Департамент информационных технологий
города Москвы

Социальная инженерия: как не попасть на удочку мошенников в мессенджерах?

[Играя на чувствах и слабостях жертвы, мошенники заставляют ее действовать в своих интересах]

Оглавление

1. Основные методы социальной инженерии в мессенджерах

В связи с возросшей популярностью использования в повседневной жизни мессенджеров (WhatsApp, Telegram и Viber) развивается и киберпреступность.

Самый распространенный метод, которым пользуются мошенники – это целевой фишинг от лица руководителя или коллеги.

При целевом фишинге злоумышленник тщательно собирает информацию о собеседнике, используя в беседе обращение по имени и отчеству, чтобы повысить степень доверия к себе.

Принцип проведения фишинговой атаки:

2. Примеры мошеннических схем с использованием социальной инженерии в мессенджерах

1. Схема мошенничества в мессенджерах в отношении сотрудников и работников органов исполнительной власти города Москвы и подведомственных им организациям (далее – работник).

Работник получает сообщение от лица руководителя организации (поддельный аккаунт) с поручением провести диалог с внешней службой безопасности.

Для повышения доверия к сообщению преступник использует реальные фамилию, имя, отчество руководителя и его официальное фото на аватарке.

Используется давление на человека через авторитет его непосредственного руководителя и репутацию ФСБ России. Часто дополнительно разыгрываются роли с участием фиктивных Центробанка и МВД России.

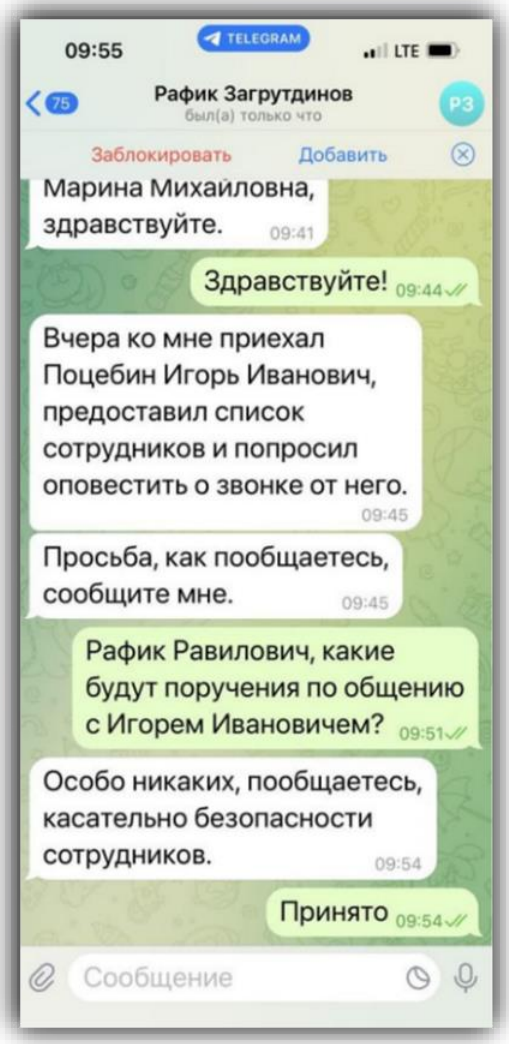
Продолжение переписки может привести к финансовым потерям, хищению личной и конфиденциальной информации и подрыву репутации Вашей, Ваших коллег или организации в целом.

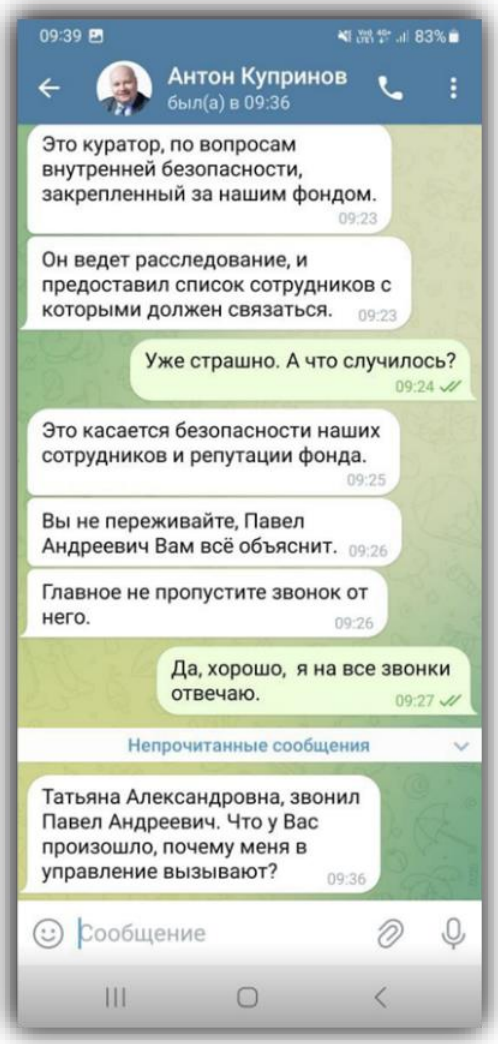
Примеры реальных атак злоумышленников:

- на левом рисунке сообщение от якобы председателя Комитета ветеринарии города Москвы;
- на правом рисунке сообщение от якобы директора ГКУ «Московский центр развития социальных технологий».

Еще примеры:

- на левом рисунке сообщение от якобы руководителя Департамента строительства города Москвы;
- на правом рисунке сообщение от якобы исполнительного директора Фонда содействия кредитованию малого бизнеса Москвы.

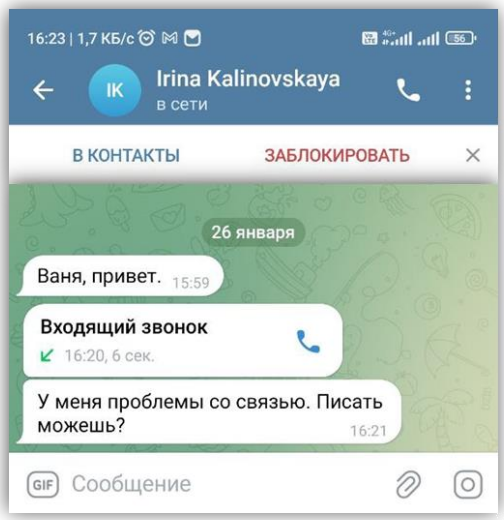




Мошенники, используя «маску» руководителя, стараются расположить к себе собеседника (общаются на «ты», спрашивают о жизни и т.д.)

