

БЫТЬ ХАКЕРОМ -



УПРАВЛЕНИЕ
ПО ПРОТИВОДЕЙСТВИЮ
КИБЕРПРЕСТУПНОСТИ
УВД ВИТЕБСКОГО
ОБЛИСПОЛКОМА

БОЛЬШЕ ИНФОРМАЦИИ
В TELEGRAM-КАНАЛЕ
ЦИФРОВАЯ ГРАМОТНОСТЬ
T.ME/CIFGRAM



НЕ РАЗВЛЕЧЕНИЕ,
▶ А ПРЕСТУПЛЕНИЕ

УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ
ЗА КИБЕРПРЕСТУПЛЕНИЯ НАСТУПАЕТ:

с 14 лет

статья 212 УК

Хищение имущества путем
модификации компьютерной
информации

наказывается вплоть до
лишения свободы на срок
до 12 лет

статья 340 УК

Заведомо ложное
сообщение об опасности

наказывается вплоть до
лишения свободы на срок
до 7 лет

с 16 лет

статья 222 УК

Незаконный оборот средств
платежа и (или) инструментов

наказывается вплоть до
лишения свободы на срок
до 10 лет

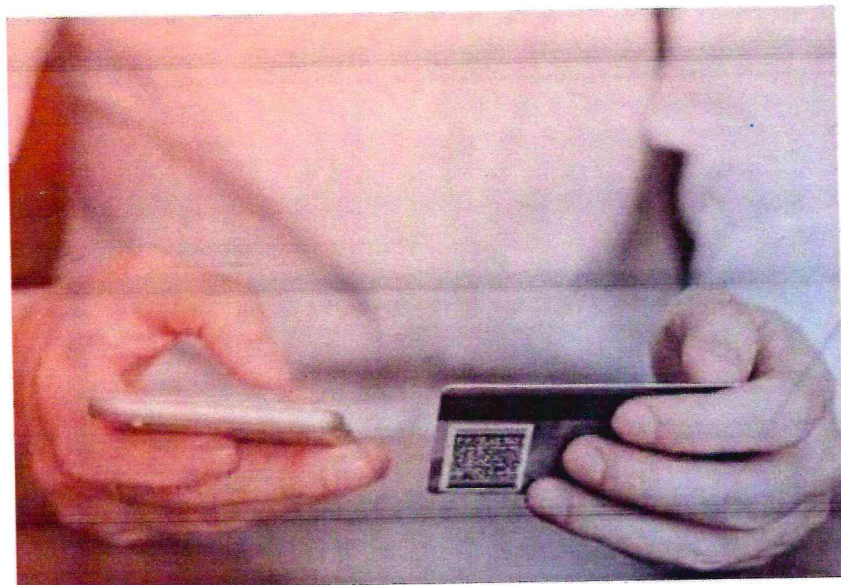
статья 349 УК

Несанкционированный
доступ к компьютерной
информации

наказывается вплоть до
лишения свободы на срок
до 7 лет

**ВЫ ДОЛЖНЫ
ЗНАТЬ!**

СТАТЬЯ 222 УГОЛОВНОГО КОДЕКСА РЕСПУБЛИКИ БЕЛАРУСЬ, ИЛИ КАК НЕ СТАТЬ ПРЕСТУПНИКОМ



Все чаще в социальных сетях и мессенджерах пользователям стали приходить сообщения с предложениями без особых усилий за день заработать до 100 долларов. Что для этого нужно? Всего ни чего, оформить на себя банковскую карту в банке, на который укажет мнимый работодатель, и передать сообщением в сети Интернет полученные реквизиты карты потенциальному работодателю.

Как правило, все общение проходит в сети Интернет без личного контакта. Истории, для чего нужна работодателю банковская карта чужого человека, различны. В основном это необходимость перевода денег на счета в Беларуси, а сам он не может, так как находится в другой стране.

Человек, согласившийся на такие условия сделки, становится так называемым «ДРОПОМ» – подставным лицом в серых схемах кибермошенников. Дроп – это тот человек, который соглашается, чтобы его банковская карта стала «транзитной» для украденных мошенниками денег. Дроп переводит незаконно полученные денежные средства между разными счетами. Такая цепочка переводов нужна для того, чтобы запутать следы киберпреступников и усложнить работу милиции.

Кто такой ДРОП?

Дропы бывают «разводные» и «неразводные». Отличие их только в том, что неразводные осознают всю тяжесть совершаемых ими деяний и умышленно занимаются этим. В большинстве своем это студенты, школьники, малоимущие, которые нуждаются в финансах. Разводные «дропы» не знают о том, что идут на преступление. Они думают, что действительно работают, получают зарплату и т.д.

Ответственность за такие действия наступает по статье 222 УК Республики Беларусь (незаконный оборот средств платежа и (или) инструментов) с 16 летнего возраста.

1. Изготовление в целях сбыта либо сбыт поддельных банковских платежных карточек, иных платежных инструментов и средств платежа, а равно совершенное из корыстных побуждений незаконное распространение реквизитов банковских платежных карточек либо аутентификационных данных, посредством которых возможно получение доступа к счетам либо электронным кошелькам, – наказываются штрафом, или ограничением свободы на срок от двух до пяти лет, или лишением свободы на срок от двух до шести лет.

2. Те же действия, совершенные повторно, либо организованной группой, либо в особо крупном размере, – наказываются ограничением свободы на срок от трех до пяти лет или лишением свободы на срок от трех до десяти лет со штрафом или без штрафа.

СТАТЬЯ 212
Уголовного Кодекса
Республики Беларусь

Хищение путем использования
компьютерной техники

Хищение имущества путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, либо путем введения в компьютерную систему ложной информации наказывается лишением свободы на срок **ДО ТРЕХ ЛЕТ.**



МИЛИЦИЯ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ МВД РБ



Министерство внутренних дел Республики Беларусь

Служим Закону, Народу, Отчизне!



