ПАМЯТКА О СПОСОБАХ СОВЕРШЕНИЯ ПРАВОНАРУШЕНИЙ В СФЕРЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ И НЕОБХОДИМЫХ МЕРАХ БЕЗОПАСНОСТИ

СТАТИСТИКА СОВЕРШЕНИЯ ПРАВОНАРУШЕНИЙ В СФЕРЕ ИКТ С НАЧАЛА ПРОВЕДЕНИЯ СПЕЦИАЛЬНОЙ ВОЕННОЙ ОПЕРАЦИИ

в 10 раз

сократилось число телефонных атак мошенников

212 - 67,28%

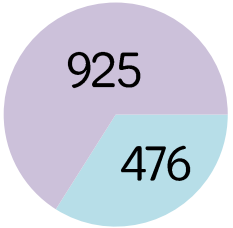
преступлений совершено путем звонка потерпевшему от имени сотрудника банка

- динамика по сравнению с 2021 г.

1401 - 17,25%

зарегистрированных имущественных преступлений совершены с использованием ИКТ

Данные ГУ МВД России по Челябинской области, 2022 г.



Мошенничество - 3,24%

Хищение средств с банковского счета - 35,41%

+ 900%

реклама с предложением инвестировать в акции Газпрома

+ 4,07%

число звонков от имени полиции о родственнике, попавшем в беду

+ 566,67%

недостоверная информация о совместной поездке на blablacar

НОВЫЕ СООБЩЕНИЯ МОШЕННИКОВ

1

Перевод денег на безопасный счет потому что:
- банк под санкциями
- отключение банков от системы SWIFT

2

Требования немедленно погасить несуществующий кредит от лица одного из крупнейших российских банков

3

Предложения от лжеброкеров по инвестиционным инструментам или имитация рекламы известных российских инвестиционных и финансовых компаний

4

Тезисы о поддержке украинской армии и призывы к протестной активности среди матерей российских солдатов-срочников

5

Ссылки на зараженные сайты российских компаний с сообщениями о якобы полученных начислениях или выигрыше ценных призов

РАССЫЛКА ПИСЕМ И СООБЩЕНИЙ ОТ ИМЕНИ ОРГАНОВ ВЛАСТИ

КАК ОРГАНИЗОВАНО

Приходит сообщение на эл. почту или в соцсетях от лица российских органов власти:

- предупреждение о незаконности использования запрещенных в России
- веб-сайтов, соцсетей, мессенджеров и VPN-сервисов;
- информация о новых соцвыплатах

Приложение к письму: файл RTF

КАК НА САМОМ ДЕЛЕ

- При открытии документа скачивается вредоносный файл
- Активируется скрипт, с помощью которого мошенник получает удаленный доступ к данным вашего устройства
- Мошенник переводит денежные средства с банковских счетов или копирует персональную информацию

КАК ПОСТУПИТЬ

Не торопитесь!
Не открывайте файлы и не переходите по ссылкам, особенно в случае призыва к срочным действиям

Проверьте файлы активирусом
Все сомнительные файлы проверяйте антивирусными программами или на сервисах (пример opentip.kaspersky.com)

Проверьте адрес сайта
Проверьте написание адресов сайтов, прежде чем переходить по ним и вводить на них данные

МОШЕННИЧЕСТВО С БАНКОВСКИМИ КАРТАМИ

КАК ОРГАНИЗОВАНО

Приходит сообщение или звонок о том, что банковская карта заблокирована либо идет попытка перевода денежных средств

Предлагается совместно с банком уточнить детали, чтобы предотвратить блокировку карты или перевод средств.

Мошенники по телефону просят сообщить номер карты/счета, cvc-код с оборота карты, сумму средств на счете, код из смс

КАК НА САМОМ ДЕЛЕ

После сообщения номера карты или счета, cvc-кода или кода из смс злоумышленники снимут деньги с вашего счета

КАК ПОСТУПИТЬ

Не торопитесь!
Не сообщайте реквизиты вашей карты (никто не вправе требовать данные карты)

Проверьте информацию
Чтобы проверить информацию о блокировании или списании с карты, позвоните в службу поддержки банка

Номер телефона службы поддержки банка указан на обороте карты, мобильном приложении или официальном сайте

ОПЛАТА В ПОДДЕЛЬНОМ ИНТЕРНЕТ-МАГАЗИНЕ

КАК ОРГАНИЗОВАНО

- Злоумышленники создают фальшивый интернет-магазин
- Пользователей привлекают на сайт низкие цены, дефицитные товары и услуги
- Человек оформляет заказ