Примеры:

- на первом рисунке сообщение от якобы руководителя Департамента культурного наследия города Москвы (Емельянова А.А.)
- на втором и третьем рисунках сообщения от якобы начальника Государственной инспекции города Москвы по качеству сельскохозяйственной продукции, сырья и продовольствия (Калиновской И.Б.)

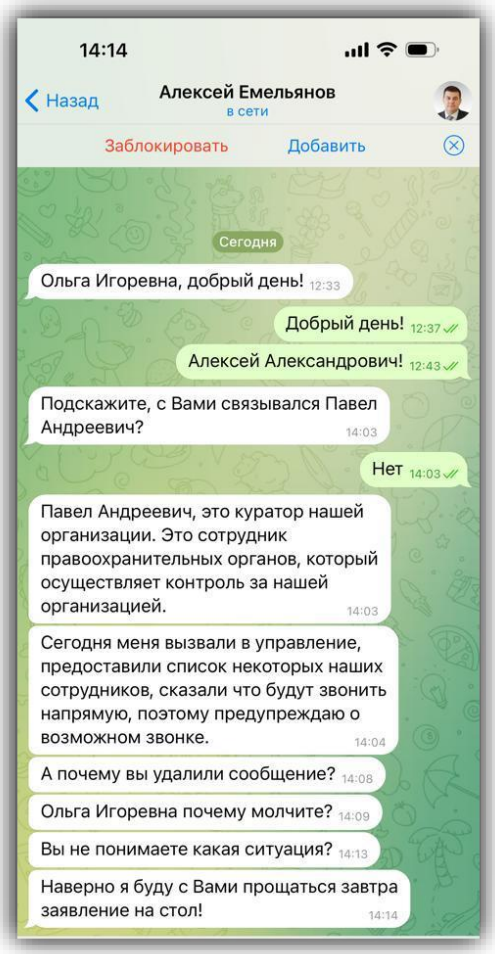


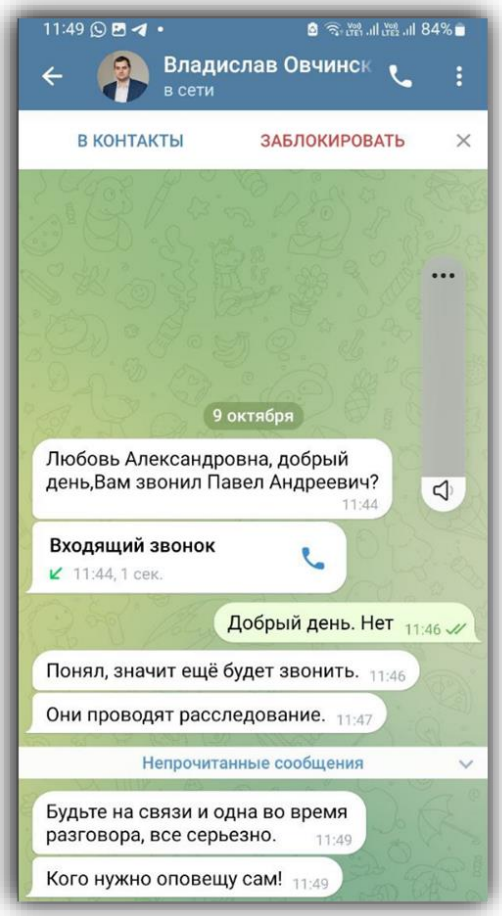
Основная цель первого этапа общения – подготовить работника к общению с лже-сотрудником ФСБ России.

Причем уже на первом этапе доходит и до угроз.

Примеры:

- на левом рисунке сообщение от якобы руководителя Департамента культурного наследия города Москвы;
- на правом рисунке сообщение от якобы руководителя Департамента инвестиционной и промышленной политики города Москвы.





Пример:

- на следующем рисунке сообщение от якобы заместителя Мэра Москвы в Правительстве Москвы по вопросам региональной безопасности и информационной политики Горбенко А.Н.

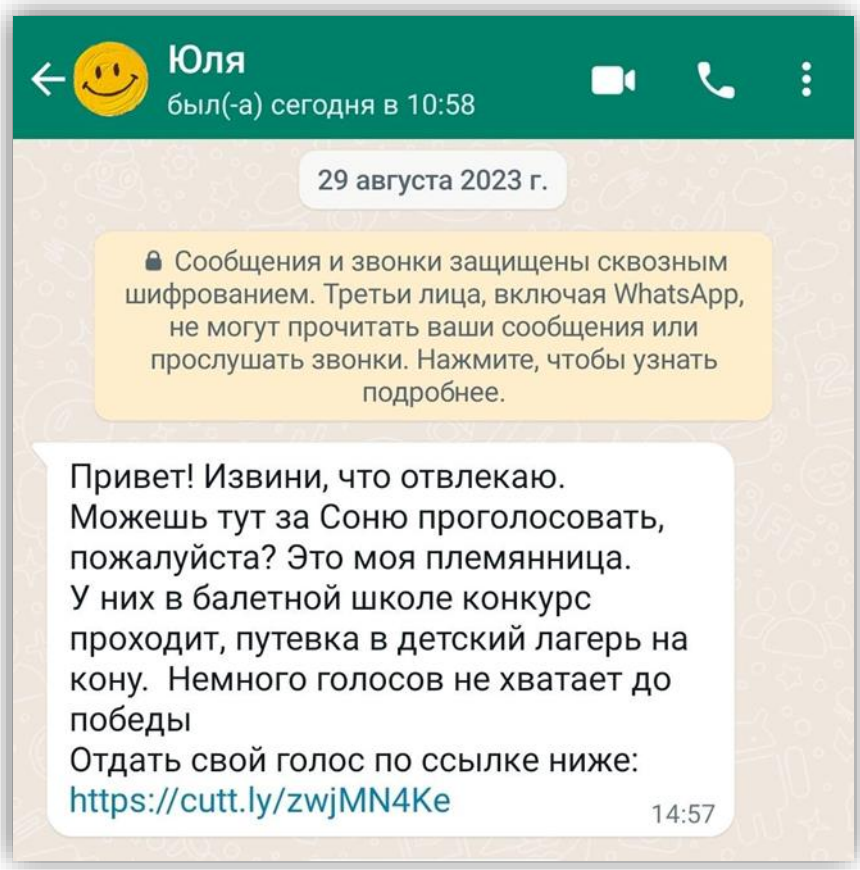
2. Еще одна распространенная схема мошенничества, когда работник получает сообщение от своего коллеги, аккаунт которого взломали.