Профилактика

Рекомендации по соблюдению мер информационной безопасности

Рекомендации по соблюдению мер «цифровой гигиены»

Необходимо:

Не рекомендуется:

Защита данных банковской платежной карточки

Хранить в тайне пин-код, сведения с карточки сеансовых кодов

Хранить пин-код вместе с карточкой/на карточке

Прикрывать ладонью клавиатуру при вводе пин-кода

Сообщать кому-либо реквизиты карты или отправлять их фото по сети Интернет

Оформить отдельную карту для онлайн-покупок, выезда за границу, и не хранить на ней большие суммы. Для карты, используемой в Беларуси, рекомендуется ограничить возможность ее использования за пределами нашей страны

Распространять свои персональные данные (информацию личного характера, номер мобильного телефона), логин и пароль доступа к системе «Интернет-банкинг»

Использовать двухфакторную аутентификацию, установить лимиты на максимальные суммы операций, подключить смс-оповещение о проведении операций по карте

Сообщать данные, полученные в виде SMS-сообщений: сеансовые пароли, код авторизации, пароль «3-D Secure» и т.д.

Скрыть CVV номер на карте (трехзначный номер на оборотной стороне), предварительно сохранив его

Пользоваться системой «Интернет-банкинг» на чужих компьютерах или мобильных устройствах

Вводить логин и пароль к системе «Интернет-банкинг» только на официальном сайте или в мобильном приложении банка

В случае утери (кражи) карты, незамедлительно по телефону обратиться в банк для ее блокирования

При обнаружении несанкционированного списания денежных средств с карт-счета, незамедлительно обратиться с заявлением в

ВНИМАНИЕ!

БЕЗОПАСНОЕ ИСПОЛЬЗОВАНИЕ СОЦСЕТЕЙ, МЕССЕНДЖЕРОВ И ЭЛЕКТРОННОЙ ПОЧТЫ!

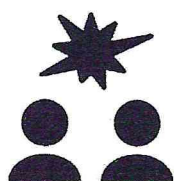
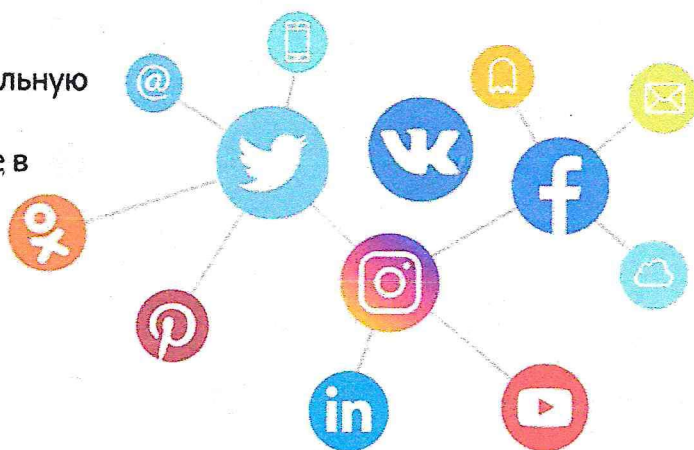


Размещать персональную
и контактную
информацию о себе в
открытом доступе



Использовать
указание геолокации
на фото в постах

НЕЛЬЗЯ



Отвечать на агрессию и
обидные выражения



Реагировать на
письма от
неизвестного
отправителя



Открывать
подозрительное
вложение к письму



Сохрани эту информацию и поделись с другими

Как не стать жертвой киберпреступника.

ЗАЩИТА БАНКОВСКОЙ КАРТОЧКИ

Основные правила информационной безопасности по защите банковской карточки:

-  хранить в тайне пин-код карты
-  прикрывать ладонью клавиатуру при вводе пин-кода
-  оформлять отдельную карту для онлайн-покупок
-  деньги зачислять только в размере предполагаемой покупки
-  использовать услугу 3-D Secure* и лимиты на максимальные суммы онлайн-операций
-  скрыть CVV-код на карте (трехзначный номер на обратной стороне), предварительно сохранив его
-  подключить услугу "SMS-оповещение"



Не рекомендуется

-  хранить пин-код вместе с карточкой/на карточке
-  сообщать CVV-код или отправлять его фото
-  распространять личные данные (например паспортные), логин и пароль доступа к системе "Интернет-банкинг"
-  сообщать данные, полученные в виде SMS-сообщений, сеансовые пароли***, код авторизации, пароли 3-D Secure

* Услуга 3-D Secure - для подтверждения онлайн-платежа держатель карточки вводит особый код (получает его в смс-сообщении на телефон).

** Код CVV - последние 3 цифры номера на обратной стороне платежной карты справа на белой линии, предназначенной для подписи. Код дает возможность распоряжаться средствами, находящимися на счету, физически не контактируя с картой.

*** Сеансовый пароль - предоставляется при входе в интернет-банкинг, действителен лишь в течение одного платежного сеанса.



Источник: МВД Беларуси.

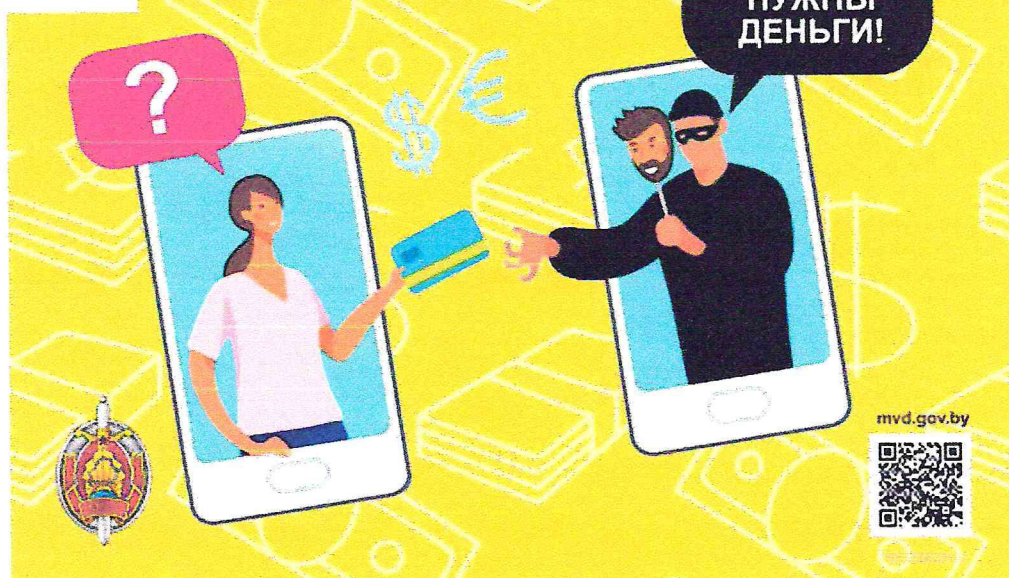
© Инфографика 

ВНИМАНИЕ, МОШЕННИКИ!

