


Федеральный проект «Информационная безопасность»

в национальном проекте
«Цифровая экономика»

Цели проекта

«Информационная безопасность»

- Увеличение внутренних затрат на развитие цифровой экономики за счёт всех источников не менее чем в три раза по сравнению с 2017 годом.
- Создание устойчивой и безопасной информационно-телекоммуникационной инфраструктуры высокоскоростной передачи, обработки и хранения больших объёмов данных, доступной для всех организаций и домохозяйств.
- Использование преимущественно отечественного программного обеспечения государственными органами, органами местного самоуправления и организациями.



Основная задача проекта «Информационная безопасность»

Обеспечение информационной безопасности на основе отечественных разработок при передаче, обработке и хранении данных, гарантирующей защиту интересов личности, бизнеса и государства

Основная задача включает в себя 56 подзадач

Задачи проекта «Информационная безопасность»

- Разработка мер регулирования вопросов целостного, устойчивого и безопасного функционирования российского сегмента сети «Интернет» (на 31.01.2021)
- Проведение мероприятий по развитию отечественной инфраструктуры телерадиовещания и обеспечения безопасности ее функционирования (на 31.12.2021)

Задачи проекта «Информационная безопасность»

- Оперативная передача данных о признаках противоправных действий (компьютерного мошенничества, навязанных услуг операторов связи, фишинговых схем) (на 30.06.2020)

Задачи проекта

«Информационная безопасность»

- Внесения изменений в Уголовный кодекс Российской Федерации, касающихся расширения криминализации новых типов деяний, совершенных с использованием информационных технологий (на 30.06.2020)
- Обеспечение контроля обработки и доступа к персональным, большим пользовательским данным, в том числе в социальных сетях и прочих средствах социальной коммуникации, а также возможности отзыва или уменьшения объёма ранее данного согласия на обработку персональных данных (на 31.12.2021)

Задачи проекта

«Информационная безопасность»

- Обеспечение развития значимых платежных систем и обеспечение их информационной безопасности, в том числе в части использования в них российских криптографических средств (на 31.10.2021)
- Создание условия для развития образования в области информационной безопасности в интересах реализации задач цифровой экономики (на 31.12.2021)

Задачи проекта

«Информационная безопасность»

- В целях обеспечения национальной безопасности нормативное обеспечение предустановки отечественных антивирусных программ на все персональные компьютеры, ввозимые и создаваемые на территории Российской Федерации (на 31.08.2020)
- Создание и обеспечение функционирования информационных систем мониторинга маршрутов трафика в сети Интернет, мониторинга и управления сетью связи общего пользования и фильтрации интернет-трафика при использовании информационных ресурсов детьми (на 31.12.2024)

Риски, возникающие при использовании услуг, сервисов и ресурсов сети Интернет

- **Электронные риски** - вредоносное программное обеспечение, целью которых заведомо является нанесение ущерба конечному пользователю.
- **Контентные риски** связаны с нахождением в сети различных материалов, содержащих противозаконную, неэтичную и вредоносную информацию.
- **Коммуникационные риски** связаны с общением и межличностными отношениями интернет-пользователей.
- **Потребительские риски** - злоупотребление в Интернете правами потребителя, кибермошенничество.
- **Компьютерная и интернет-зависимость** - навязчивый, намеренный уход в виртуальную реальность с потерей прежнего интереса к другим обязанностям и занятиям.

Компьютерное мошенничество

Мошенники используют следующие мотивы:

- беспокойство за близких и знакомых;
- беспокойство за свой телефонный номер, счёт в банке или банковскую карту;
- желание выиграть крупный приз;
- любопытство – желание получить доступ к какой-либо информации;
- желание купить или продать товар;
- желание помочь больным детям или людям, пострадавшим от стихийных бедствий.