Злоумышленник делает рассылку фишингового сообщения с вредоносной ссылкой или вложением всем контактам из телефонной книги взломанного аккаунта. При этом, его владелец этого даже не замечает и не видит этой переписки.

В сообщении описывается проблема и просьба о помощи (в данном случае идет давление через жалость или желание помочь), любопытный факт или новость с предложением перейти по ссылке или скачать файл (в данном случае преступник надеется на любопытство собеседника или пытается вызвать страх и т.д.).

Переход по ссылке или открытие вредоносного файла ведет к заражению вашего смартфона и получению мошенником контроля над ним.

Затем схема мошенничества повторяется, теперь уже вашим контактам рассылается фишинговое письмо.


Юля
был(-а) сегодня в 10:58
29 августа 2023 г.
Сообщения и звонки защищены сквозным шифрованием. Третьи лица, включая WhatsApp, не могут прочитать ваши сообщения или прослушать звонки. Нажмите, чтобы узнать подробнее.
Привет! Извини, что отвлекаю.
Можешь тут за Соню проголосовать, пожалуйста? Это моя племянница.
У них в балетной школе конкурс проходит, путевка в детский лагерь на кону. Немного голосов не хватает до победы
Отдать свой голос по ссылке ниже:
https://cutt.ly/zwjMN4Ke
14:57

3. Мошенники действуют под «маской» Telegram с целью кражи аккаунтов.

Жертвы мошенников получают сообщения якобы от Команды Телеграм, в которых предлагается перейти по ссылкам.

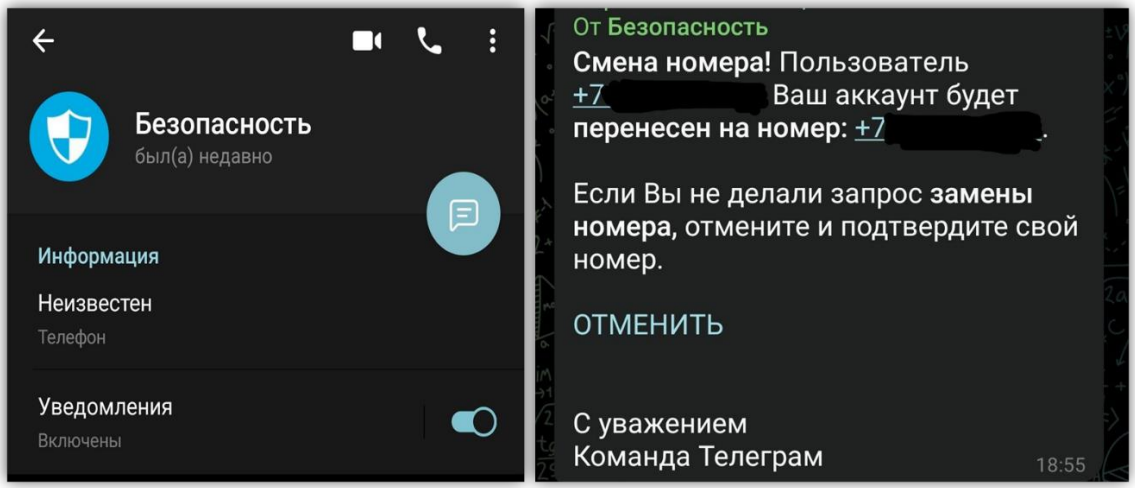
Сами ссылки спрятаны под текст: «Отменить», «Нажмите на сообщение» (под таким текстом скрываются подобные фишинговые ссылки: hxxps://telegramn[.]ru/MTgzNzU= или hxxps://telegramn[.]ru/MTg0MTI).

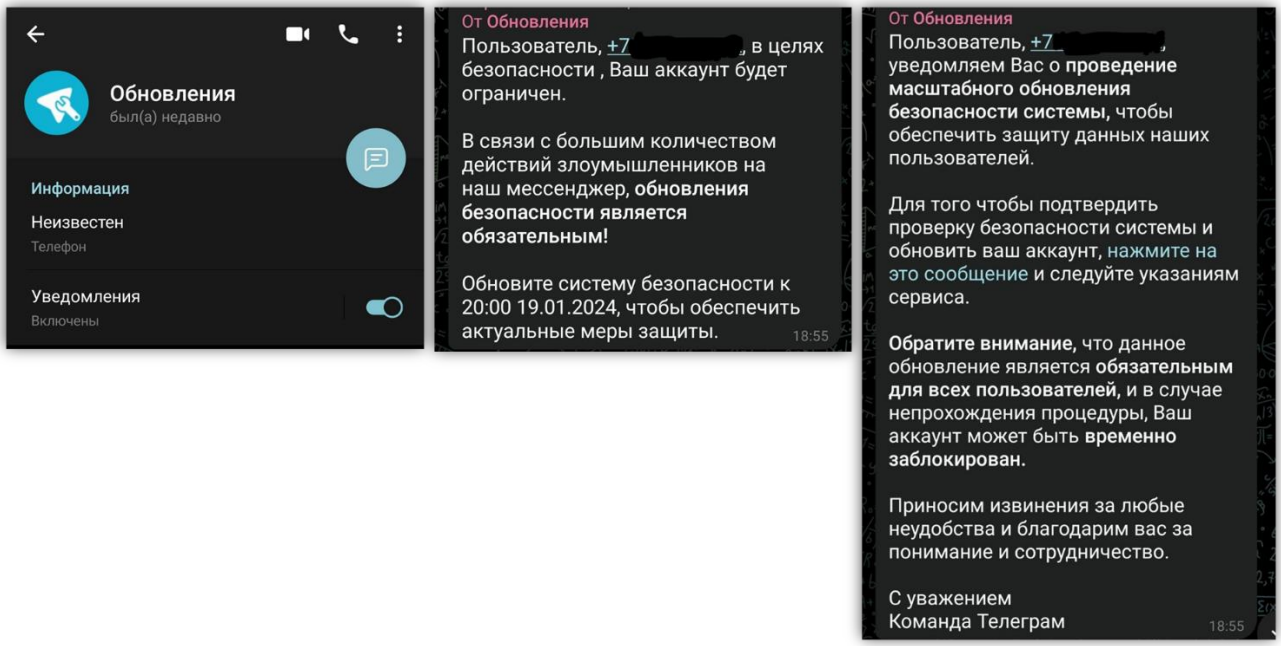
В сообщении побуждают:

– обновить систему безопасности;
– отменить привязку другого номера к аккаунту;
– обновить аккаунт и т.д.

