

УТВЕРЖДАЮ

Заместитель
Сморгонского
исполнительного

председателя
районного
комитета

И.П.Счастный

марта 2024 г.

МЕХАНИЗМ

выполнения Комплексного плана мероприятий, направленных на принятие эффективных мер по противодействию киберпреступлениям, профилактике их совершения, повышению цифровой грамотности населения на территории Сморгонского района на 2024 – 2025 годы

Мероприятие	Срок исполнения	Ответственные
Профилактические мероприятия		
1. Размещение и регулярное обновление на интернет-сайте райисполкома информационных материалов по профилактике и противодействию киберпреступности	2024 – 2025 годы	отдел внутренних дел Сморгонского районного исполнительного комитета (далее – РОВД), отдел идеологической работы и по делам молодежи райисполкома
2. Включение вопросов профилактики киберпреступности и мошенничеств, совершаемых с использованием информационно-коммуникационных технологий, в тематику единых дней информирования	2024 – 2025 годы	отдел идеологической работы и по делам молодежи райисполкома, РОВД
3. Размещение и обновление на информационных стендах, официальных сайтах организаций	2024 – 2025 годы	отдел идеологической работы и по делам молодежи

Мероприятие	Срок исполнения	Ответственные
информационных профилактических материалов по тематике противодействия киберпреступности		райисполкома, организации района
4. Размещение на информационных стендах учреждений культуры и образования социальной рекламы, наглядной агитации по тематике профилактики и противодействия киберпреступности, информации об ответственности за совершение киберпреступлений	2024 – 2025 годы	учреждения культуры и образования в сфере культуры
5. Проведение тематических мероприятий по противодействию кибербуллингу, вовлечению несовершеннолетних в противоправную деятельность в сети Интернет	2024 – 2025 годы	ГУК «Сморгонская районная библиотека», ГУК «Сморгонский районный центр культуры»
6. Организация и проведение выступлений представителей правоохранительных органов по тематике кибербезопасности и профилактике киберпреступности	2024 – 2025 годы	учреждения культуры и образования в сфере культуры, отдел идеологической работы и по делам молодежи райисполкома
7. Освещение вопросов цифровой безопасности, этикета, ответственности за правонарушения, безопасной работы в сети Интернет на информационных, классных часах	2024 – 2025 годы	управление образования райисполкома
8. Размещение и обновление на информационных стендах (уголках правовых знаний), официальных сайтах учреждений образования памяток для обучающихся и законных представителей «Компьютерная безопасность»	2024 – 2025 годы	управление образования райисполкома
9. Размещение (распространение) социальной, телевизионной, наружной рекламы, рекламы на	2024 – 2025 годы	отдел идеологической работы и по делам молодежи

Мероприятие	Срок исполнения	Ответственные
транспортных средствах по тематике кибербезопасности, а также ее распространение в местах массового пребывания граждан и в глобальной компьютерной сети интернет		райисполкома, филиал «Автомобильный парк № 17» ОАО «Гроднооблавтотранс»
10. Распространение среди социально уязвимых слоев граждан (престарелых, инвалидов) тематических информационных материалов (буклетов, памяток и др.) о формах и методах совершения киберпреступлений, правилах безопасной работы в сети Интернет, цифровой и финансовой грамотности	2024 – 2025 годы	управление по труду, занятости и социальной защите райисполкома, учреждение «Территориальный центр социального обслуживания населения «Теплый дом» (далее – УТЦСОН «Теплый дом»)
11. Проведение занятий для социальных работников территориальных центров социального обслуживания населения по вопросам профилактики киберпреступлений и мошенничеств, совершаемых в отношении пожилых граждан и инвалидов, в рамках «Школы социального работника»	2024 – 2025 годы	управление по труду, занятости и социальной защите райисполкома, УТЦСОН «Теплый дом»
12. Информирование населения (при необходимости) о новых способах совершения киберпреступлений путем размещения информационных материалов на стендах объектов торговли	2024 – 2025 годы	управление экономики, торговли и услуг райисполкома, РОВД
13. Размещение профилактических материалов по тематике противодействия киберпреступности на извещениях об оплате жилищно-коммунальных услуг	2024 – 2025 годы	отдел жилищно-коммунального хозяйства райисполкома, РОВД

УТВЕРЖДАЮ

Директор государственного учреждения культуры «Сморгонский районный центр культуры»

Г.И. Кротенок

План

мероприятий, направленных на принятие эффективных мер по противодействию киберпреступлениям, профилактике их совершения, повышению цифровой грамотности населения на 2025 год