Вам звонят посредством мессенджера
или с неизвестного номера...

ВАШИ ДЕЙСТВИЯ:

- не паникуйте и не верьте тому, что вам говорят
- не выполняйте никаких действий по просьбе третьих лиц
- прекратите разговор
- перезвоните родственникам и убедитесь, что ничего не случилось
- сообщите в милицию о звонке



ОСТОРОЖНО!

МОШЕННИКИ В ИНТЕРНЕТЕ



НЕ следуй инструкциям
незнакомцев, позвонившим
с неизвестного номера



НЕ сообщай неизвестным
лицам свои персональные
данные



НЕ совершай никаких
действий на смартфоне по
просьбе посторонних лиц



НЕ переводи деньги
незнакомым людям в
качестве предоплаты



Сохрани эту информацию и поделись с другими

ВНИМАНИЕ!

ЗАЩИТИ СВОЮ БАНКОВСКУЮ КАРТУ

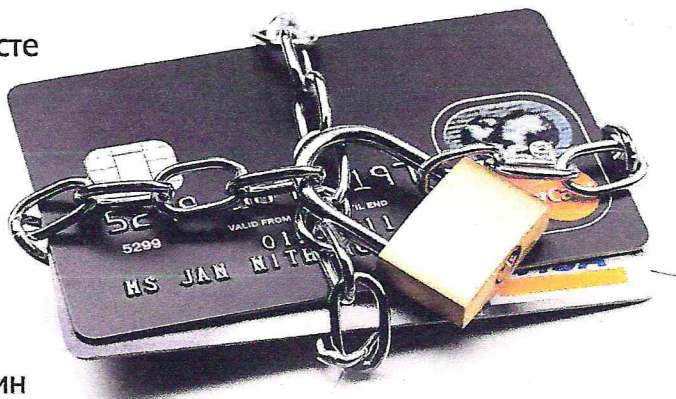


Хранить пинкод вместе
с картой



Распространять
личные данные, логин
и пароль доступа к
системе
«Интернет-банкинг»

НЕЛЬЗЯ



Сообщать CVV-код или
отправлять его фото



Сообщать данные,
полученные в виде
SMS-сообщений,
сеансовые пароли, код
авторизации и т.д.



Сохрани эту информацию и поделись с другими

научись пользоваться интернетом правильно!

СОХРАНИ ИНФОРМАЦИЮ

БЕЗОПАСНЫЙ INTERNET ДЕТЯМ

- 1** не сообщай незнакомцам свой логин и пароль
- 2** не открывай файлы из непроверенных источников
- 3** не заходи на сайты, которые защита компьютера считает подозрительными

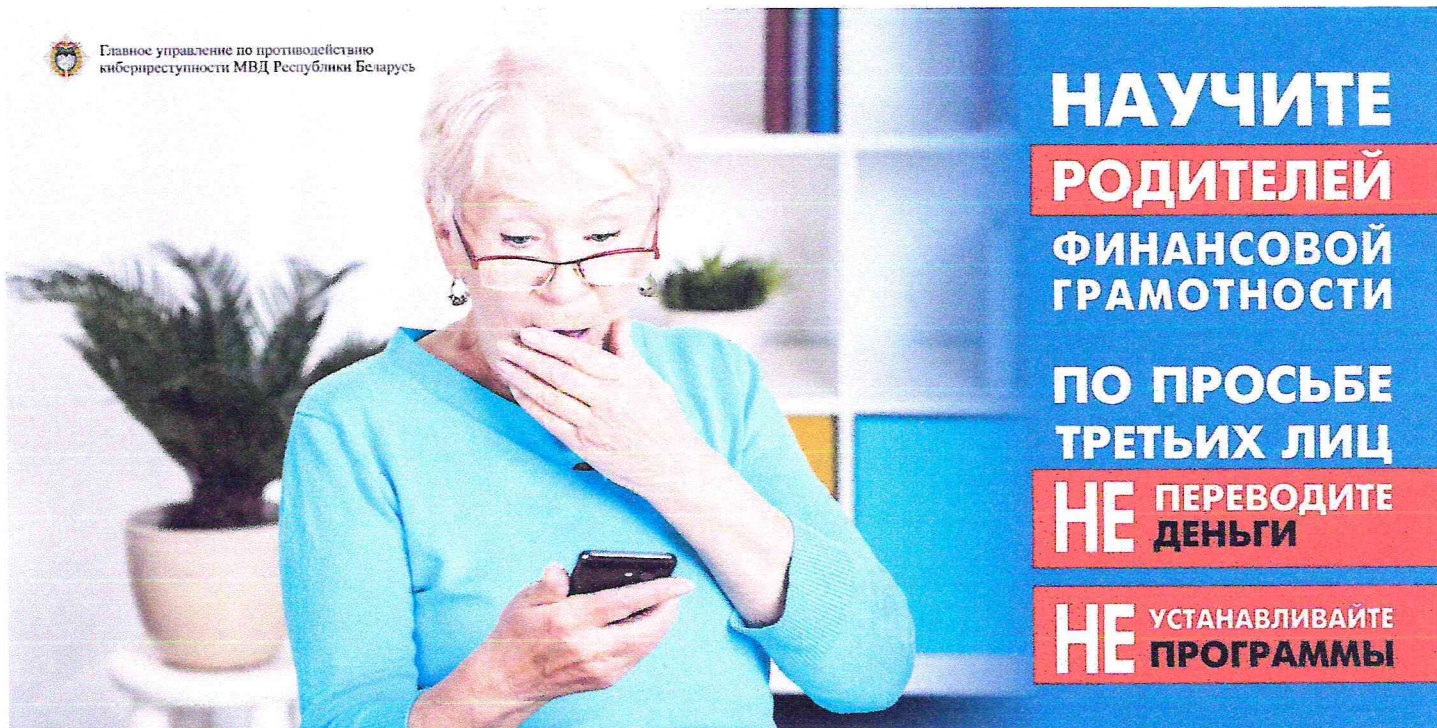
не дай себя обмануть!