Во всех таких сообщениях мошенники скрыто манипулируют человеком, побуждая к необдуманным действиям.

На рисунках ниже приведены примеры подобных сообщений в Telegram.





4. Используя современные технологии, мошенники генерируют фейковые **ГОЛОСОВЫЕ СООБЩЕНИЯ**, которые отправляют через мессенджеры

Будьте бдительны если:

- сообщение выходит за рамки привычного обсуждения – например, связано с денежным переводом, запросом пароля, необходимостью взаимодействия с правоохранительными органами и т.п.;
- вы не ждали личного сообщения от руководителя;
- в сообщении присутствует давление через свой авторитет;
- в сообщении присутствует момент срочности.

5. Как не попасться на удочку мошенников и что делать в случае получения фишингового сообщения в мессенджере?

ВАЖНО:

1	**Не вступайте в переписку, если:** • **вы не ждали данное сообщение;** • **если собеседник манипулирует своим авторитетом;** • **использует ваши слабости *(страх, любопытство, желание помочь, срочность и т.д.)*, чтобы достичь своих целей.**
2	**Никому не сообщайте ваши пароли, коды подтверждения операций, приходящие на устройство.**
3	**Прежде чем переходить по ссылке или открывать файл:** • **решите, а есть ли в этом необходимость;** • **проанализируйте входящее сообщение на скрытую манипуляцию вашими эмоциями или желаниями.**
4	**Настройте двухфакторную аутентификацию аккаунта в мессенджере**

Для заметок

ВНИМАНИЕ!

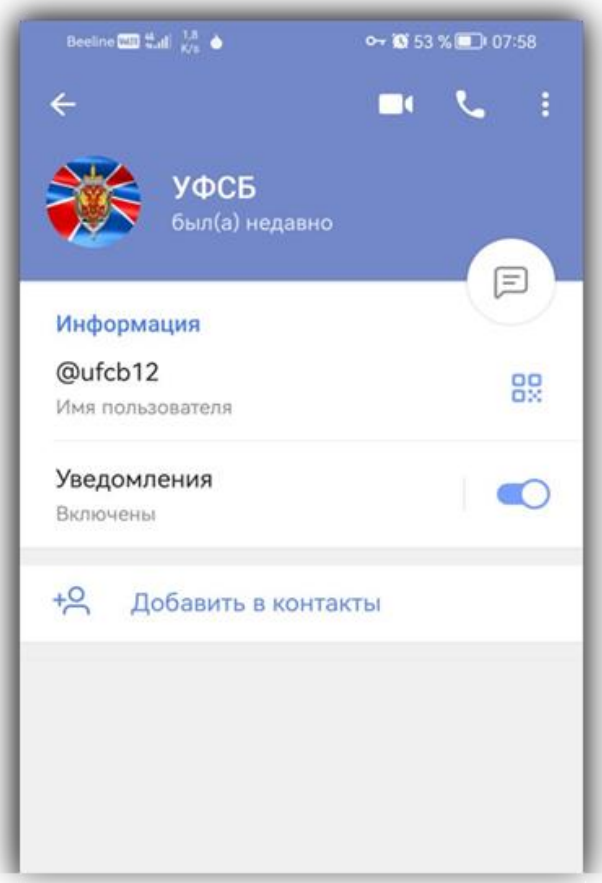
Злоумышленники пытаются максимально расположить к себе собеседника, для этого:

- **подменяют номер телефона на официальный** *(например, при входящем звонке отображается телефон ФСБ России и т.д.)*;
- **направляют фото якобы своего служебного удостоверения;**
- **используют официальную символику органов государственных власти** *(например, при входящем звонке отображается геральдический знак – эмблема ФСБ России и т.д.)*.
- **направляют от имени органа государственной власти якобы официальные обращения, заверенные подписью и печатью руководителя, в которых сообщают:**
  - о голосовом согласии в сотрудничестве с органами государственной власти;
  - о том, что вы являетесь подозреваемым (обвиняемым);
  - об установлении в отношении вас факта мошеннических действий;
  - о необходимости выполнения процедуры обновления единого лицевого счета;
  - о необходимости получения кредита и перевода денег на «безопасный счет» или передачи их курьеру и т.д.

ВАЖНО ПОМНИТЬ!

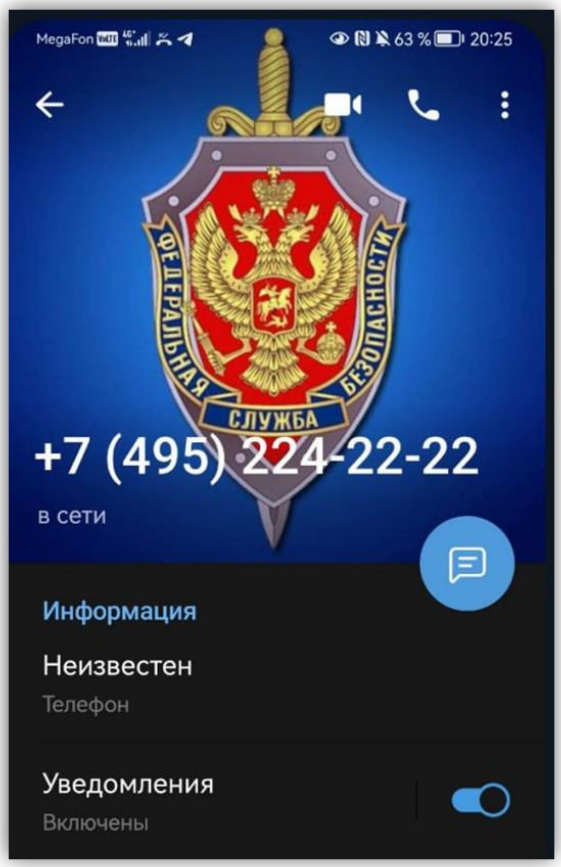
- ✓ **Уведомление гражданина органы государственной власти осуществляют лично ИСКЛЮЧИТЕЛЬНО В ПИСЬМЕННОМ ВИДЕ И ВРУЧАЮТ ЛИЧНО.**
- ✓ **Сотрудники органов государственной власти НИКОГДА НЕ ПРИСЫЛАЮТ гражданам копии своих служебных удостоверений.**
- ✓ **Органы государственной власти НЕ ИСПОЛЬЗУЮТ личные сбережения или кредитные средства граждан для оказания помощи оперативным подразделениям в предупреждении и раскрытии преступлений.**
- ✓ **Официальные телефоны органов государственной власти используются ИСКЛЮЧИТЕЛЬНО ДЛЯ ПРИЕМА ИНФОРМАЦИИ от граждан и организаций.**

