

**РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ ОТ ВОЗДЕЙСТВИЯ
ПРОГРАММНЫХ КОДОВ, ПРИВОДЯЩИХ К НАРУШЕНИЮ
ШТАТНОГО ФУНКЦИОНИРОВАНИЯ СРЕДСТВ
ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ В ЦЕЛЯХ ПРОТИВОДЕЙСТВИЯ
НЕЗАКОННЫМ ФИНАНСОВЫМ ОПЕРАЦИЯМ**

Оглавление

1. Перечень сокращений.....	3
2. Общие положения.....	4
2.1. Область применения и нормативная база	4
2.2. Цель рекомендаций.....	4
3. Рекомендации при работе с персональным компьютером (АРМ, ноутбук)	5
3.1. Требования к установке и обновлению ПО	5
3.2. Требования к антивирусной защите.	5
3.3. Контроль конфигурации и физического доступа	5
3.4. Блокировка компьютера при уходе.....	5
4. Рекомендации при работе с информационно-телекоммуникационной сетью «Интернет»	6
4.1. Общие принципы безопасности в Интернете	6
4.2. Обработка файлов и вложений из внешних источников	6
4.3. Защита от фишинга и социальной инженерии	6
4.4. Использование защищённых каналов связи	7
5. Рекомендации по созданию, хранению и обновлению парольной защиты АРМ ...	8
5.1. Требования к паролям	8
5.2. Хранение и управление паролями	8
6. Рекомендации при работе и хранении носителя ключевой информации ЭП	10
6.1. Требования к хранению	10
6.2. Требования к использованию ЭП	10
6.3. Процедура отзыва компрометированного ключа.....	10
6.4. Защита ключевой информации при передаче	11

1. Перечень сокращений

Сокращение	Расшифровка
АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
АВПО	Антивирусное программное обеспечение
ДБО	Дистанционное банковское обслуживание
ЭП	Электронная подпись
ИБ	Информационная безопасность
МФА	Многофакторная аутентификация
НСД	Несанкционированный доступ
НФО	Некредитная финансовая организация
ОС	Операционная система
ПД	Персональные данные
ПО	Программное обеспечение
ППО	Прикладное программное обеспечение
СКЗИ	Средства криптографической защиты информации
УЦ	Удостоверяющий центр

2. Общие положения

2.1. Область применения и нормативная база

Настоящие Рекомендации разработаны в соответствии с требованиями:

- **Положением Банка России от 20.04.2021 № 757-П** «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций
- **ГОСТ Р 57580.1-2017** «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер»
- **Федеральным законом от 27.07.2006 № 152-ФЗ** «О персональных данных» (в редакции от 28.12.2024)

Настоящие Рекомендации применяются ко всем **некредитным финансовым организациям**, осуществляющим деятельность в сфере финансовых рынков.

2.2. Цель рекомендаций

Целью является обеспечение защиты информации от:

- несанкционированного доступа и модификации;
- воздействия вредоносного программного кода;
- утечек чувствительных данных клиентов;
- несанкционированного проведения финансовых операций;
- целевых киберпреступных атак;
- компрометации критичной инфраструктуры.

3. Рекомендации при работе с персональным компьютером (АРМ, ноутбук)

3.1. Требования к установке и обновлению ПО

На АРМ рекомендуется устанавливать **только лицензионное программное обеспечение**, приобретённое организацией и имеющее все лицензии, и сертификаты от поставщика, предварительно протестированное на совместимость.

На АРМ **обязательно проводить своевременное обновление** операционной системы и прикладного ПО в течение 30 дней от выпуска критичного патча согласно требованиям стандарта.

3.2. Требования к антивирусной защите.

На всех АРМ должно быть установлено **лицензированное антивирусное ПО (АВПО)** с актуальными базами.

Дополнительно к классическому антивирусу рекомендуется внедрить **решение EDR (Endpoint Detection & Response)** для обнаружения поведенческих аномалий и реагирования на компрометированные устройства в режиме реального времени.

3.3. Контроль конфигурации и физического доступа

Любые работы на АРМ, связанные с изменением конфигурации (программной или аппаратной), должны производиться **только квалифицированными сотрудниками** с соответствующим допуском и/или **под контролем ИБ-подразделения.**

На АРМ **рекомендуется блокировать USB-выходы** или использовать **USB-фильтрацию** для предотвращения несанкционированного подключения внешних устройств.

3.4. Блокировка компьютера при уходе

Сотрудникам **рекомендуется обязательно блокировать компьютер** при уходе с рабочего места, используя комбинацию клавиш **Win+L.**

Компьютер должен быть заблокирован или выключен в конце рабочего дня согласно политике ИБ организации.

4. Рекомендации при работе с информационно-телекоммуникационной сетью «Интернет»

4.1. Общие принципы безопасности в Интернете

При работе в сети Интернет сотруднику **рекомендуется**:

- Соблюдать требования российского законодательства, нормы корпоративной этики и требования трудовой дисциплины;
- **Не открывать** письма и вложения из неожиданных источников, особенно от неизвестных отправителей;
- **Проверять домен отправителя** — убедиться, что письмо пришло с официального адреса организации;
- Сообщать о подозрительных письмах в **ИБ-подразделение или SOC (Security Operations Center)** для анализа;
- **Не переходить по ссылкам** из писем, если вы не уверены в их источнике — вместо этого введите адрес вручную в браузер.