Спойлер: но не получит желаемый товар или услугу

КАК НА САМОМ ДЕЛЕ

- Поддельные сайты копируют дизайн оригинального сайта и агрессивно продвигаются на онлайн-сервисах
- Человек вводит данные банковской карты
- Информация попадает злоумышленникам
- Деньги будут украдены

КАК ПОСТУПИТЬ

Совершайте покупки только в проверенных интернет-магазинах

Будьте внимательны при оплате

Проверяйте, чтобы окно ввода данных карты было открыто в защищенном режиме

На защищенный режим указывают замок в адресной строке, https в адресе

ОБМАН ПО ТЕЛЕФОНУ: ТРЕБОВАНИЕ ВЫКУПА

КАК ОРГАНИЗОВАНО

- Поступает звонок с незнакомого номера
- Мошенник представляется знакомым, сообщает, что задержан полицией и обвинён в преступлении
- В разговор вступает якобы сотрудник полиции. Сообщает, для решения вопроса нужна не раз помогал людям. Для решения вопроса нужна определенная сумма денег

КАК НА САМОМ ДЕЛЕ

- В организации обмана участвуют несколько преступников.
- Ваш номер набран наугад, фраза мошенника - заготовлена, его действия – по обстоятельствам
- Если жертва поддалась на обман ей называют адрес, куда приехать, или счет для перевода денег. Запугивают до получения денег

КАК ПОСТУПИТЬ

Прервите разговор

Позвоните тому, в ком идет речь
Если телефон отключён - свяжитесь с его коллегами, друзьями, уточните информацию

Незнакомец требует деньги – мошенник

Задайте уточняющие вопросы «знакомому»
Примеры вопросов: Как я выгляжу? Когда мы виделись последний раз?

Уточните у полицейского номер отделения.
После наберите «02», узнайте у дежурного, действительно ли ваш родственник задержан

SMS-ПРОСЬБА О ПОМОЩИ

КАК ОРГАНИЗОВАНО

Абонент получает смс: «У меня проблемы, кинь 900 рублей на этот номер. Мне не звони, перезвоню сам»

Нередко добавляется обращение «мама», «друг» или другие

КАК НА САМОМ ДЕЛЕ

В роли вымышленного друга или родственника выступает мошенник

В зоне особого риска: пожилые или слишком юные владельцы телефонов

КАК ПОСТУПИТЬ

Проинформируйте близких
Пожилым людям, детям и подросткам следует объяснить, что на SMS с незнакомых номеров реагировать нельзя, это могут быть мошенники

ТЕЛЕФОННЫЙ НОМЕР-ГРАБИТЕЛЬ

КАК ОРГАНИЗОВАНО

- Приходит SMS с просьбой перезвонить на указанный номер телефона
- Просьба обоснована разными причинами – помощь другу, изменение тарифов связи, проблемы со связью и др.
- После того, как вы перезваниваете, вас долго держат на линии. Когда это надоедает, вы отключаетесь. Со счёта списываются крупные суммы

КАК НА САМОМ ДЕЛЕ

- Существуют сервисы с платным звонком. Например, для развлечений. Плата взимается дополнительно за сам звонок
- Мошенники регистрируют сервис и распространяют номер без предупреждения о снятии платы за звонок

КАК ПОСТУПИТЬ

Не звоните по незнакомым номерам
Это единственный способ обезопасить себя от телефонных мошенников

ТЕЛЕФОННЫЕ ВИРУСЫ

КАК ОРГАНИЗОВАНО

- В смс или в соцсетях приходит сообщение: «Вам направлена информация. Для получения пройдите по ссылке...»
- При переходе по адресу на телефон скачивается вирус и происходит списание денежных средств с вашего счета
- С вашего номера рассылаются подобные сообщения по адресной книге

КАК ПОСТУПИТЬ

Не переходите по незнакомым ссылкам
Не переходите по ссылкам даже, если номер знакомый (его могли взломать)

Пользуйтесь официальными источниками
Для скачивания приложений используйте только официальные источники

Проверьте настройки приложений в телефоне
Не давайте лишних разрешений приложениям в настройках телефона

ВЫИГРЫШ В ЛОТЕРЕЕ

КАК ОРГАНИЗОВАНО

- На телефон приходит сообщение или звонок от якобы ведущего популярной радиостанции
- Ведущий поздравляет вас с крупным выигрышем в лотерее (телефон, ноутбук , автомобиль и др.)
- Чтобы получить приз просят представиться, назвать год рождения, данные карты и просят сообщить код из смс для подтверждения выигрыша

КАК НА САМОМ ДЕЛЕ

Полученной информации о ФИО, банковской карте достаточно, чтобы мошенники списали деньги с вашего счета.