Примеры:


Beeline
53 %
07:58
УФСБ
был(а) недавно
Информация
@ufcb12
Имя пользователя
Уведомления
Включены
Добавить в контакты


Вы
Сегодня, 16:04
СЛУЖЕБНОЕ УДОСТОВЕРЕНИЕ
ХАСАНОВ
РУСЛАН
СЕРГЕЕВИЧ
4. 01.01.1990 РОССИЯ
5а. 27.01.2019 4b. 27.04.2029 4c. ПРОДЛЕН
6. ТН. 674101 ЦЕН. БАНК РФ
7. РУКОВОДИТЕЛЬ ОТДЕЛА
СЛУЖБЫ БЕЗОПАСНОСТИ
ЦЕНТРАЛЬНОГО БАНКА
РОССИЙСКОЙ ФЕДЕРАЦИИ


МВД РОССИИ
НВК № 958841
Действительно
до 20 марта 2024
Личный № А-14491
ГЛАВНОЕ УПРАВЛЕНИЕ МВД РОССИИ
ПО МОСКОВСКОЙ ОБЛАСТИ
СЛУЖЕБНОЕ УДОСТОВЕРЕНИЕ
№ 958841
Старший Лейтенант внутренней службы
Савин
Андрей Владимирович
должность Старший Следователь
ГУ МВД РФ
Начальник (заместитель)
20 марта 2021


MegaFon
63 %
20:25
ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
+7 (495) 224-22-22
в сети
Информация
Неизвестен
Телефон
Уведомления
Включены


Пересланное сообщение
От
Здравствуйте,нет 18:00
Пересланное сообщение
От
О проверке которую проводит Морозов Е.В слышали ? 18:00
Пересланное сообщение
От
Нет 18:00
Пересланное сообщение
От
Вы были в прошлом году на лекции внешней безопасности? 18:00


? 10:10
Здравствуйте, я сейчас на смене. 10:11
Понял.
Тогда много времени не отниму. Вас с утра о проверке Савельева Маргарита предупредила? 10:13
Нет, меня не предупреждали. 10:14
Значит не успела, с другими коллегами сейчас. 10:15
Тогда кратко, чтоб без сюрпризов: Савельева Маргарита Владимировна - куратор внешней безопасности, она ответственна за проверку и проведение лекций. 10:16
Мы для нее составили списки сотрудников, она будет выборочно с некоторыми связываться.
Не пропустите от нее звонок. 10:17

ФСБ РОССИИ
Управление
Федеральной службы безопасности
Российской Федерации
по Московской области
(УФСБ России по Московской области)
ул.Большая Лубянка,д.2,г.Москва,107031

Согласие на сотрудничество

_____ дав голосовое согласие на сотрудничество с Федеральной Службой Безопасности Российской Федерации обязуется не разглашать сведений, составляющих государственную и служебные тайны, точно выполнять относящиеся к ней (нем) требования приказов, положений, инструкций по обеспечению режима секретности проводимых работ.

Об ответственности по закону разглашений сведений, составляющих государственную тайну, утрату документов, содержащие такие сведения, а также об ответственности за нарушения установленного режима секретности проводимых работ предупрежден (а).

Инструктаж провел _____

ст. следователь следственного отдела УФСБ

«26» сентября 2023 г. _____

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
УПРАВЛЕНИЕ ПО МОСКВЕ И МОСКОВСКОЙ ОБЛАСТИ
Ул.Большая Лубянка, 20 стр.2, г.Москва, 101000

У/Д 429513 /23

ПОСТАНОВЛЕНИЕ

о приобщении отдельного эпизода преступления
к материалам уголовного дела № 429513 /23

г.Москва [redacted]

Старший следователь по особо-важным делам Управления ФСБ Российской Федерации по г.Москва, майор Калашников В.Н., рассмотрев сообщение о совершении преступления, поступившее от заместителя начальника ОПИО РОО "Москва" Центрального Банка Российской Федерации.

УСТАНОВИЛ:

[redacted] в отношении гр. [redacted] обнаружен факт мошенничества, который заключается в попытках хищения денежных средств путем различных манипуляций с основным счетом со стороны злоумышленников.

В процессе телефонного разговора с [redacted], который отрицает свою причастность к подобного рода операциям, т.е. никаких изъятий, переводов денежных средств, в т.ч. переводов в адрес третьих лиц не проводил, в связи с чем [redacted], в установленном законом порядке, был проинформирован об ответственности за нарушения ст. 310 УК РФ и предоставил под запись диалога голосовое соглашение[1] на сотрудничество с органами ФСБ России и Центральным банков Российской Федерации, таким образом обязуясь сотрудничать с вышеупомянутыми структурами в рамках предотвращения действий по основному счету.

В связи с вышеупомянутым деяния совершенные по отношению к гр. [redacted], являются неправомерными и попадают под ч.3 ст. 159 УК РФ. Учитывая характерные признаки совершенного преступления в отношении [redacted] следует сделать вывод, что эти деяния попадают под уголовное дело № 429513 /23 от 26.09.2023 г., которое находится в сопровождении УФСБ РФ по г.Москве.

Принимая во внимание, что имеются достаточные данные, указывающие на признаки преступления, предусмотренного ч.3 ст.159 УК РФ, руководствуясь ст. 140, 145, ч.2 ст.156 УПК РФ.