4.2. Обработка файлов и вложений из внешних источников

При необходимости переноса файлов из внешних источников (Интернет, USB-накопители, облачные сервисы) в производственную сеть **обязательно проверить файлы** на предмет вредоносного кода:

- Использовать **лицензированное АВПО с актуальными базами**;
- Использовать **SAST-сканеры** для анализа исходного кода;
- Проводить **изоляция** файлов в песочнице перед интеграцией в систему.

Запретить использование корпоративной почты для рассылки развлекательного, рекламного контента или материалов, не относящихся к должностным обязанностям согласно политике ИБ.

4.3. Защита от фишинга и социальной инженерии

Сотруднику **рекомендуется**:

- **В случае получения поздравительных писем, банковских уведомлений или иных сообщений**, заведомо не относящихся к производственному процессу, **удалять такие письма без открытия** — они могут содержать вредоносный код согласно методическим рекомендациям Банка России;

- **Проверять подлинность письма**, запросив подтверждение через официальный канал связи (позвонить в компанию, открыть личный кабинет официального сайта);

4.4. Использование защищённых каналов связи

При передаче конфиденциальной информации и ПД по сети Интернет **обязательно использовать защищённые каналы связи:**

- **HTTPS (TLS 1.2 или выше)** для веб-приложений;
- **VPN** для удалённого доступа к критичным системам;
- **Криптографическая защита** данных при хранении на облачных сервисах согласно требованиям ГОСТ Р 57580.1-2017.

5. Рекомендации по созданию, хранению и обновлению парольной защиты АРМ

5.1. Требования к паролям

Пароли должны соответствовать следующим требованиям согласно требованиям регулятора и нормативным стандартам

Требование	Описание
Минимальная длина	Не менее 8 символов для пользователей; не менее 16 символов для администраторов
Состав	Три или более из четырёх категорий: прописные буквы, строчные буквы, цифры, спецсимволы
Легко вычисляемые сочетания	Запретить (например: 112, qwerty, password)
Личная информация	Пароль не должен содержать имя пользователя, даты рождения, клички питомцев
Повторяющиеся символы	Запретить (например: 111111, wwwww)
История паролей	При смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях

5.2. Хранение и управление паролями

НЕ РЕКОМЕНДУЕТСЯ:

- Записывать пароли на бумаге, в текстовых файлах или электронных записных книжках

- Сообщать другим пользователям свой личный пароль
- Регистрировать других сотрудников в системе под своим паролем
- Использовать одинаковые пароли для разных систем

РЕКОМЕНДУЕТСЯ:

- Использовать **менеджеры паролей** для безопасного хранения паролей
- При необходимости передачи пароля другому сотруднику использовать **защищённый канал связи** или **двухэтапный процесс**;
- Изменять пароль **каждые 90 дней** согласно требованиям стандарта
- В случае подозрения на компрометацию пароля **немедленно изменить** его и уведомить ИБ-подразделение.

6. Рекомендации при работе и хранении носителя ключевой информации ЭП

6.1. Требования к хранению

НЕ рекомендуется:

- Оставлять носитель без присмотра;
- Хранить в ящике рабочего стола или других легкодоступных местах;
- Передавать носитель кому-либо (даже временно);
- Использовать один носитель для нескольких пользователей

РЕКОМЕНДУЕТСЯ:

- Хранить носитель в безопасном месте (сейф, дома и т.д.) согласно требованиям стандарта;
- Использовать **дополнительную защиту** (например, зашифровать накопитель);
- Иметь **резервный носитель**, хранящийся в другом месте;
- Применять **средства криптографической защиты информации (СКЗИ)**, сертифицированные ФСБ России при использовании ЭП.

6.2. Требования к использованию ЭП

При первой аутентификации необходимо **заменить временный пароль** на новый пароль.

При работе с носителем ключевой информации ЭП использовать **только лицензированные средства криптографической защиты информации (СКЗИ)**.

6.3. Процедура отзыва компрометированного ключа

В случае подозрения на компрометацию ключа ЭП:

- **Немедленно прекратить** использование скомпрометированного ключа;
- **Обратиться в Удостоверяющий центр (УЦ)**, выпустивший ключ, с запросом на **отзыв сертификата ЭП;**

- **Запросить выпуск нового ключа ЭП** в соответствии с установленной процедурой;
- **Уведомить ИБ-подразделение** о компрометации и провести анализ логов на предмет несанкционированного использования.

6.4. Защита ключевой информации при передаче

При передаче информации о ключах (например, начальных паролей, восстановительных кодов) **использовать защищённый канал связи:**

- Шифрование данных при передаче (HTTPS, TLS);
- Раздельная передача по разным каналам связи (половина по email, половина по телефону);