 **МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РЕСПУБЛИКИ БЕЛАРУСЬ**

круглосуточный
единый
номер **102**



Главное управление по противодействию киберугрозам МВД Республики Беларусь



**НАУЧИТЕ
РОДИТЕЛЕЙ
ФИНАНСОВОЙ
ГРАМОТНОСТИ**

**ПО ПРОСЬБЕ
ТРЕТЬИХ ЛИЦ**

**НЕ ПЕРЕВОДИТЕ
ДЕНЬГИ**

**НЕ УСТАНОВЛИВАЙТЕ
ПРОГРАММЫ**

ВАМ ЗВОНЯТ ПО ТЕЛЕФОНУ И СООБЩАЮТ

ЧТО ДЕЛАТЬ:

ВАШ БЛИЗКИЙ РОДСТВЕННИК (СЫН, ВНУК, МУЖ) ПОПАЛ В БЕДУ (АВАРИЮ, ОГРАБЛЕН, АРЕСТОВАН), И ЧТОБЫ «ВЫПУТАТЬСЯ» ИЗ ИСТОРИИ, ОН ПРОСИТ ПЕРЕВЕСТИ ДЕНЬГИ ЧЕЛОВЕКУ, КОТОРЫЙ ПОМОЖЕТ

ПОПРОСИТЕ ЗВОНЯЩЕГО ПЕРЕДАТЬ ТРУБКУ ВАШЕМУ РОДСТВЕННИКУ; ПЕРЕЗВОНИТЕ ЕМУ САМИ И УБЕДИТЕСЬ, ЧТО С НИМ ВСЕ В ПОРЯДКЕ

У ВАС ОБНАРУЖЕНО ОПАСНОЕ ЗАБОЛЕВАНИЕ, ПРЕДЛАГАЮТ БЫСТРОЕ ОБСЛЕДОВАНИЕ ИЛИ ЛЕЧЕНИЕ «УНИКАЛЬНЫМ» ЛЕКАРСТВОМ

ПРЕДСТАВИТЕЛИ МЕДУЧРЕЖДЕНИЙ НЕ НАЗЫВАЮТ ДИАГНОЗЫ ПО ТЕЛЕФОНУ, НЕ «ВЕДИТЕСЬ» НА ПОДОБНЫЕ ЗВОНКИ

ВАМ ВЫДЕЛЕНА БЕСПЛАТНАЯ ПУТЕВКА В САНАТОРИЙ, НО НУЖНО НЕМНОГО ДОПЛАТИТЬ, НАПРИМЕР, ЗА ВЫБОР МЕСТА ОТДЫХА

НИКАКИХ ДОПЛАТ ОФИЦИАЛЬНЫЕ СОЦИАЛЬНЫЕ СЛУЖБЫ НИКОГДА НЕ ТРЕБУЮТ

ВЫ ВЫИГРАЛИ В ЛОТЕРЕЕ ИЛИ РОЗЫГРЫШЕ ПРИЗОВ, ДЛЯ ОФОРМЛЕНИЯ ПОТРЕБУЕТСЯ ВНЕСТИ НЕБОЛЬШИЕ ДЕНЬГИ

НЕ ВЕРЬТЕ, ВАМ НАВЕРНЯКА ЗВОНЯТ МОШЕННИКИ

С ВАШЕЙ БАНКОВСКОЙ КАРТЫ БЫЛА ПОПЫТКА ПЕРЕВЕСТИ ДЕНЬГИ, И БАНК ЕЕ ЗАБЛОКИРОВАЛ; ЗВОНИТ ЯКОБЫ ПРЕДСТАВИТЕЛЬ СЛУЖБЫ БЕЗОПАСНОСТИ БАНКА И ПРЕДЛАГАЕТ РАЗБЛОКИРОВАТЬ КАРТУ, НО ДЛЯ ЭТОГО ЕМУ НУЖНО СООБЩИТЬ ЕЕ НОМЕР И КОД, ВАШИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

– СОТРУДНИКИ БАНКОВ НЕ ЗВОНЯТ КЛИЕНТАМ И НИКОГДА НЕ ТРЕБУЮТ НАЗВАТЬ СЕКРЕТНЫЕ СВЕДЕНИЯ О КАРТЕ ИЛИ СЧЕТЕ;
– НИКОГДА НЕ НАЗЫВАЙТЕ И НЕ ВВОДИТЕ ПИН-КОД, ТРЕХЗНАЧНЫЙ КОД НА ОБРАТНОЙ СТОРОНЕ КАРТЫ ИЛИ ОДНОРАЗОВЫЙ ПАРОЛЬ ИЗ СМС;
– НЕ НАБИРАЙТЕ НИКАКИХ КОМБИНАЦИЙ НА ТЕЛЕФОНЕ;
– ПОЛОЖИТЕ ТРУБКУ И НЕ ПЕРЕЗВНИВАЙТЕ В БАНК ВСТРЕЧНЫМ ЗВОНКОМ. МОЖНО ПЕРЕЗВОНИТЬ В БАНК ПО ОФИЦИАЛЬНОМУ НОМЕРУ (ОН УКАЗАН НА КАРТЕ) И СООБЩИТЬ О ЗВОНКЕ

ВАЖНО!

МОШЕННИКИ ВОРУЮТ БАЗЫ ДАННЫХ И НАЗЫВАЮТ ВАС ПО ИМЕНИ-ОТЧЕСТВУ, А В ТЕЛЕФОНЕ ВИДЕН НОМЕР ВАШЕГО БАНКА

БУДЬТЕ ГОТОВЫ И ПРОЯВИТЕ БДИТЕЛЬНОСТЬ

На что следует обратить внимание? Создание Интернет-магазина – дело нескольких часов, изменение его названия и переезд на другой адрес – дело нескольких минут. Будьте осторожны при совершении покупок в только что открывшихся Интернет-магазинах.

6. Неточности или несоответствия в описании товаров. Если в описании товара присутствуют явные несоответствия, следует осторожно отнестись к подобному объявлению.