Код из смс-сообщения нужен для подтверждения списания денежных средств

КАК ПОСТУПИТЬ

Прекратите общение

Игнорируйте сообщения с такой тематикой

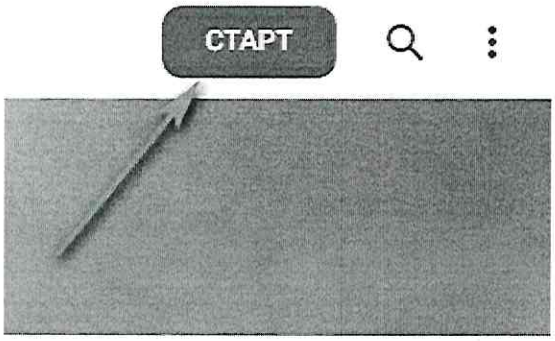
Приложение

Инструкция о работе в телеграмм-боте

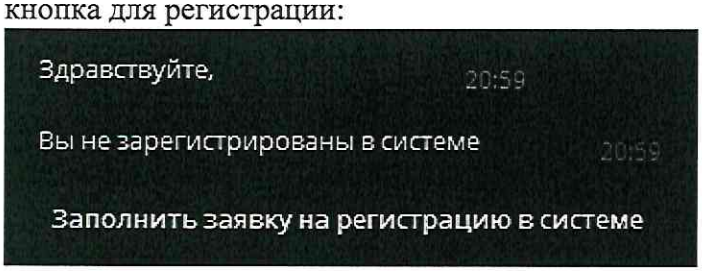
Для начала работы начните общение с ботом https://t.me/mininform74_bot

РЕГИСТРАЦИЯ

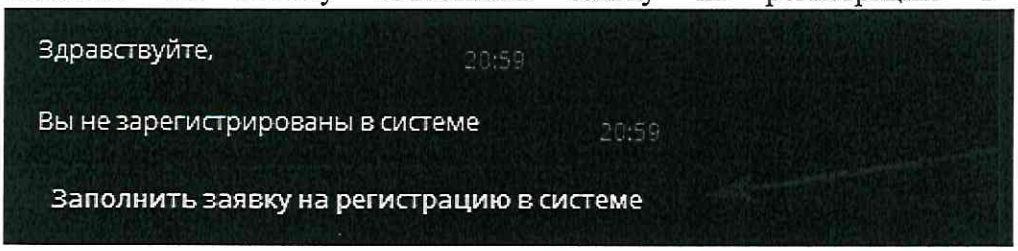
1. Нажмите кнопку СТАРТ (START), расположенную либо внизу чата, либо в правом верхнем углу рядом с кнопкой поиска по чату:



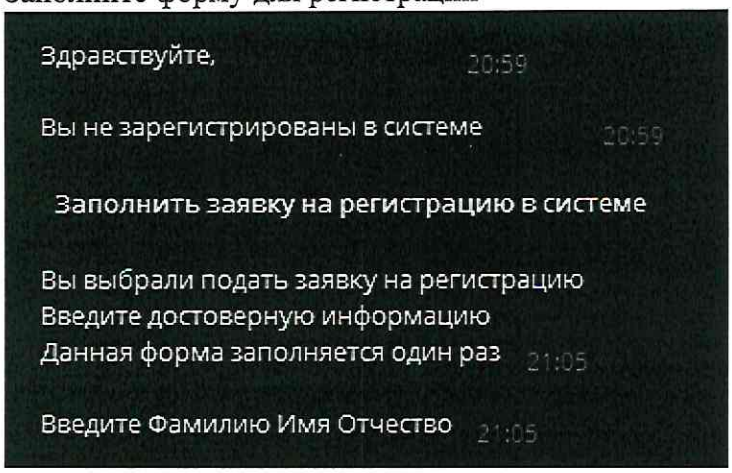
2. Бот поприветствует вас, сообщит о том, что вы не зарегистрированы в Системе (в качестве слова «Система» подразумевается сам Бот). Далее вам станет доступна кнопка для регистрации:



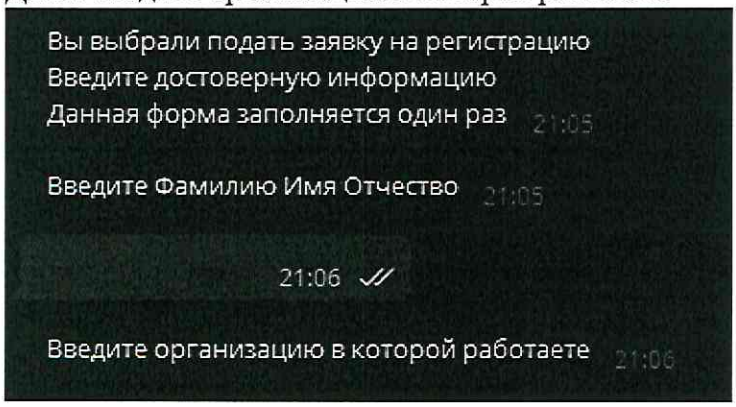
3. Нажмите на кнопку «Заполнить заявку на регистрацию в системе»



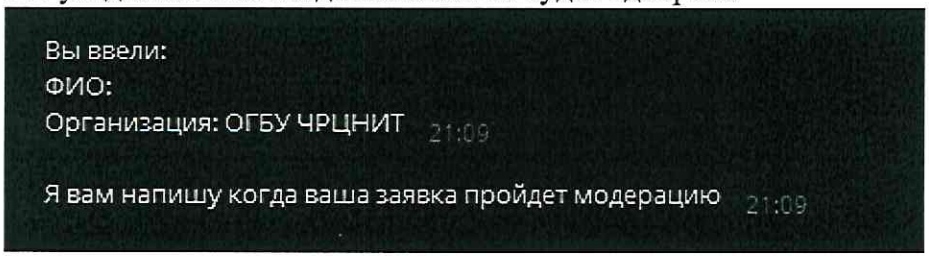
4. Заполните форму для регистрации



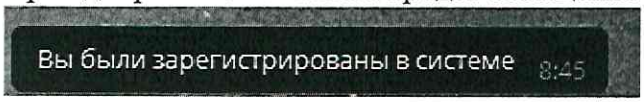
5. Далее введите организацию в которой работаете



6. После ввода информации Бот выведет сообщение с введённой вами информации и бот уведомить Вас когда ваша заявка будет одобрена

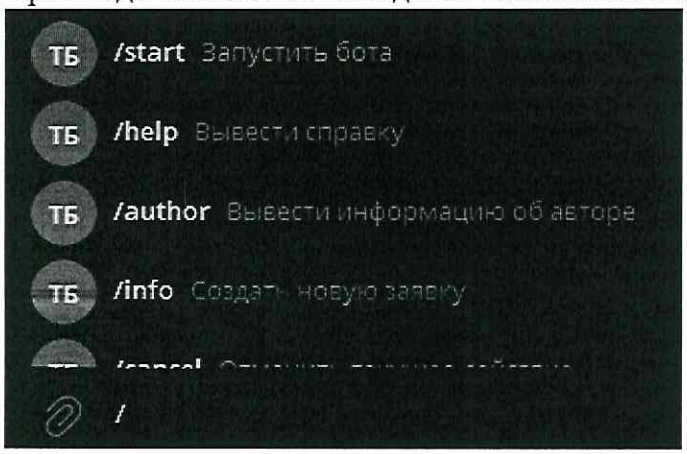


7. При одобрении заявки Вам придет сообщение от бота:

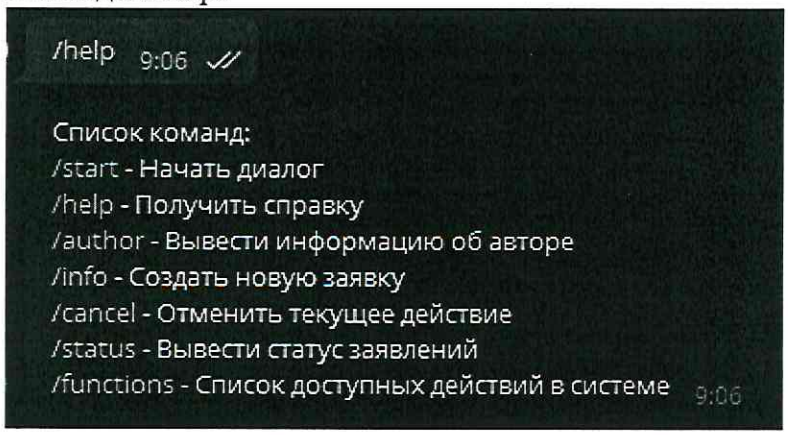


КОМАНДЫ

1. При вводе символа «/» выводится список всех команд бота:



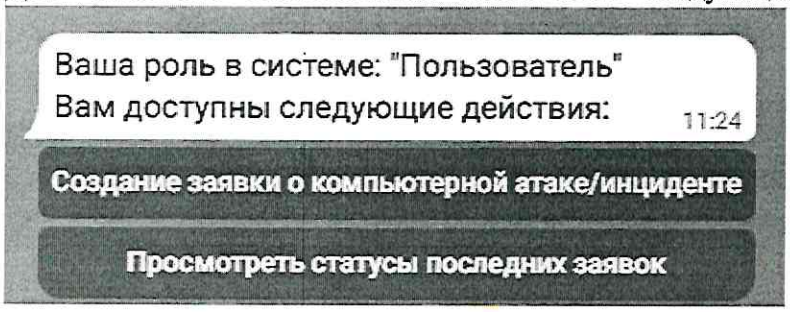
2. Команда «/help»



3. Команда «/author»

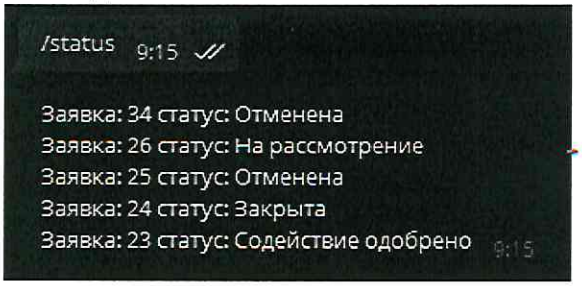
4. Команда «/functions»

Для обычного пользователя высветится следующий перечень действий:

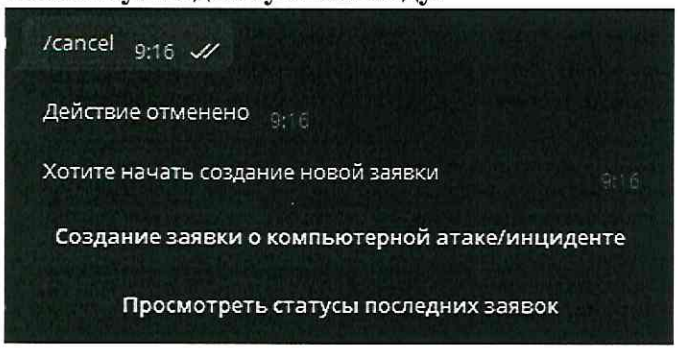


Для ответственного пользователя дополнительно есть действие «регистрация новых пользователей»

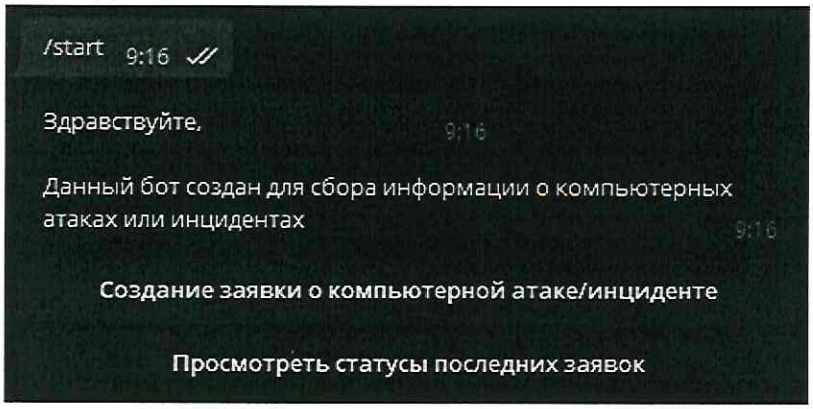
5. Команда «/status»



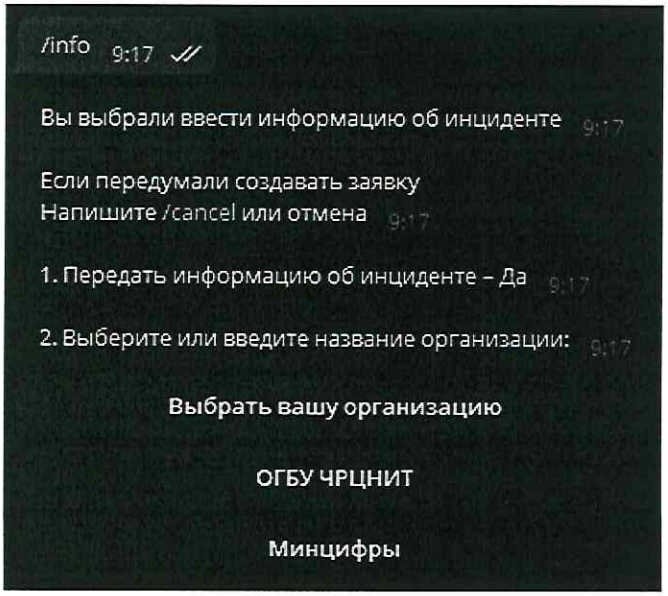
6. Команда «/cancel». **В случае если бот не отвечает на Ваши действия, используйте данную команду.**