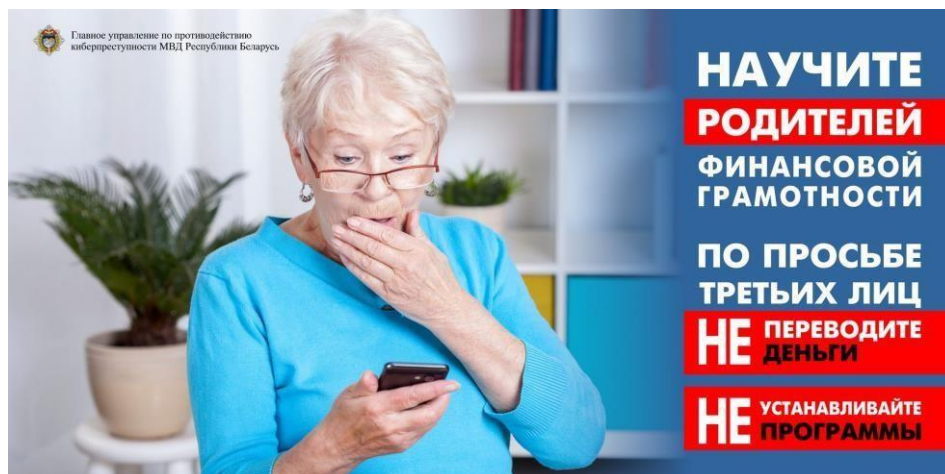
Дата проведения	Форма и название мероприятия	Место проведения	Ответственный
На протяжении года	Включение вопросов профилактики киберпреступности и мошенничеств, совершаемых с использованием информационно-коммуникационных технологий в тематику единых дней информирования	ГУК «Сморгонский районный центр культуры»	Сабинская А.С., заместитель директора
На протяжении года	Постоянное информирование общественности о современных угрозах, индивидуальных и общих мерах борьбы с ними, порядке сообщения правоохранительным органам о признаках и фактах преступлений, получение помощи пострадавшим и их близким. Размещение информационного материала: 1. «Защита банковской карточки», 2. «Не дай себя обмануть!», 3. «Осторожно! Мошенники»	Сайт ГУК «Сморгонский РЦК», официальные страницы ВК, ОК, Фейсбук, Инстаграм, Телеграм канал «Культура Сморгонщины. Информационные стенды РЦК и структурных подразделений	Смагур И.Ф., заведующий сектором рекламы и менеджмента; заведующие структурными подразделениями

	интернете» и др.		
На протяжении года	Проведение тематических мероприятий по противодействию кибербуллингу, вовлечению несовершеннолетних в противоправную деятельность в сети Интернет	ГУК «Сморгонский РЦК», структурные подразделения	Сабинская А.С., заместитель директора; заведующие структурными подразделениями
На протяжении года	Организация и проведение выступлений представителей правоохранительных органов по тематике кибербезопасности и профилактики киберпреступности	ГУК «Сморгонский РЦК», структурные подразделения	Сабинская А.С., заместитель директора; заведующие структурными подразделениями

Заместитель директора



А.С. Сабинская



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

ОСТОРОЖНО!

МОШЕННИКИ В ИНТЕРНЕТЕ



Не торопись переходить по ссылке, полученной от незнакомца: возможно, она ведет на фишинговый сайт



Не спеши переходить по ссылке: введи адрес вручную



НЕ пользуйся открытыми вай-фай-сетями в кафе или на улице



Фишинговая ссылка может прийти в мессенджере, по электронной почте, в sms-сообщении



Сохрани эту информацию и поделись с другими

ВАМ ЗВОНЯТ ПО ТЕЛЕФОНУ И СООБЩАЮТ

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

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

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

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

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

ЧТО ДЕЛАТЬ:

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

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

НИКАКИХ ДОПЛАТ ОФИЦИАЛЬНЫЕ СОЦИАЛЬНЫЕ СЛУЖБЫ НИКОГДА НЕ ТРЕБУЮТ

НЕ ВЕРЬТЕ, ВАМ НАВЕРНЯКА ЗВОНЯТ МОШЕННИКИ

СОТРУДНИКИ БАНКОВ НЕ ЗВОНЯТ КЛИЕНТАМ И НИКОГДА НЕ ТРЕБУЮТ НАЗЫВАТЬ СЕКРЕТНЫЕ СВЕДЕНИЯ О КАРТЕ ИЛИ СЧЕТЕ;

