Приложение №4 к Письму
Министерства цифрового развития
и связи Кузбасса
от _____ № _____

Методические рекомендации
Алгоритм действий после взлома аккаунта руководителей

1.Немедленные действия (Первые 5-10 минут)

1.1) Немедленно проинформировать:

- ответственного за информационную безопасность Вашего органа государственной власти (организации) о взломе аккаунта для фиксации инцидента и получения помощи специалистов при необходимости.
- ближайших родственников
- коллег(секретарь, помощник), чтобы через рабочие группы в используемых мессенджерах оповестили о взломе аккаунта и возможном мошенничестве от имени взломанного аккаунта.

Примерный текст для информирования: «У меня взломали аккаунт [название мессенджера]. Не отвечайте на любые сообщения, которые могут прийти с этого номера, не открывайте файлы, ссылки и не отвечайте на попытки узнать любую конфиденциальную информацию. Новый аккаунт создам позже.»

1.2) Рекомендуется поставить статус во всех рабочих мессенджерах о взломе аккаунта с примерным текстом: «У меня взломали аккаунт [название мессенджера или социальной сети] - [имя аккаунта]. Не отвечайте на любые сообщения с этого аккаунта и ни в коем случае не открывайте отправленные с этого аккаунта файлы и ссылки».

1.3) Необходимо с Вашего мобильного устройства проверить и осуществить выход из всех активных сессий мессенджера/социальных сетей (завершить все сеансы). Если к аккаунту нет доступа, переходите к п.4:

- Telegram: пункт меню Настройки Устройства Завершить все другие сеансы.
- MAX: пункт меню Настройки Приватность Завершить все сессии, кроме текущей.
- VK пункт пункт меню Настройки Управление аккаунтом VK ID История активности Выйти на других устройствах.

1.4) Заблокируйте аккаунт через персональный компьютер, используя Yandex браузер (рекомендуется), если не можете войти с мобильного устройства:

- Telegram: перейдите на официальную страницу восстановления (скопировать ссылку в адресную строку браузера): https://my.telegram.org/auth?to=deactivate. На открывшемся сайте необходимо ввести свой номер телефона, подключенный к Telegram. Это временно заблокирует аккаунт, и злоумышленник не сможет им пользоваться. После этого, следуйте инструкциям по восстановлению аккаунта.
- VK/VK мессенджер: отдельно заблокировать аккаунты в системе VK невозможно, поэтому следуйте инструкциям по восстановлению из пункта «Восстановление контроля и безопасность».
- MAX: отдельно заблокировать аккаунт в MAX невозможно, следуйте инструкциям по

восстановлению аккаунта из следующего пункта.

2. Восстановление доступа

2.1) Восстановите доступ к аккаунту. Используйте официальные процедуры восстановления через SMS, email или техподдержку:

- Telegram: вам будет предложено восстановить аккаунт через номер телефона, так как это единственное, что связывает аккаунт и пользователя. После ввода номера на экране восстановления следуйте дальнейшим инструкциям на сайте.
- VK/VK мессенджер: перейдите на страницу входа в VK, выберете пункт «Забыли пароль?» и следуйте дальнейшим инструкциям на сайте по восстановлению. После восстановления, вы сможете зайти в VK и VK мессенджер под новым паролем.
- MAX: перейдите на страницу входа, введите номер телефона, на который должен прийти код подтверждения. Введите код подтверждения в предназначенное для него поле. Если у вас была подключена двухфакторная аутентификация, потребуется подтверждение через смс или приложение – генератор паролей.

2.2) Смените все пароли:

- Пароль от самого мессенджера (если он есть), либо от VK ID, так как это единый аккаунт для входа во все сервисы VK.
- Пароль от электронной почты, привязанной к аккаунту. Это критически важно, так как через почту часто сбрасывают пароли и возникает вероятность повторного взлома аккаунта.
- Пароль от самого номера телефона (личный кабинет у оператора связи), чтобы злоумышленник не мог перехватить SIM-карту.

Рассчитывайте на то, что ваши пароли скомпрометированы. Будет лучше сгенерировать новый сложный пароль в онлайн-генераторе (например randomus.ru), и записать в ежедневник или на листочке.