ПОСТАНОВИЛ:

1. Приобщить эпизод преступления в отношении гр. [redacted] к уголовному делу № 429513 /23, и приступить к его расследованию.
2. Копию настоящего постановления направить первому заместителю Генерального прокурора Российской Федерации.

Старший следователь по ОВД
УФСБ по г. Москве Калашников В.Н.

Копия настоящего постановления направлена первому заместителю Генерального прокурора Российской Федерации.
Старший следователь по ОВД
УФСБ по г. Москве Калашников В.Н.

[redacted]

[1] К документу прилагается запись голосового согласия, далее именуется "запись № 3 от 26.09.2023 г."

Банк России ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: d107312a3a9a80b8543c329a8bbf9ab6
Владелец: А. С. Набережный
Действителен с 07.10.2022 по 06.03.2024

Банк России
Центральный банк Российской Федерации

Исх. № 53517742 г. Москва

Документ № 53517742

Центральный Банк Российской Федерации настоящим письмом уведомляет, что Вы, , стали жертвой мошеннических действий. Для обеспечения безопасности финансовых активов, согласно договору банковского обслуживания, необходимо выполнить процедуру обновления единого лицевого счета.
Процедура обновления единого лицевого счета разделена на несколько этапов:

I этап:
- Переоформление кредитной заявки.
Если в системе банков отображается активная заявка на кредит - её необходимо отклонить, путем подачи новой заявки. Финансы для проведения операции по отклонению кредитной заявки предоставляются из резервного фонда ЦБ РФ (согласно ФЗ "О противодействии отмывания доходов, полученных преступным путем, и финансированию терроризма", в целях совершенствования контроля). Данная заявка не будет отображаться в кредитной истории и не влияет на кредитный рейтинг в дальнейшем.

II этап:
- Погашение кредитнорй задолженности.
Выполняется методом внесения финансовых активов, предоставленных вам из резервных фондов ЦБ РФ. Внесение выполняется зашифрованным методом (с помощью АТМ устройства, рассчетно-кассового центра страхового банка партнера), предоставленным отделом финансового мониторинга.

III этап:
После выполнения всех регламентных работ, представителем ЦБ РФ будет назначено время и адрес отделения банка в которое клиенту необходимо явиться для: актуализации паспортных данных, перевыпуска пластиковых носителей, подписания и получения документации.

Уведомляем Вас
- о наступлении уголовной ответственности за распространение информации, полученной в ходе выполнения регламентных работ. (Согласно ст. 183 УК РФ (соблюдение политики конфиденциальности, коммерческой, налоговой и банковской тайны)).
- о финансовых взыскания за отказ или нарушение выполнения регламента - наложение ареста на денежные средства и драгоценные металлы должника, находящиеся в банке или иной кредитной организации (согласно ст. 81 УК РФ) и взыскании денежных средств, выделенных Банком для выполнения регламентных действий (выпуск исполнительного листа, согласно ФЗ №229-ФЗ "Об исполнительном производстве").

Срок обновления реквизитов с момента выполненных работ, составляет 2 часа.
Специалист Банка России: Беляев Роман Алексеевич.
Финансово-ответственное лицо: Ожидает закрытие кредитного договора.

Зам. Начальника ОДИО РОО "Москва"
филиала №3 ЦБ РФ
М.П.

А. С. Набережный

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

16.01.2024 г. 029

Москва

О проведении проверки прикрепленным оператором (советником по безопасности Макаровым Дмитрием Александровичем, назначенным приказом №24-0810/22) к АО «МАРКА» (7703422320).

Причиной проведения проверки может быть одна, или несколько из следующих причин:

- у контрольного (надзорного) органа есть сведения о причинении вреда охраняемым законом ценностям или об угрозе этого;
- контрольный (надзорный) орган выявил соответствие объекта контроля параметрам, - утвержденным индикаторами риска нарушения обязательных требований или отклонение объекта от параметров;
- истек срок исполнения решения контрольного (надзорного) органа об устранении - нарушения обязательных требований (в установленных случаях);
- наступило событие, указанное в программе проверок;
- поступило поручение Президента РФ или Правительства РФ о проведении указанных мероприятий в отношении конкретных контролируемых лиц;

ФЗ от 31 июля 2020 г. №248 "О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации".

В границах от 09 января 2024г. по 22 января 2024г. ответственному оператору необходимо подготовить акт о наличии нарушения по одному (или нескольких), пунктов и, при наличии таковых, - акт об оценке степени вреда в соответствии со ч. 3 ст. 7 Закона №248-ФЗ.

Акт (акты) передать для урегулирования инспектору Федеральной службой по Финансовому Мониторингу в соответствии с п. 5 ст. 18.1 Закона от 27.07.2006 №152-ФЗ.

На установление причин и ликвидацию последствий дано 10 рабочих дней, - приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 14.11.2022 №187-ФЗ.

Директор: А. Бортников

6. Настройка двухфакторной аутентификации аккаунта

Для Telegram

Перейдите в Настройки, выберите раздел Конфиденциальность и там кликните на пункт Облачный пароль

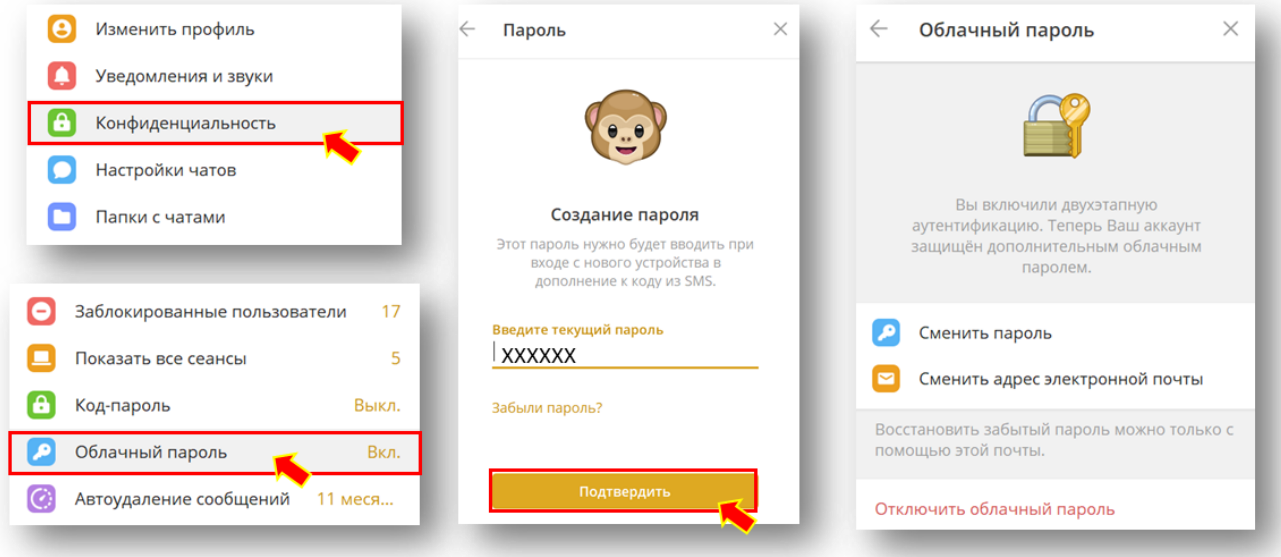
Сгенерируйте безопасный пароль и нажмите Подтвердить