7. Команда «/start»

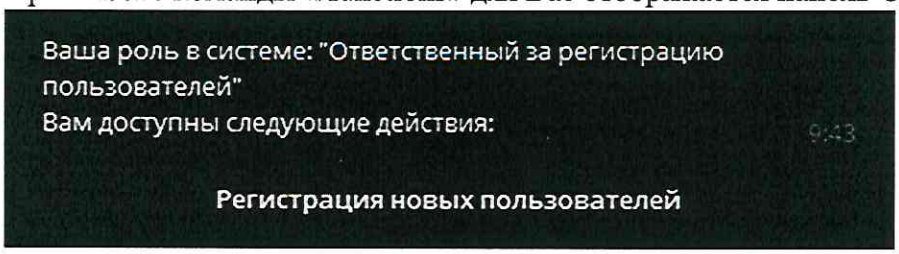


8. Команда «/info»

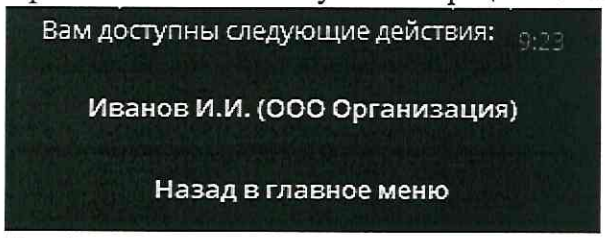


ОТВЕТСТВЕННЫЙ ЗА РЕГИСТРАЦИЮ ПОЛЬЗОВАТЕЛЕЙ

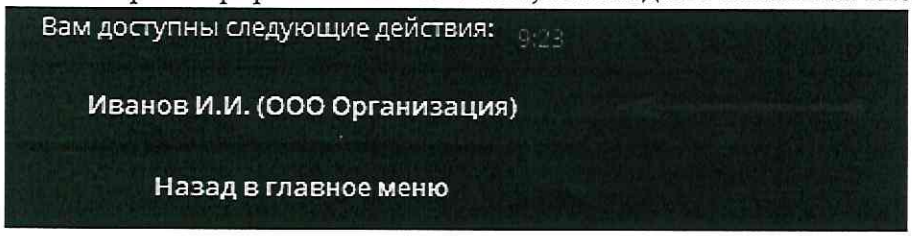
1. При вызове команды «/functions» для Вас отображается панель Ответственного:



2. При нажатии на кнопку «Регистрация новых пользователей»:

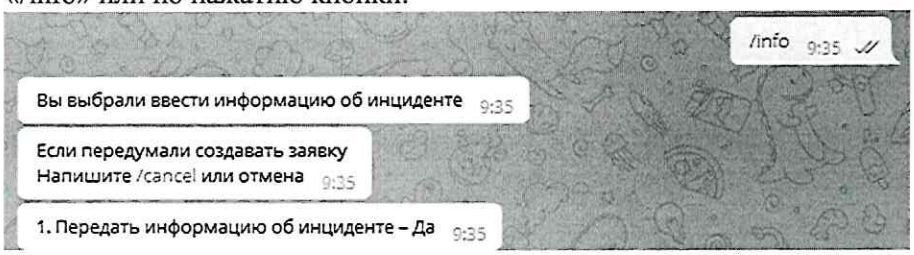


Чтобы зарегистрировать пользователя, необходимо нажать на кнопку с его именем:



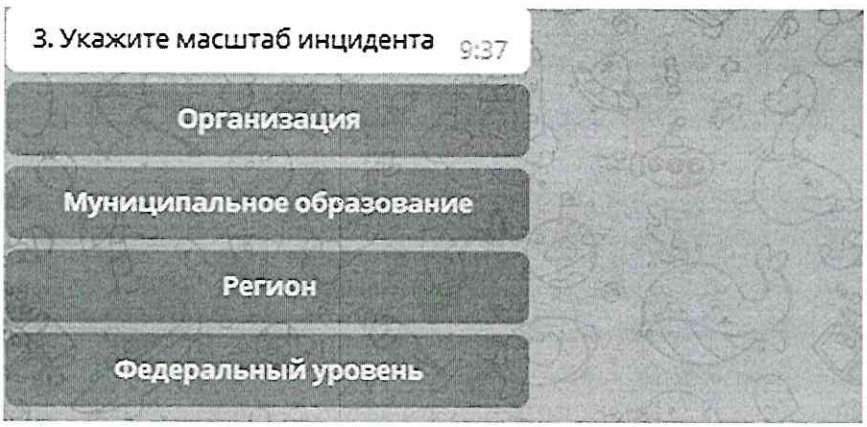
ВСЕ ЗАРЕГИСТРИРОВАННЫЕ ПОЛЬЗОВАТЕЛИ

1. Для того что бы начать заполнять заявку об инциденте, необходимо вызвать команду «/info» или по нажатию кнопки:

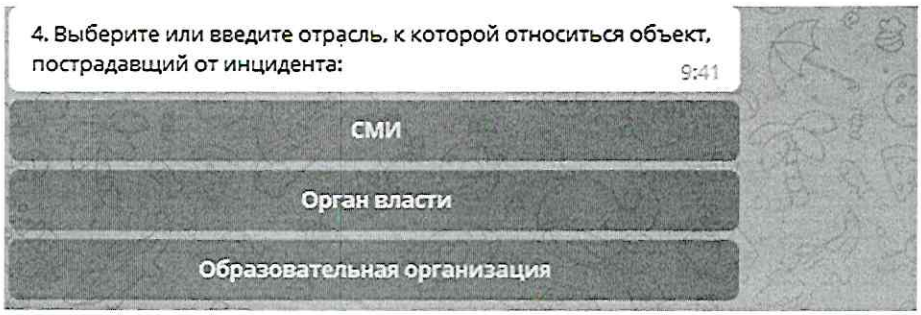


2. Нужно выбрать или ввести название организации. Выделено три группы организаций: органы исполнительной власти, органы местного самоуправления и другие. В «Другие» попадают все подведомственные организаций и иные, зарегистрированные в системе. При нажатии на кнопку «Выбрать вашу организацию» в поле организация автоматически проставляется та организация, которая была указана при регистрации Вас в качестве пользователя.

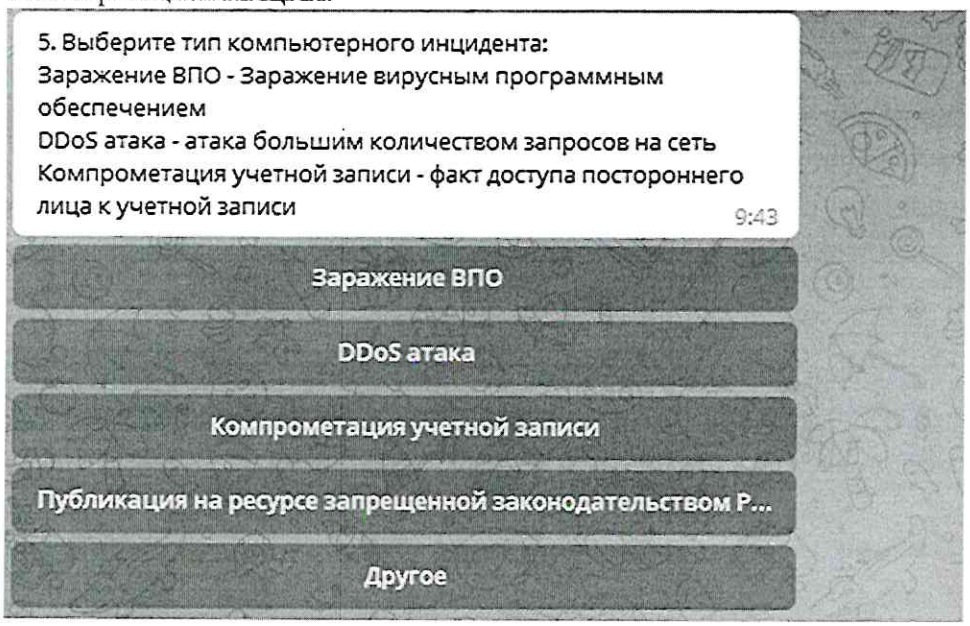
3. Укажите масштаб инцидента.
Организация – инцидент затрагивает только инфраструктуру организации
Муниципальное образование – инцидент затрагивает несколько организаций в пределах одного муниципального образования.
Регион - инцидент затрагивает несколько организаций в пределах Челябинской области.
Федеральный уровень - инцидент затрагивает несколько организаций расположенных в разных субъектах РФ



4. Выберите или введите отрасль, к которой относиться объект, пострадавший от инцидента. На данный момент возможно выбрать одну из трех отраслей или ввести свой вариант. Со временем список будет пополняться.

