с использованием внешних устройств (USB, FLASH, HDD, CD и т. д.).
4.4. Ограничьте доступ к АРМ других пользователей.
4.5. Ограничьте кол-во учетных записей с повышенными привилегиями (права администратора) в операционной системе до минимально необходимых.
4.6. При использовании операционных систем Windows удостоверьтесь в том что компонент безопасности UAC (контроль учетных записей) включен и работает исправно, если Ваша версия операционной системы включает данный компонент.
4.7. Не используйте Автоматический вход в учетную запись операционных систем (автологин).
4.8. Ограничьте посещение сети интернет с АРМ (средствами антивирусного ПО, шлюзов безопасности и др.).
4.9. Ограничьте использование входящей почты, в том числе с использованием web-интерфейса на АРМ (используйте проверенные почтовые клиенты).
4.10. Используйте специализированные средства защиты информации от несанкционированного доступа («Аккорд», «Соболь» и т. п.).
4.11. Исключите доступ к АРМ (в том числе обслуживание) ненадежных IT-сотрудников (например, фрилансеров).
4.12. Обеспечьте контроль использования АРМ (контроль включения логов, журналов учёта событий программного обеспечения и операционных систем, произведение визуального контроля во время обслуживания устройства и т. п.).
4.13. В случае физического повреждения носителя ключевой информации, но сохранения работоспособности, не дожидайтесь полного выхода из строя устройства, произведите замену на полностью исправный экземпляр.

5. Рекомендации физическим лицам

5.1. При работе используйте АРМ, которое не подвергалось операциям повышения привилегий или взлома операционной системы.
5.2. Загружайте программное обеспечение только из официальных источников (сайт АО «Таганрогбанк», сайт АО «БИФИТ», сайт АО «Актив-софт» и др.).

5.3. Убедитесь, что на АРМ не установлены сомнительные приложения и (или) приложения из сомнительных источников.
5.4. Убедитесь, что вы не подключали АРМ к устройствам, безопасность которых не гарантирована.

6. Требования по информационной безопасности ключевой информации

6.1. Генерируйте криптографические ключи самостоятельно (генерация может также осуществляться работником Банка на территории Банка при необходимости в Вашем присутствии).
6.2. Порядок хранения и использования носителей ключевой информации должен исключать возможность несанкционированного доступа к ним.
6.3. Храните носители ключевой информации только самостоятельно.
6.4. Используйте надежные металлические сейфы или запираемые шкафы для хранения носителей ключевой информации.
6.5. Хранение носителей ключевой информации допускается в одном сейфе с другими документами, при этом отдельно от них, и в упаковке, исключающей возможность негласного доступа к ним посторонних лиц.
6.6. Определите приказом или распоряжением список лиц, имеющих доступ к носителям ключевой информации, и наделите их соответствующими полномочиями.
6.7. Во время работы с носителями ключевой информации исключите доступ к ним посторонних лиц.
6.8. Производите подключение устройств идентификации и аутентификации только непосредственно во время работы с системой.
6.9. При увольнении работников производите блокировку ключевой информации.
6.10. Запрещается копирование ключевой информации на иные машинные носители информации.
6.11. Запрещается передавать носители ключевой информации лицам, к ним не допущенным.
6.12. Запрещается выводить секретные ключи на дисплей или принтер.
6.13. Запрещается вставлять носитель ключевой информации в считывающее устройство компьютера в режимах, не предусмотренных функционированием АРМ, а также в считывающие устройства других компьютеров.
6.14. Запрещается оставлять носитель ключевой информации без присмотра на рабочем месте.
6.15. Запрещается записывать (производить попытки записи) на носитель ключевой информации посторонние файлы.
6.16. Запрещается подключать носитель ключевой информации к заведомо неисправным портам АРМ (во избежание физического повреждения носителя ключевой информации).

7. Противодействие фишингу

7.1. Фишинг — вид мошенничества, целью которого является получение доступа к аутентификационным данным Клиента.
7.2. Наиболее актуальные виды фишинга:
— телефонные звонки (социальная инженерия – звонки от служб безопасности Банков, предупреждения о подозрительных операциях и т.п.);
— подделка интернет-сайта компании (фишинговые сайты);
— смс-рассылки (смс-фишинг) с просьбой перевести те или иные средства по номеру телефона или счету;
— электронные письма (спам-рассылки).
7.3. Регулярно обновляйте программное обеспечение (в том числе, используемый браузер) и операционную систему (прошивку).

7.4. Установите панель инструментов или расширение веб-браузера для защиты от известных фишинговых веб-сайтов (зачастую в комплекте с антивирусным средством поставляются расширения для защиты веб-браузеров).
7.5. Запускайте антивирусное программное обеспечение и регулярно обновляйте его (при технической возможности включите автоматическое обновление).
7.6. Используйте брандмауэр.
7.7. Используйте корпоративные VPN и/или фильтрацию почтового трафика.
7.8. Не отвечайте на подозрительные сообщения, не переходите по ссылкам в них, и не загружайте вложения.
7.9. Не доверяйте электронной почте или веб-сайту, который запрашивает личную, корпоративную или финансовую информацию.
7.10. Не копируйте и не вставляйте ссылки из писем.
7.11. Проверяйте содержание писем на грамматические и орфографические ошибки.
7.12. Никогда не нажимайте ненадежные сокращенные URL-адреса (например, ow.ly, bit.ly и т.д.).
7.13. Не вводите учётные данные в случае возникновения подозрений.
7.14. Проверяйте адрес отправителя.
7.15. Проверяйте адрес сайта, в том числе, на защищенность (указанное в начале адресной строки HTTPS указывает на защищенность сайта).
7.16. Вводите адрес сайта вручную.
7.17. Не сообщайте по телефону свои учётные данные и коды из SMS.
7.18. В случае возникновения подозрений, самостоятельно свяжитесь с Банком, используя указанный в документах или на официальном сайте Банка номер телефона.