На что следует обратить внимание? Внимательно прочитайте описание товара и сравните его с описаниями на других Интернет-ресурсах.

7. Излишняя настойчивость продавцов и менеджеров. Если в процессе совершения покупки менеджер магазина начинает торопить вас с заказом и оплатой товара, убеждая в том, что если не заказать его сейчас, то цена изменится или товар будет снят с продажи, не поддавайтесь на уговоры и трезво оценивайте свои действия.

На что следует обратить внимание? Злоумышленники часто используют временной фактор для того, чтобы не дать жертве оценить все нюансы сделки. Тщательно проверяйте платежную информацию и при наличии любых сомнений откладывайте сделку.

8. Подтверждение личности продавца путем направления отсканированного изображения паспорта. Ожидая перевода денег, продавцы в социальных сетях часто направляют изображение своего паспорта покупателю с целью подкупить его доверие.

На что следует обратить внимание? Помните, что при современном развитии техники изготовить изображение паспорта на компьютере не представляет никакого труда. Данное изображение никаким образом не может подтверждать личность лица, направившего его вам.

ВЫВОД

Если Интернет-магазин или объявление соответствуют хотя бы одному из указанных признаков, это серьезный повод задуматься о целесообразности совершения сделки.

Если под их описание подходят два или более признака, мы настоятельно рекомендуем вам воздержаться от контактов с данным продавцом или магазином.

Адрес страницы в интернете: <https://www.mvd.gov.by/ru/page/urpsvt/profilaktika/pokupki-cherez-internet-ne-stan-zhetvoj-obmana>

2024 © Министерство внутренних дел Республики Беларусь

ВНИМАНИЕ!

ЗАЩИТИ СВОЮ БАНКОВСКУЮ КАРТУ



Хранить пинкод вместе
с картой

НЕЛЬЗЯ



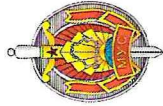
Сообщать CVV-код или
отправлять его фото



Распространять
личные данные, логин
и пароль доступа к
системе
«Интернет-банкинг»



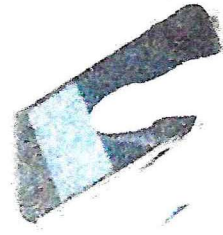
Сообщать данные,
полученные в виде
SMS-сообщений,
сеансовые пароли, код
авторизации и т.д.



Сохрани эту информацию и поделись с другими

КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ?

ВАМ ПОЗВОНИЛ НЕИЗВЕСТНЫЙ
И ПРЕДСТАВИЛСЯ
СОТРУДНИКОМ БАНКА



ЭТО

МОШЕННИКИ! ПРЕРВИТЕ РАЗГОВОР

ОН СООБЩИЛ О ПОДОЗРИТЕЛЬНЫХ
ОПЕРАЦИЯХ И ПОПРОСИЛ ВАС
ПРЕДОСТАВИТЬ ЛЮБУЮ
ИНФОРМАЦИЮ ПО КАРТЕ
или ПРОЙТИ К БАНКОМАТУ

И ОБРАТИТЕСЬ

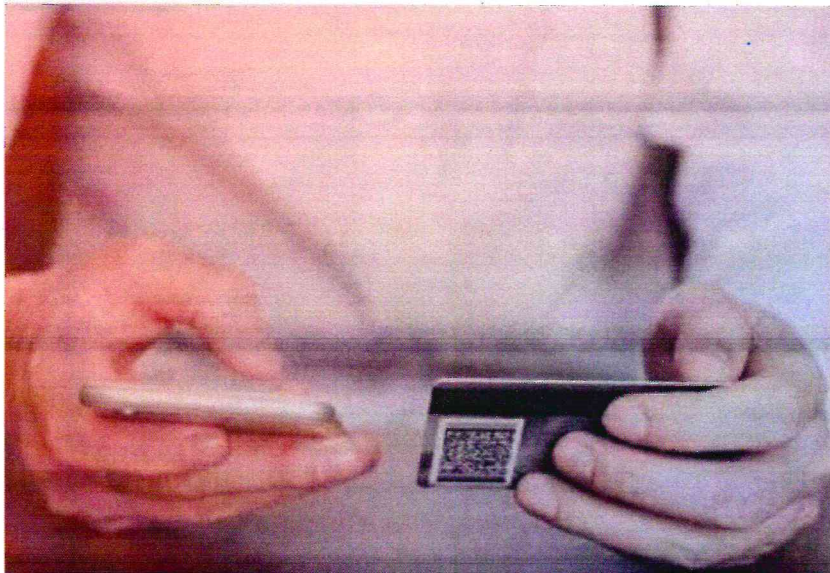
В ОТДЕЛЕНИЕ БАНКА!

БУДЬТЕ БДИТЕЛЬНЫ!



**ВЫ ДОЛЖНЫ
ЗНАТЬ!**

СТАТЬЯ 222 УГОЛОВНОГО КОДЕКСА РЕСПУБЛИКИ БЕЛАРУСЬ, ИЛИ КАК НЕ СТАТЬ ПРЕСТУПНИКОМ



Все чаще в социальных сетях и мессенджерах пользователям стали приходить сообщения с предложениями без особых усилий за день заработать до 100 долларов. Что для этого нужно? Всего ни чего, оформить на себя банковскую карту в банке, на который укажет мнимый работодатель, и передать сообщением в сети Интернет полученные реквизиты карты потенциальному работодателю.

Как правило, все общение проходит в сети Интернет без личного контакта. Истории, для чего нужна работодателю банковская карта чужого человека, различны. В основном это необходимость перевода денег на счета в Беларуси, а там он не может, так как находится в другой стране.

Человек, согласившийся на такие условия сделки, становится так называемым «ДРОПОМ» – подставным лицом в серых схемах кибермошенников. Дроп – это тот человек, который соглашается, чтобы его банковская карта стала «транзитной» для украденных мошенниками денег. Дроп переводит незаконно полученные денежные средства между разными счетами. Такая цепочка переводов нужна для того, чтобы запутать следы киберпреступников и усложнить работу милиции.