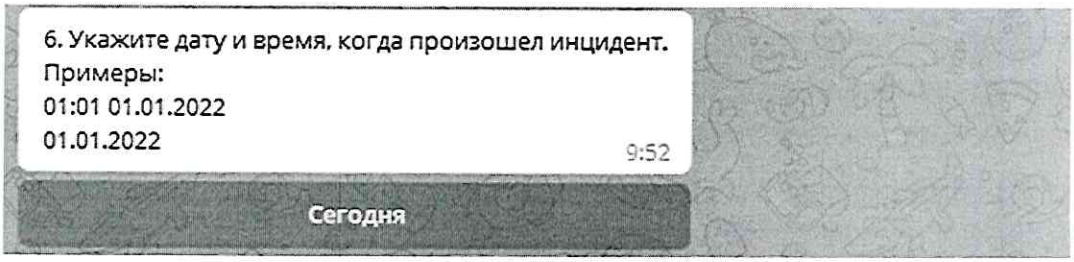


5. Выберите тип компьютерной атаки или компьютерного инцидента. Сейчас классификация содержит четыре пункта, самые часто встречающиеся в последние два месяца. В следующем обновлении будут добавлены остальные типы атак и инцидентов в соответствии с классификацией НКЦКИ.



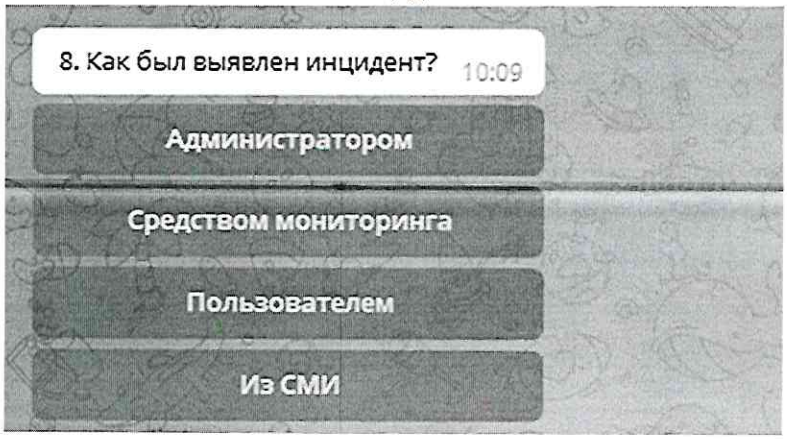
Далее идут дополнительные вопросы, которые зависят от выбранного пункта при классификации. Необходимо указать количество зараженных хостов, на какой ресурс произошла DDoS-атака, сколько скомпрометировано учетных записей или на каком ресурсе опубликована запрещенная информации.

6. Укажите дату и время, когда произошел инцидент. При нажатии на кнопку «сегодня» автоматически проставляется дата сегодняшнего дня.

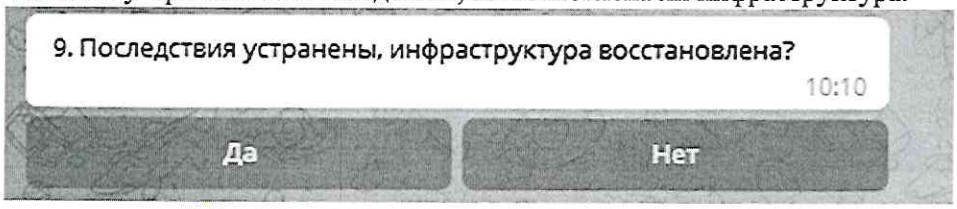


7. Кратко опишите компьютерный инцидент или компьютерную атаку, последствия и возможный ущерб.
   В следующем обновлении здесь появится возможность добавлять файл, чтобы прикрепить скриншоты, логи или что-либо другое.

8. Укажите кем был выявлен инцидент.



9. Укажите устранены ли последствия, восстановлена ли инфраструктура.



10. Если в предыдущем вопросе был ответ «нет», то необходимо указать, необходимо ли Вам содействие со стороны оперативного штаба по обеспечению кибербезопасности Челябинской области.

11. Кратко опишите какие меры были приняты.

12. Укажите контакты специалиста, который сможет дать дополнительную информацию. Введите в одном сообщение ФИО и номер телефона.

13. Проверьте введенную информацию и подтвердите отправку.