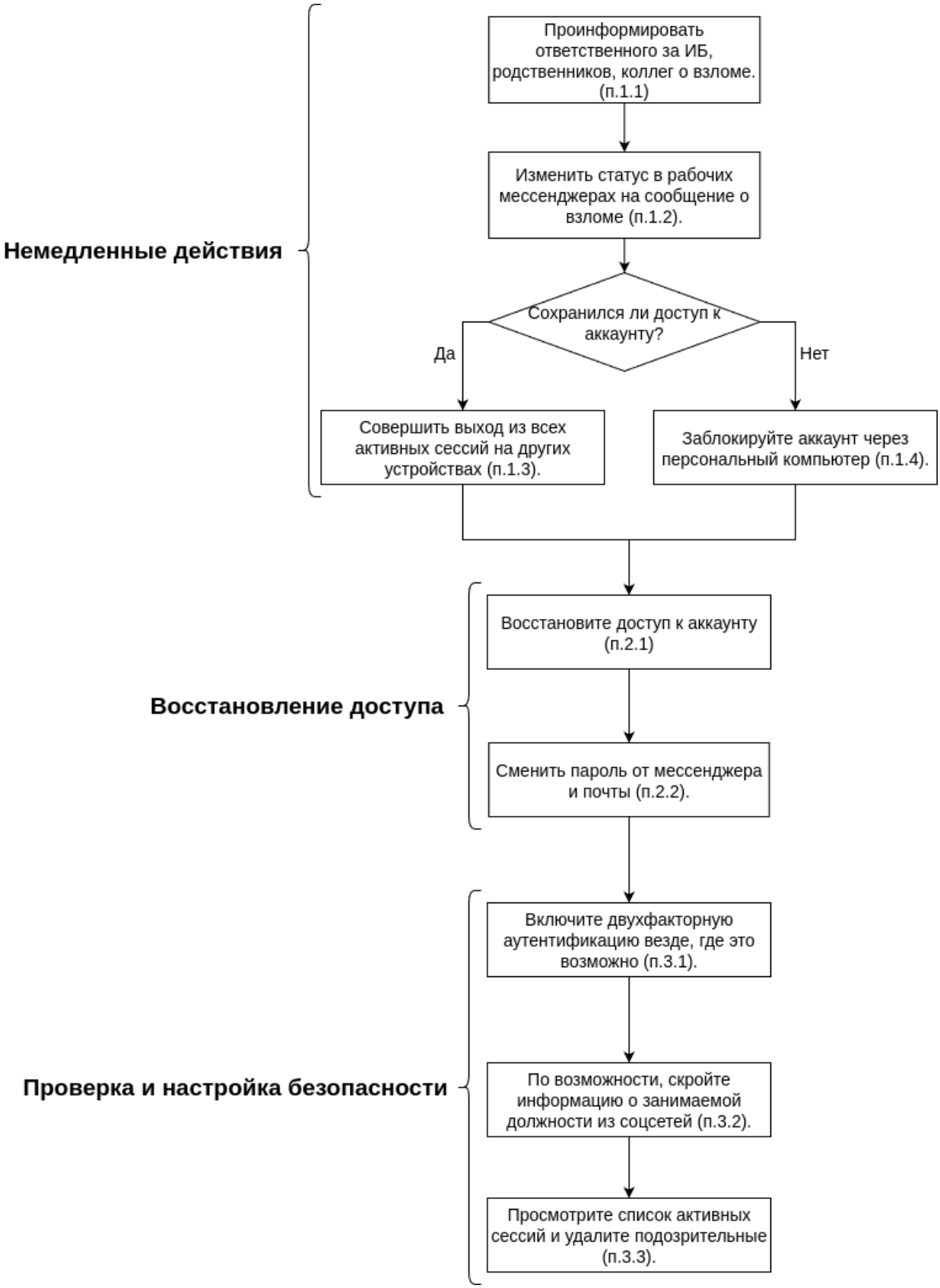
3. Проверка и настройка безопасности

3.1) Включите двухфакторную аутентификацию везде, где это возможно (Telegram, почта, социальные сети). Это главный барьер от взлома. В случае мессенджера MAX, есть возможность подключить аккаунт к VK ID (если вы регистрировались в VK) в настройках мессенджера.

3.2) Проверьте настройки конфиденциальности и общедоступную информацию на своей странице: кто может видеть ваш номер, фото, статус. Скройте или удалите все упоминания о занимаемой должности (по возможности), с целью минимизации целевых атак на свой аккаунт.

3.3) Просмотрите список активных сессий/подключенных устройств (п.3) и завершите все, которым не доверяете.

Блок-схема последовательности действий при взломе аккаунта



Рекомендации по предотвращению взлома аккаунтов

Цифровой след: старайтесь минимально оставлять свои личные данные при регистрации на сайтах в сети Интернет. Так же не рекомендуется использовать одинаковые пароли на разных сайтах. Иногда сайты могут взламывать, похищать базы данных пользователей и сливать их мошенникам.

Пароли: рекомендуется использовать сложные пароли, содержащие строчные и заглавные буквы, специальные символы, цифры. Рекомендуется использовать генератор паролей для создания максимальной сложности в подборе вашего пароля, например - randomus.ru.

Антивирусные программы: Для защиты от воздействия фишинговых рассылок и целенаправленного взлома рекомендуется использовать мобильный антивирус, например «Kaspersky Internet Security для Android», «Dr.Web Security Space» или иные. Если вы используете IPhone, установка сторонних программ для защиты устройства не рекомендуется из-за закрытости данной системы.