Двухэтапная аутентификация включена

1

2

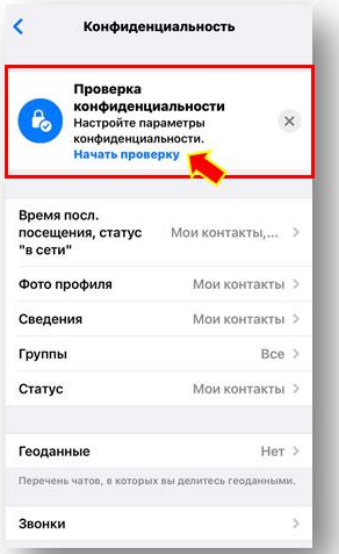
3



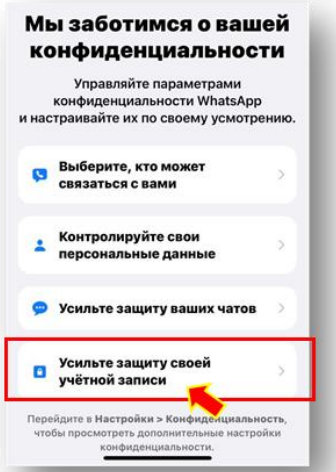
Для заметок

Для WhatsApp

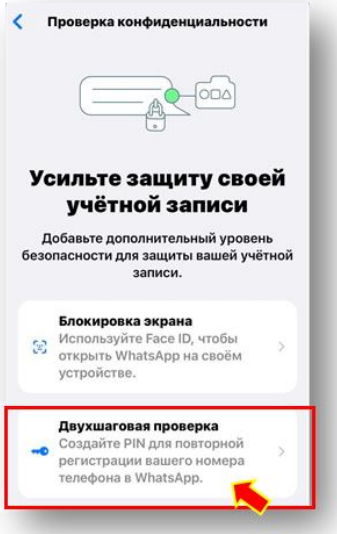
1. Перейдите в Настройки, выберите раздел Конфиденциальность и там кликните на пункт Начать проверку



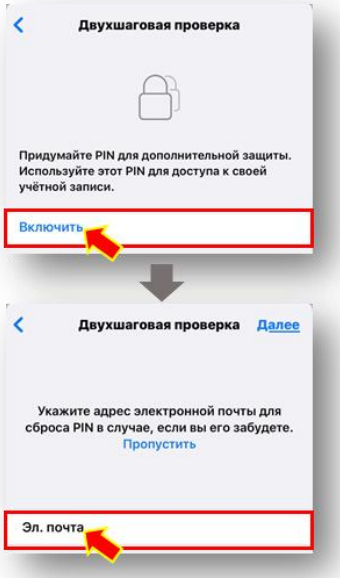
2. Перейдите в раздел Усильте защиту своей учётной записи



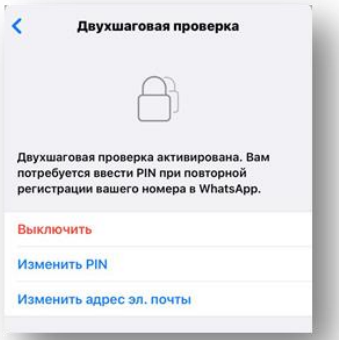
3. Выберите раздел Двухшаговая проверка



4. Введите PIN-код и укажите адрес электронной почты



5. Двушаговая проверка активирована



7. Задания для самопроверки

1. От коллеги пришло письмо с просьбой посмотреть документ в мессенджере и направить замечания при их наличии.

Какие действия Вы предпримете?

- ☐ Задам себе вопрос: Я ждал это сообщение? Я знаю о чем этот документ?
- ☐ Задам себе вопрос: Есть ли в данном сообщении скрытая манипуляция моими чувствами?
- ☐ Сразу скачаю документ и открою его, это же просьба
- ☐ Если я не в курсе данной темы сообщения, то свяжусь с коллегой и уточню вопрос