НИКОГДА НЕ НАЗЫВАЙТЕ И НЕ ВВОДИТЕ ПИН-КОД, ТРЕХЗНАЧНЫЙ КОД НА ОБРАТНОЙ СТОРОНЕ КАРТЫ ИЛИ ОДНОРАЗОВЫЙ ПАРОЛЬ ИЗ SMS;

НЕ НАБИРАЙТЕ НИКАКИХ КОМБИНАЦИЙ НА ТЕЛЕФОНЕ;

ПОЛОЖИТЕ ТРУБКУ И НЕ ПЕРЕЗВАНИВАЙТЕ 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

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**

НАУЧИТЕ СВОИХ РОДИТЕЛЕЙ ФИНАНСОВОЙ ГРАМОТНОСТИ

ПО ПРОСЬБЕ ТРЕТЬИХ ЛИЦ

НЕ УСТАНАВЛИВАЙТЕ
ПРОГРАММЫ

НЕ ПЕРЕВОДИТЕ
ДЕНЬГИ



Главное управление по противодействию
киберпреступности МВД Республики Беларусь

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

**ВАШ СЫН
ПОПАЛ В БЕДУ!
НУЖНЫ
ДЕНЬГИ!**



mvd.gov.by



Безопасный интернет для детей

**СОХРАНИ
ИНФОРМАЦИЮ**

**не сообщай незнакомцам
свой логин и пароль**

**не открывай файлы из
непроверенных источников**

**не заходи на сайты, которые
защита компьютера считает
подозрительными**



**НЕ отправляй незнакомцам
свои фото и видео**

Злоумышленники могут узнать что-то
нужное им о твоей жизни

**ГЛАВНЫЕ
ПРАВИЛА
ЦИФРОВОЙ
ГИГИЕНЫ**



**НЕ встречайся с людьми,
с которыми знакомишься
только в интернете**

За маской онлайн-собеседника
может скрываться злоумышленник



**НЕ сообщай в интернете
свой реальный
адрес и телефон**

Злоумышленник может встретить
тебя с недобрыми намерениями



**НЕ отправляй личные данные
для участия в конкурсах
на малоизвестных сайтах**

Информацией могут завладеть и
воспользоваться недоброжелатели

**РОДИТЕЛИ!
научите детей**

**пользоваться
интернетом
правильно!**



**Всегда важно помнить: неправильное поведение
в интернете может принести большой вред.**

не дай себя обмануть!



**МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РЕСПУБЛИКИ БЕЛАРУСЬ**

**круглосуточный
единый
номер**

102

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

Безопасный интернет для детей

ПРАВИЛА ЦИФРОВОЙ ГИГИЕНЫ

- НЕ отправляй** незнакомцам свои фото и видео
Злоумышленники могут узнать что-то нужное о твоей жизни
- НЕ встречайся** с людьми, с которыми знаком только в интернете
За маской онлайн-собеседника может скрываться злоумышленник
- НЕ сообщай** в интернете свой реальный адрес и телефон
Злоумышленник может встретить тебя с недобрыми намерениями
- НЕ отправляй** деньги донельзя для участия в конкурсах на малоизвестных сайтах
Информацией могут заманить и воспользоваться недоброжелатели

Всегда важно помнить: неправильное поведение в интернете может принести большой вред.

не дай себя обмануть!

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РЕСПУБЛИКИ БЕЛАРУСЬ

круглосуточный
единый
номер **102**

научись пользоваться интернетом правильно!

ВНИМАНИЕ!

ЦИФРОВАЯ БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ



НЕ переходите по ссылкам и письмам от незнакомцев, не нажимайте на картинки и кнопки



НЕ верьте обещаниям внезапных выигрышей

**УСТАНОВИТЕ АНТИВИРУС НА ВСЕ
ВАШИ УСТРОЙСТВА**



НЕ сообщайте свои персональные данные и данные банковской карты



НЕ указывайте личную информацию в открытых источниках



НЕ используйте одинаковые пароли для всех аккаунтов



Сохрани эту информацию и поделись с другими

! ВНИМАНИЕ, ОПАСНОСТЬ !

ЗАЩИТИТЕ СЕБЯ ОТ МОШЕННИКОВ:

НЕ ПЕРЕХОДИТЕ по ссылкам и письмам от
незнакомцев, не нажимайте на картинки и кнопки...