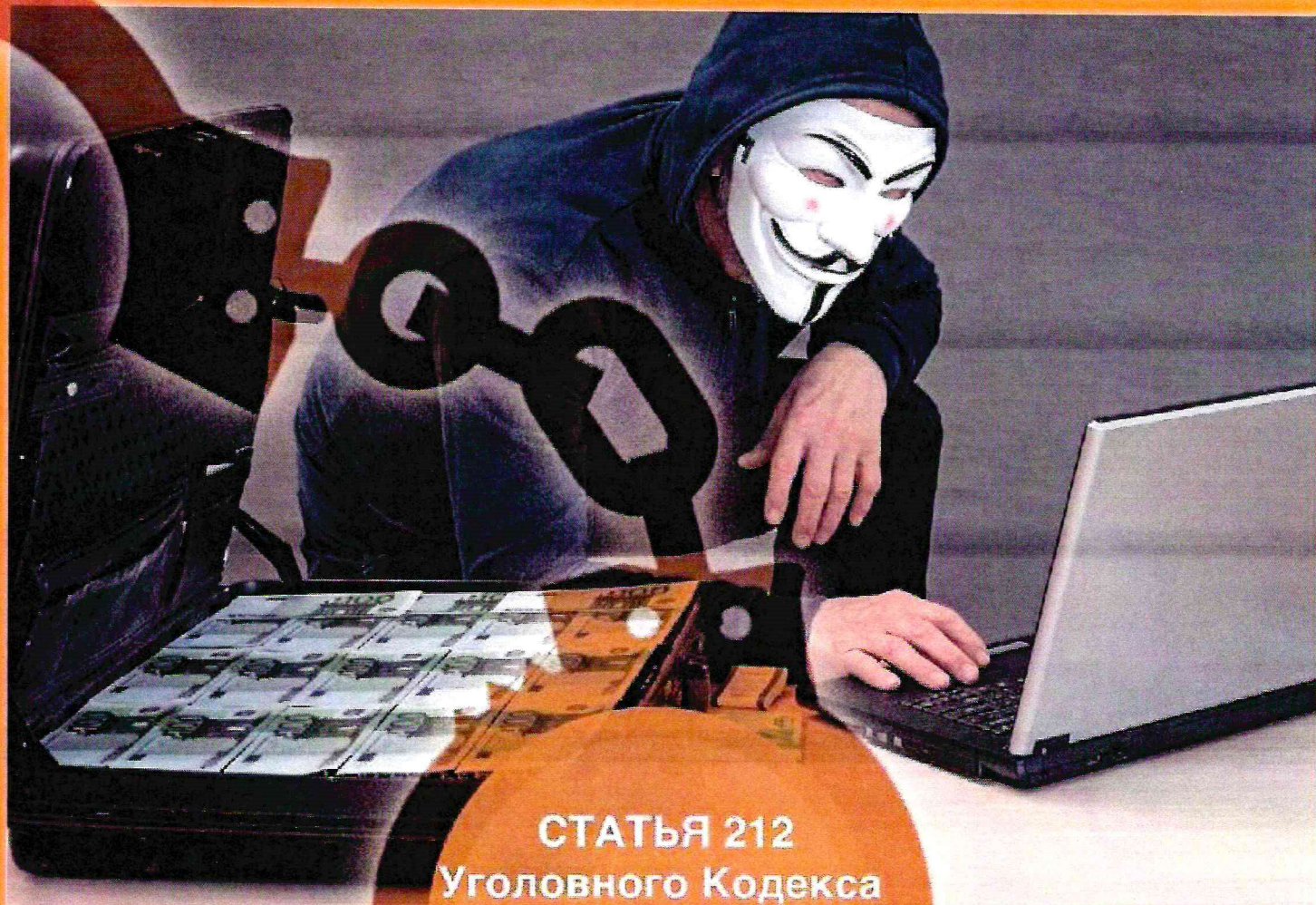
Кто такой ДРОП?

Дропы бывают «разводные» и «неразводные». Отличие их только в том, что неразводные осознают всю тяжесть совершаемых ими деяний и умышленно занимаются этим. В большинстве своем это студенты, школьники, малоимущие, которые нуждаются в финансах. Разводные «дропы» не знают о том, что идут на преступление. Они думают, что действительно работают, получают зарплату и т.д.

Ответственность за такие действия наступает по статье 222 УК Республики Беларусь (незаконный оборот средств платежа и (или) инструментов) с 16 летнего возраста.

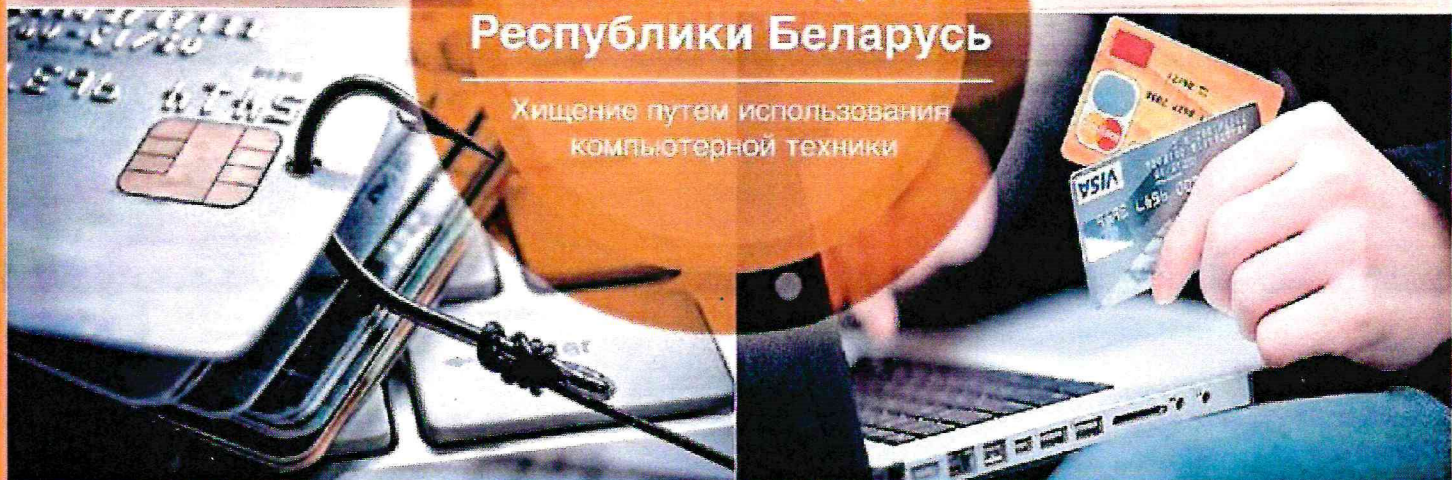
1. Изготовление в целях сбыта либо сбыт поддельных банковских платежных карточек, иных платежных инструментов и средств платежа, а равно совершенное из корыстных побуждений незаконное распространение реквизитов банковских платежных карточек либо аутентификационных данных, посредством которых возможно получение доступа к счетам либо электронным кошелькам, – наказываются штрафом, или ограничением свободы на срок от двух до пяти лет, или лишением свободы на срок от двух до шести лет.