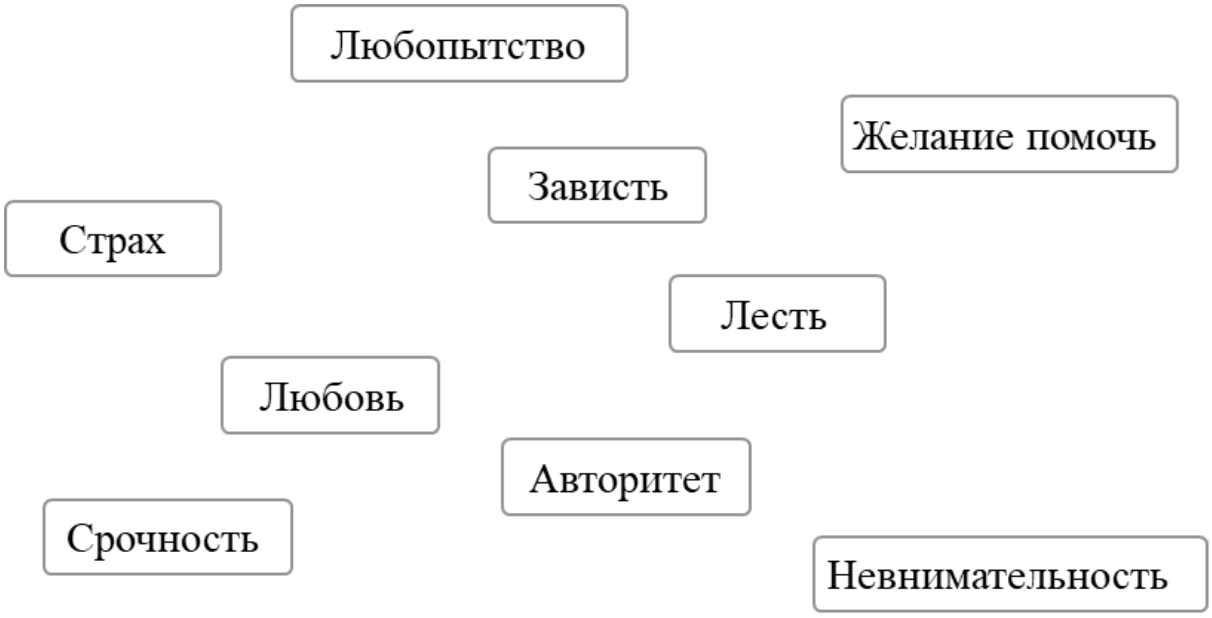
2. Неожиданно Вы получили письмо от руководителя организации (указаны реальные фамилия, имя и отчество, а также представлена его фотография), при этом ранее вы не общались и его контактных данных у Вас нет. В сообщении он явно манипулирует своим авторитетом, дает поручения, не связанные с Вашими должностными обязанностями, настаивает на общении с сотрудниками органов государственной власти?

Как Вы поступите?

- ☐ Выполню поручение руководителя организации
- ☐ Прекращу переписку, внесу данный номер в черный список и не буду вести беседу с лжесотрудником госучреждения
- ☐ Сообщу о данном инциденте своему непосредственному руководителю

3. Чем пользуется мошенник, чтобы добиться своих целей (располагая к себе собеседника, побуждая сообщить личные данные или перейти по ссылке)?

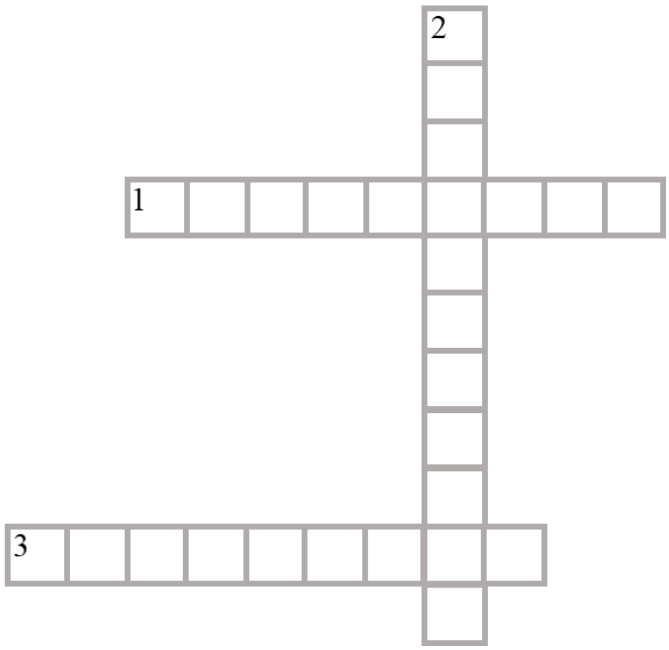
Отметьте, на Ваш взгляд, правильные ответы.



4. Какие могут быть последствия поддержания беседы с мошенником или перехода по ссылке из фишингового сообщения?

- [ ] Никаких последствий, если ссылку прислал коллега, он же не мошенник, я ему доверяю
- [ ] Финансовые потери
- [ ] Устройство будет заражено и может перейти под контроль мошенника
- [ ] Репутационные проблемы

5. Разгадайте кроссворд:



Вопрос 1. Чем манипулирует мошенник (какой психологический прием применяет), если работник получает сообщение от лица руководителя организации?

Вопрос 2. Форма психологического воздействия, применяемая в фишинговом сообщении.

Вопрос 3. Что происходит с устройством при переходе по вредоносной ссылке или открытии вредоносного файла?

6. Вы получили в мессенджере официальное письмо от Управления Федеральной службы безопасности Российской Федерации по городу Москве и Московской области о подозрении Вас к совершению незаконных действий, в частности, переводу денежных средств на корреспондентский счет, открытый в недружественном государстве.

Как Вы поступите?

- ☐ Продолжу общение в мессенджере с представителем УФСБ России по г. Москве и Московской области
- ☐ Не буду включаться в переписку, а также в переговоры по телефону
- ☐ Удалю сообщение и занесу номер в черный список
- ☐ Оповещу о данном инциденте своего руководителя

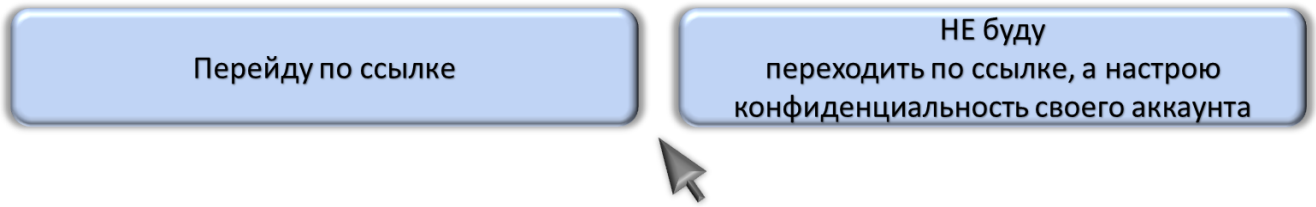
7. Вам пришло сообщение от Команды Telegram:

«Пользователь, +7XXX-XXX-XX-XX Вы инициировали изменение телефонного номера на +7XXX-XXX-XX-XX.

Если Вы этого не делали или считаете, что посторонние лица получили доступ к Вашему аккаунту немедленно перейдите по ссылке Отменить изменение телефона, в противном случае номер будет изменен.

С уважением, Команда Telegram»

Как вы поступите?



Предложения и замечания отправляйте на адрес электронной почты: DITsecurity@mos.ru.