НЕ ВЕРЬТЕ обещаниям внезапных выигрышей

НЕ ИСПОЛЬЗУЙТЕ одинаковые пароли для всех
аккаунтов

НЕ УКАЗЫВАЙТЕ личную информацию в открытых
источниках

НЕ СООБЩАЙТЕ свои персональные данные
и данные банковской карты



НЕ ДАЙТЕ СЕБЯ ОБМАНУТЬ!

Если вы или ваши близкие стали
жертвами мошенников, или вы
подозреваете, что в отношении вас
планируются противоправные действия
НЕЗАМЕДЛИТЕЛЬНО СООБЩАЙТЕ В МИЛИЦИЮ!

102



mvd.gov.by



Министерство внутренних дел Республики Беларусь

БУДЬ КИБЕРГЕРОЕМ!



Будь как ниндзя!
Не сообщай незнакомым людям в
Интернете свое настоящее имя,
адрес и номер телефона.
Будь осторожен с тем, что
пишешь о себе.



Придумай сложный
пароль, как у супергероя!
Никому его не говори, ведь
это твой секретный
ключ!



Помни, что в Интернете не все
те, кем кажутся!
Не добавляй в друзья людей,
которых не знаешь в реальной
жизни.



Будь как хакер!
Не кликай на
подозрительные
ссылки.



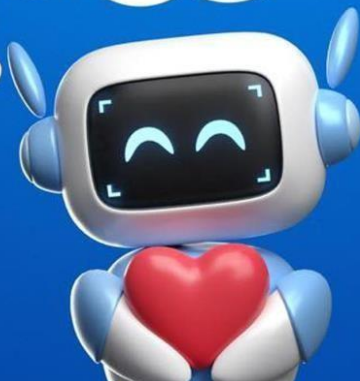
Будь осторожен, как на
минном поле!
Скачивай приложения только
из официальных магазинов.
Антивирус - твой верный
друг!



Не бойся просить о помощи!
Если тебя что-то тревожит в
Интернете, расскажи об этом
родителям или учителю.
Вместе вы сможете решить
любую проблему.



Интернет - это круто, но
помни о безопасности!
Соблюдая эти правила, ты
сможешь стать настоящим
кибергероем!



mvd.gov.by



ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО:

МОШЕННИКИ УБЕЖДАЮТ,

представляясь
сотрудниками
правоохранительных
органов, банковских
организаций или
руководителем
вашей организации.

Получить кредит, чтобы отменить якобы оформленный неизвестными на ваше имя другой кредит и перевести деньги на специальный счет

Установить программное обеспечение, якобы для предотвращения мошеннической атаки на ваш счет

Перевести накопления на якобы безопасный счет, чтобы не изъяли при обыске

Передать личные данные и код из смс, такие сведения предоставляют мошенникам доступ к счету или сервису

ОСТОРОЖНО! МОШЕННИЧЕСТВО!

В СОЦИАЛЬНЫХ СЕТЯХ И НА ТОРГОВЫХ ПЛОЩАДКАХ:

Перевести предоплату за несуществующий товар в лжемагазине или по измененным реквизитам банка

Перейти по поддельной ссылке банковской системы и ввести личные данные (логин и пароль, номер и трехзначный код с оборотной стороны банковской карты, код из СМС, кодовое слово)

Перечислить деньги на карту или оплатить родственнику, другу, любящему человеку

На поддельной бирже вложить деньги в проект, якобы для получения пассивного дохода

МОШЕННИКИ УБЕЖДАЮТ,

представляясь
продавцами, друзьями,
партнерами по бизнесу,
руководителями
инвестиционных проектов



Больше информации
на сайте
<https://mvd.gov.by>



Главное управление
по противодействию киберпреступности
КМ МВД Республики Беларусь

ПОЛЬЗУЙСЯ БЕЗОПАСНО

«банк».by



Пользуйтесь мобильными приложениями банка



Переходите в интернет-банкинг только с официального сайта банка



Проверяйте адрес интернет-банкинга в адресной строке, между последней точкой и первой наклонной чертой должно быть только так .by/



Активируйте на карте, используемой для онлайн-платежей, услугу 3-D Secure (подтверждение платежей SMS-кодом)



Не переходите в интернет-банкинг по ссылкам в поисковых системах



Не используйте SMS-коды от банка и код с обратной стороны карты для получения денежных средств



Не переходите по ссылкам из сообщений для доступа к интернет-банкингу и иным сервисам или услугам



Главное управление
по противодействию
киберпреступности
КМ МВД Республики Беларусь



Больше информации
на сайте
<https://mvd.gov.by>

Профилактическая акция «На страже цифровой безопасности»

<https://rck.by/images/nastrage.pdf>