2. Те же действия, совершенные повторно, либо организованной группой, либо в особо крупном размере, – наказываются ограничением свободы на срок от трех до пяти лет или лишением свободы на срок от трех до десяти лет со штрафом или без штрафа.



СТАТЬЯ 212
Уголовного Кодекса
Республики Беларусь

Хищение путем использования
компьютерной техники



Хищение имущества путем изменения информации,
обрабатываемой в компьютерной системе, хранящейся
на машинных носителях или передаваемой по сетям
передачи данных, либо путем введения
в компьютерную систему ложной информации
наказывается лишением свободы на срок
ДО ТРЕХ ЛЕТ.



МИЛИЦИЯ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ МВД РБ

ВНИМАНИЕ! МОШЕННИЧЕСТВО!

1 

поступает звонок
с неизвестного
номера

2 

звонящий
представляется
вошшим
родственником

3 

он говорит,
что сбил человека
или из-за него
человек
попал в ДТП

4 

он просит денег
как компенсацию
вреда или
чтобы «замять» дело

5 

затем звонит
«милиционер»/
«следователь»
и подтверждает
легенду

6 

за деньгами
приезжает
курьер

Мама, папа, я
в беде!

Нужны деньги!
Срочно!

Что делать?

1. немедленно положить трубку
2. самому перезвонить родственнику
3. не передавать курьерам никаких денег
4. сообщить в милицию



не дай себя обмануть!



МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РЕСПУБЛИКИ БЕЛАРУСЬ

круглосуточный
единый
номер

102

ОСТРОЖНО, МОШЕННИКИ!

Наибольшие темпы прироста - у преступлений, связанных с использованием или применением расчетных пластиковых карт и средств мобильной связи

ЗВОНОК ОТ
"СЛУЖБЫ
БЕЗОПАСНОС
ТИ БАНКА"

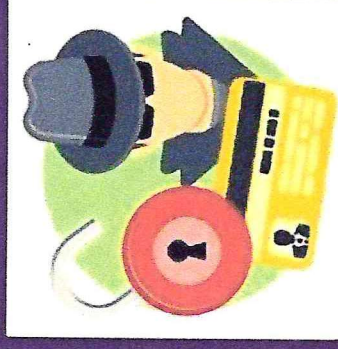
САЙТЫ-
ДВОЙНИКИ

ВИРУСНАЯ
ССЫЛКА

ВЗЛОМ
СТРАНИЧКИ
В СОЦСЕТЯХ

"РОЗЫГРЫШ
ПРИЗОВ"

"СЛУЧАЙ С
РОДСТВЕННИ
КОМ"



БЫТЬ ХАКЕРОМ -



УПРАВЛЕНИЕ
ПО ПРОТИВОДЕЙСТВИЮ
КИБЕРПРЕСТУПНОСТИ
УВД ВИТЕБСКОГО
ОБЛИСПОЛКОМА

БОЛЬШЕ ИНФОРМАЦИИ
В TELEGRAM-КАНАЛЕ
ЦИФРОВАЯ ГРАМОТНОСТЬ
T.ME/CIFGRAM



НЕ РАЗВЛЕЧЕНИЕ, ▶ А ПРЕСТУПЛЕНИЕ УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ЗА КИБЕРПРЕСТУПЛЕНИЯ НАСТУПАЕТ:

с 14 лет

статья 212 УК

Хищение имущества путем
модификации компьютерной
информации

наказывается вплоть до
лишения свободы на срок
до **12 лет**

статья 340 УК

Заведомо ложное
сообщение об опасности

наказывается вплоть до
лишения свободы на срок
до **7 лет**

с 16 лет

статья 222 УК

Незаконный оборот средств
платежа и (или) инструментов

наказывается вплоть до
лишения свободы на срок
до **10 лет**

статья 349 УК

Несанкционированный
доступ к компьютерной
информации

наказывается вплоть до
лишения свободы на срок
до **7 лет**

ВНИМАНИЕ!
ПОЯВИЛСЯ НОВЫЙ ВИД ВИШИНГА!



НЕ СОВЕРШАЙТЕ НИКАКИХ ДЕЙСТВИЙ НА СМАРТФОНЕ ПО ПРОСЬБЕ ПОСТОРОННИХ ЛЮДЕЙ! ТЕМ БОЛЕЕ, НЕ СООБЩАЙТЕ ИМ КОДЫ, ПАРОЛИ, И ДР.ИНФОРМАЦИЮ

НЕ СОХРАНЯЙТЕ В ПРИЛОЖЕНИЯХ И БРАУЗЕРАХ ПАРОЛИ, КОДЫ, ЛОГИНЫ. ПРЕСТУПНИК МОЖЕТ УЗНАТЬ КОД ИЗ ПРИСЛАННОГО SMS-СООБЩЕНИЯ



ПРЕСТУПНИК ПО ТЕЛЕФОНУ ПРОСИТ ВАС УСТАНОВИТЬ ПРОГРАММУ НА ТЕЛЕФОН ДЛЯ ДИСТАНЦИОННОГО ДОСТУПА И СООБЩИТЬ ЕМУ ПАРОЛЬ И КОД



УПРАВЛЕНИЕ «К» МВД БЕЛАРУСИ

ВНИМАНИЕ МОШЕННИКИ!!!