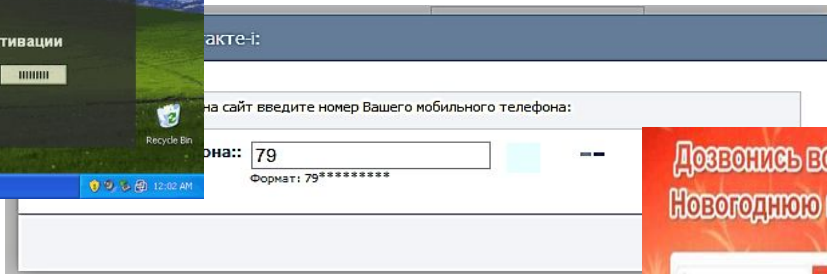
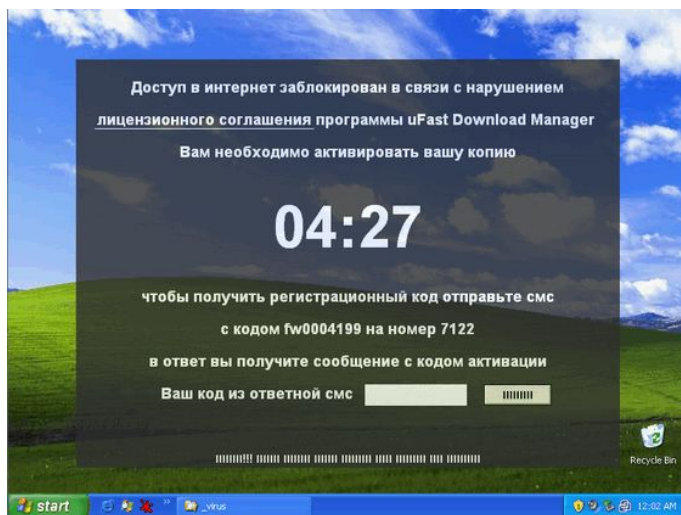
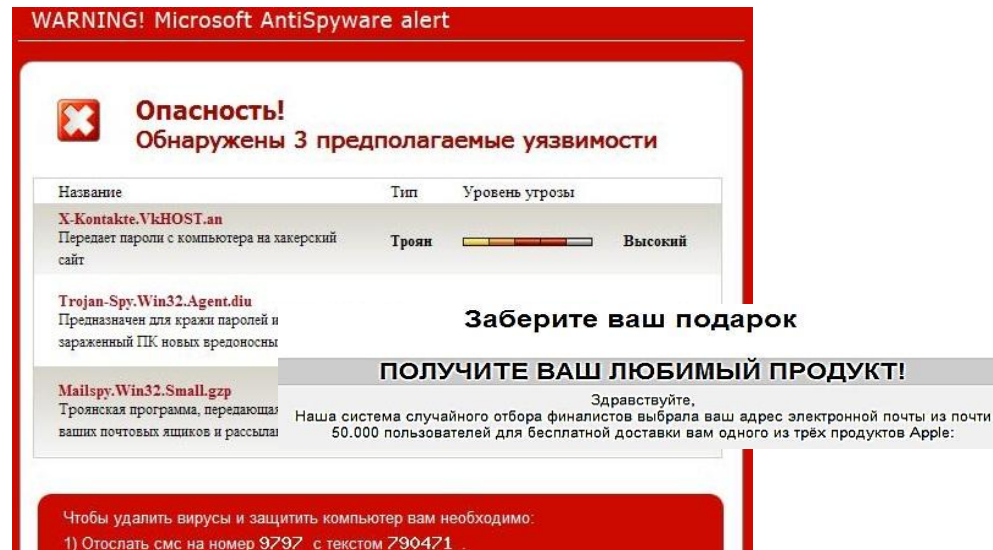
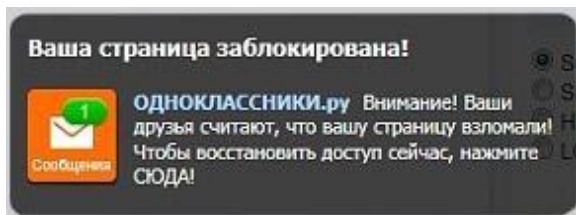
Наиболее распространенные виды мошенничества:

- телефонное мошенничество;
- мошенничество с банковскими картами;
- мошенничество в социальных сетях;
- мошенничество на сайтах бесплатных объявлений.

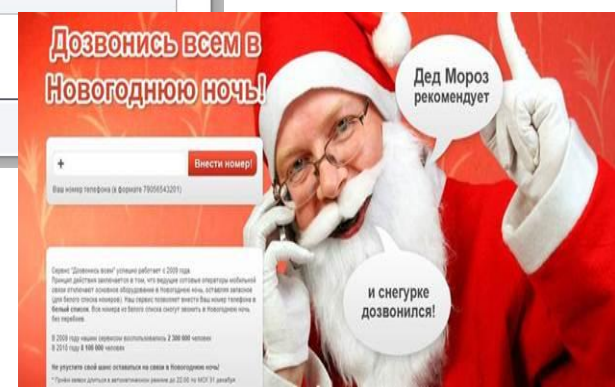
Как избежать рисков

- Используйте обновляемое антивирусное программное обеспечение.
- Устанавливайте лицензионное программное обеспечение.
- Не переходите по ссылкам и не открывайте вложения в электронных письмах, если не уверены в их содержимом.
- Проверяйте подлинность сайтов, на которых вводите персональную информацию, репутацию интернет-магазинов.
- Проводите резервное копирование информации, хранящейся на компьютере.

Примеры сообщений мошенников



Ваш аккаунт заблокирован за рассылку спам-сообщений, на основании многочисленных жалоб от пользователей. Для восстановления анкеты вам необходимо пройти процедуру активации. Активация производится в автоматическом режиме и является абсолютно **бесплатной**. Отправьте sms сообщение с текстом **151178** на номер **8353**. В ответном sms сообщении Вы получите код активации, который необходимо ввести ниже. Если в течение месяца ваш аккаунт не будет активирован, мы оставляем за собой право удалить его.



Примеры СМС-сообщений мошенников

Ваша банковская карта заблокирована! По вопросам снятия блокировки обращаться по т. 8 (800) 555-17-94 Технический отдел

МАМ!кинь УТРОМ 500р.на89654064181(Билайн)Проблемы.Потом все объясню

На ваше резюме поступила вакансия Зп до 77880 руб Сайт Zarplata.msk.ru

Платеж 200,00 р зачислен 07.11 в 11:59 через QIWI(qiwi.www.ru)

07.11.2011 11:18

Извините клал жене 200 руб.ошибочно положил вам.жене положил ещё раз,верните дочке на ном.89108050497 это МТС.Она в больнице.Спасибо!

priz.europapluz.ru

Pozdravlaem! Vy vyigrali noutbuk `Asus VX-2`.
Podrobno po telefonu: [+7-912-144-78-67](tel:+7-912-144-78-67).
Europa+

Абонент Ира оставил Вам сообщение.
Открыть: tr.im/4jz7f

с ТОБОЙ хотят познакомиться.Для получения СПИСКА отправь: МУР на 5556