Рекомендации по защите от спам-рассылок и спам-звонков.

Подходит для всех систем:

Услуга «Антиспам» от оператора связи: подключается в приложении, личном кабинете на сайте либо салоне связи вашего оператора мобильной связи. Фильтрует звонки и сообщения на уровне оператора, благодаря чему спам не доходит до телефона в принципе.

Подходит для операционной системы Android:

Настройка от спам-звонков: Необходимо иметь установленный Яндекс браузер (при необходимости скачать из магазина приложений «RuStore»). На главной странице выбрать значок ⁘, после чего в списке «Инструменты» выбрать «определитель номера яндекс» и дать приложению запрашиваемые разрешения. Данная настройка при определенной конфигурации, позволяет автоматически блокировать спам-звонки и звонки с незнакомых номеров. Так же, показывает информацию о входящем звонке, и комментарий, например: «Предложение услуг банка».

Встроенный SMS-фильтр/фильтр входящих звонков: встроены почти в каждый современный смартфон. Позволяет фильтровать входящие SMS-сообщения и звонки по ключевым словам с чёрным и белым списком, по наличию номера в адресной книге и т. д. Настраивается обычно в настройках мобильного устройства, в приложении для обмена SMS-сообщениями и в приложении для совершения звонков.

Подходит для операционной системы iOS:

Так как система iOS является закрытой, сторонние приложения на ней работают с меньшей эффективностью, чем на Android. Лучший вариант для данной системы — использовать «антиспам» от оператора связи и встроенные функции мобильного устройства.

Тихие и неизвестные абоненты (Silence Unknown Callers): встроенная функция, включается в приложении «Настройки» «Телефон» «Звонки» «Тихие и неизвестные абоненты». Все звонки от неизвестных номеров перенаправляются на голосовой почтовый ящик без звонка, при этом, отклонённые звонки отображаются в списке последних вызовов. Отклоняет все спам-звонки, однако есть вероятность пропустить важный звонок, например от врача или курьера.

SMS-фильтр: встроенная функция, включается в приложении «Настройки» «Сообщения» «Фильтр незнакомых». После включения настройки, в приложении «Сообщения» появятся две вкладки: «Известные» и «Неизвестные». В раздел «Известные» попадают сообщения от номеров из вашей адресной книги, в раздел «Неизвестные» попадают сообщения от остальных номеров.

Рекомендации по предотвращению кражи данных посредством фишинга

Обращайте внимание на ссылки:

Подмена букв или домена: examp1e-bank.ru, example-bank.com вместо examplebank.ru, (цифра «1» вместо буквы «l», домен «.com» вместо «.ru»)
Использование HTTPS: в строке со ссылкой должен отображаться значок замка, а адрес начинаться с «https://».

Оценивайте содержание сообщения:

Угрозы и срочность: «Ваш аккаунт будет заблокирован в течение 2 часов!», «Подтвердите платеж, иначе вас оштрафуют!». Подобные угрозы явно указывают на мошенников.

Щедрые предложения: «Вы выиграли iPhone! Перейдите по ссылке, чтобы получить приз». Даже если вы участвовали в розыгрыше, в настоящих сообщениях о выигрыше не попросят перейти по ссылке или отправить денег, например за почтовую отправку вам подарка.

Ошибки и небрежность: официальные письма от организаций хорошо форматируются и орфографически точны. Грубые ошибки и небрежности указывают на обман.

Никогда не сообщайте конфиденциальные данные:

Настоящие организации никогда не будут спрашивать номер и пин-код банковской карты, код с обратной стороны карты, любые пароли, личные данные и коды подтверждения из смс.

Не скачивайте и не открывайте подозрительные вложения

Фишинговые письма часто содержат вложения (Word, Excel, PDF, ZIP) с якобы «выпиской», «квитанцией» или «уведомлением». Эти файлы могут содержать вредоносное ПО, которое заразит ваше устройство. Всегда проверяйте, от кого приходят подобные письма.

Используйте двухфакторную аутентификацию (2FA)

Это ваш главный защитный рубеж, даже если мошенники узнают ваш пароль.

Включайте 2FA везде, где это возможно (почта, соцсети, банки, мессенджеры).

Даже если украдут ваш логин и пароль, без одноразового кода из SMS или приложения-аутентификатора войти в аккаунт невозможно.

Пользуйтесь антифишинговыми технологиями

Антивирусы: Современные антивирусы имеют встроенные модули для проверки ссылок, файлов и блокировки фишинговых сайтов.

Браузеры: Такие браузеры, как Google Chrome, Mozilla Firefox, Safari, Яндекс.Браузер, постоянно обновляют свои черные списки опасных сайтов и предупреждают вас перед переходом на подозрительный ресурс.

Встроенный определитель номеров: На Android (Google Звонки) и iPhone (услуги операторов) помогут определить, что звонок от «Сбербанка» на самом деле поступает не с номера колл-центра банка.