1

НЕ СЛЕДУЙ инструкциям
незнакомцев, позвонившим с
неизвестного номера

2

НЕ СОВЕРШАЙ никаких
действий на смартфоне по
просьбе посторонних лиц

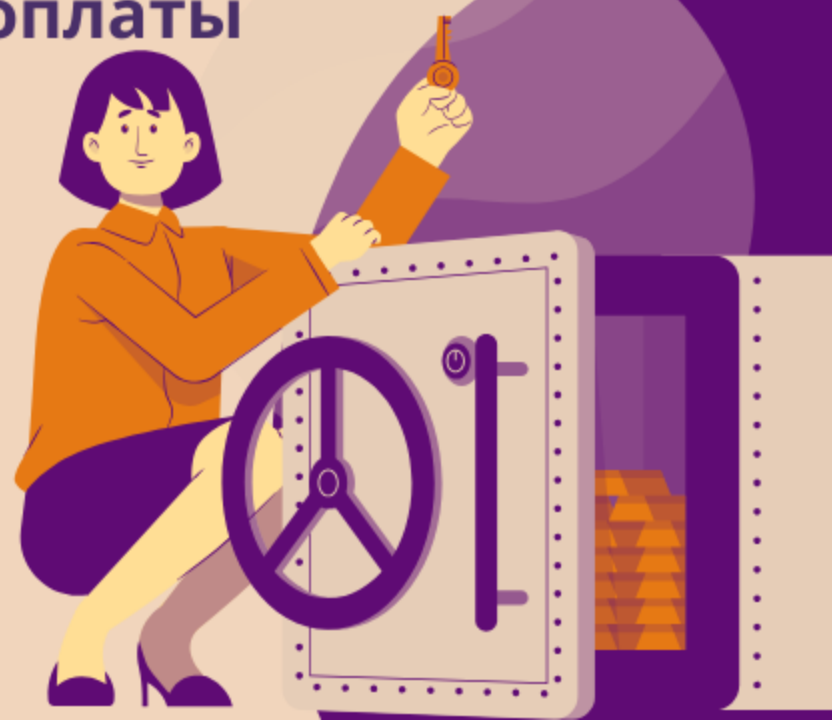
3

НЕ СООБЩАЙ неизвестным лицам
свои персональные данные

4

НЕ ПЕРЕВОДИ деньги
незнакомым людям в
качестве предоплаты

Отделение по противодействию
киберпреступности
криминальной милиции
Ленинского РУВД г.Могилева





КАК ЗАЩИТИТЬ СВОЮ БАНКОВСКУЮ КАРТУ?!

НЕЛЬЗЯ

1

Хранить пинкод вместе с картой

2

Распространять личные данные, логин и пароль к системе “Интернет-банкинг”

3

Сообщать CVV-код или отправлять его фото

4

Сообщать данные, полученные в виде SMS-сообщений, сеансовые пароли, код авторизации и т.д



Отделение по противодействию
киберпреступности
криминальной милиции
Ленинского РУВД г.Могилева



ВИШИНГ

ЭТО ВИД МОШЕННИЧЕСТВА, ПРИ КОТОРОМ

ЗАХОМЫШАБЕННИКИ ЗВОНЯТ ВАМ ПО ТЕЛЕФОНУ

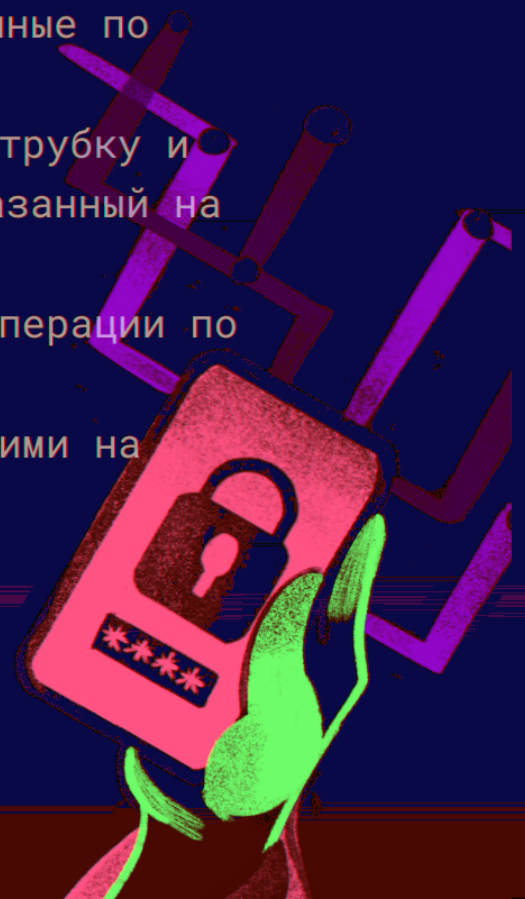
ПРЕДСТАВЛЯЯСЬ СОТРУДНИКАМИ БАНКОВ,
ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ, ТЕХПОДДЕРЖКИ
ИЛИ ДРУГИХ ОФИЦИАЛЬНЫХ СТРУКТУР, ЧТОБЫ
ВЫМАНИТЬ ЛИЧНЫЕ ДАННЫЕ, КОДЫ ИЗ SMS И
ДОСТУП К СЧЕТАМ.

КАК РАБОТАЮТ ВИШЕРЫ?

- ✗ Звонок от "банка" – мошенник представляется сотрудником службы безопасности и сообщает, что с вашего счета пытаются снять деньги. Вас убеждают назвать данные карты или код из SMS "для отмены операции".
- ✗ Сообщение о родственнике в беде – мошенники говорят, что ваш близкий человек попал в ДТП или в полицию, и требуют срочно перевести деньги.

КАК ЗАЩИТИТЬСЯ?

- ✓ Никогда не сообщайте пароли, коды из SMS, CVC-код и другие конфиденциальные данные по телефону.
- ✓ Если звонят из "банка" – положите трубку и перезвоните на официальный номер, указанный на сайте банка.
- ✓ Не выполняйте срочные финансовые операции по просьбе звонящего.
- ✓ Будьте осторожны с номерами, похожими на номера официальных организаций.
- ✓ Настройте блокировку неизвестных и подозрительных номеров.



Отделение по противодействию
киберпреступности криминальной милиции
Ленинского РОВД г.Могилёва