ОРПСВТ КМ УВД Брестского облисполкома

Преступления в сфере высоких технологий

Основы безопасности

Киберпреступнос

Масштабы угрозы

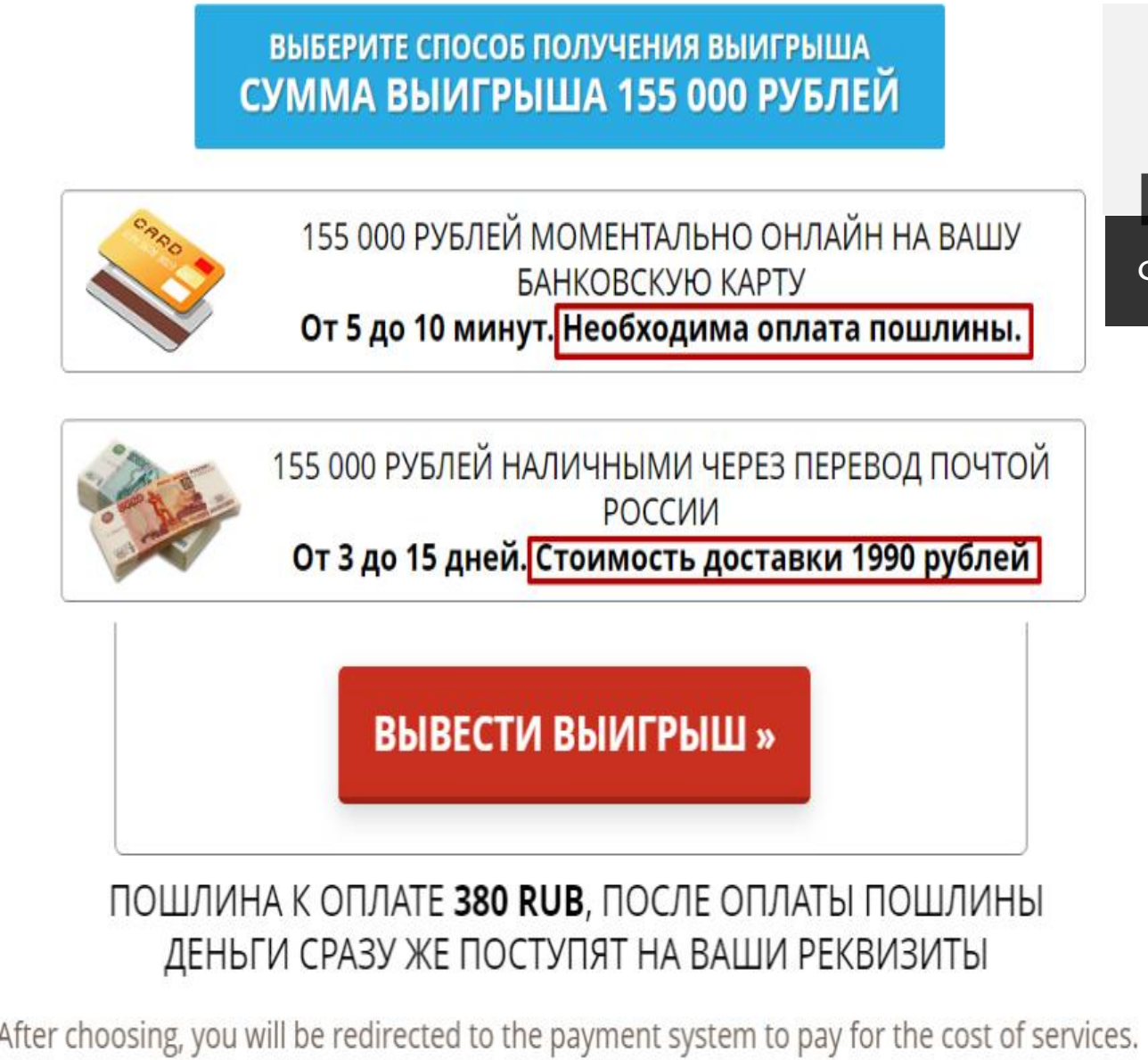

Динамика преступности в СВТ
Хищения
Информационная безопасность
В общем
243
276
260
343
728
953
225
239
182
255
476
758
18
37
78
88
252
195
2014
2015
2016
2017
2018
2019 (11 мес.)

Взлом учетных записей

Небезопасные пароли

Top 20 паролей

Gmail	Yandex	Mail.ru
123456	123456	qwerty
password	123456789	123456
123456789	111111	qwertyuiop
qwerty	qwerty	qwe123
12345678	1234567890	qweqwe
111111	1234567	klaster
abc123	7777777	1qaz2wsx
123123	123321	1q2w3e4r
1234567	000000	qazwsx
1234567890	123123	1q2w3e
iloveyou	666666	123qwe
password1	12345678	1q2w3e4r5t
000000	555555	123456789
zaq12wsx	654321	111111
tinkle	gfhjkm	zxcvbnm
qwerty123	777777	1234qwer
monkey	112233	qwer1234
target123	121212	asdfgh
dragon	987654321	marina
1q2w3e4r	159753	q1w2e3r4t5



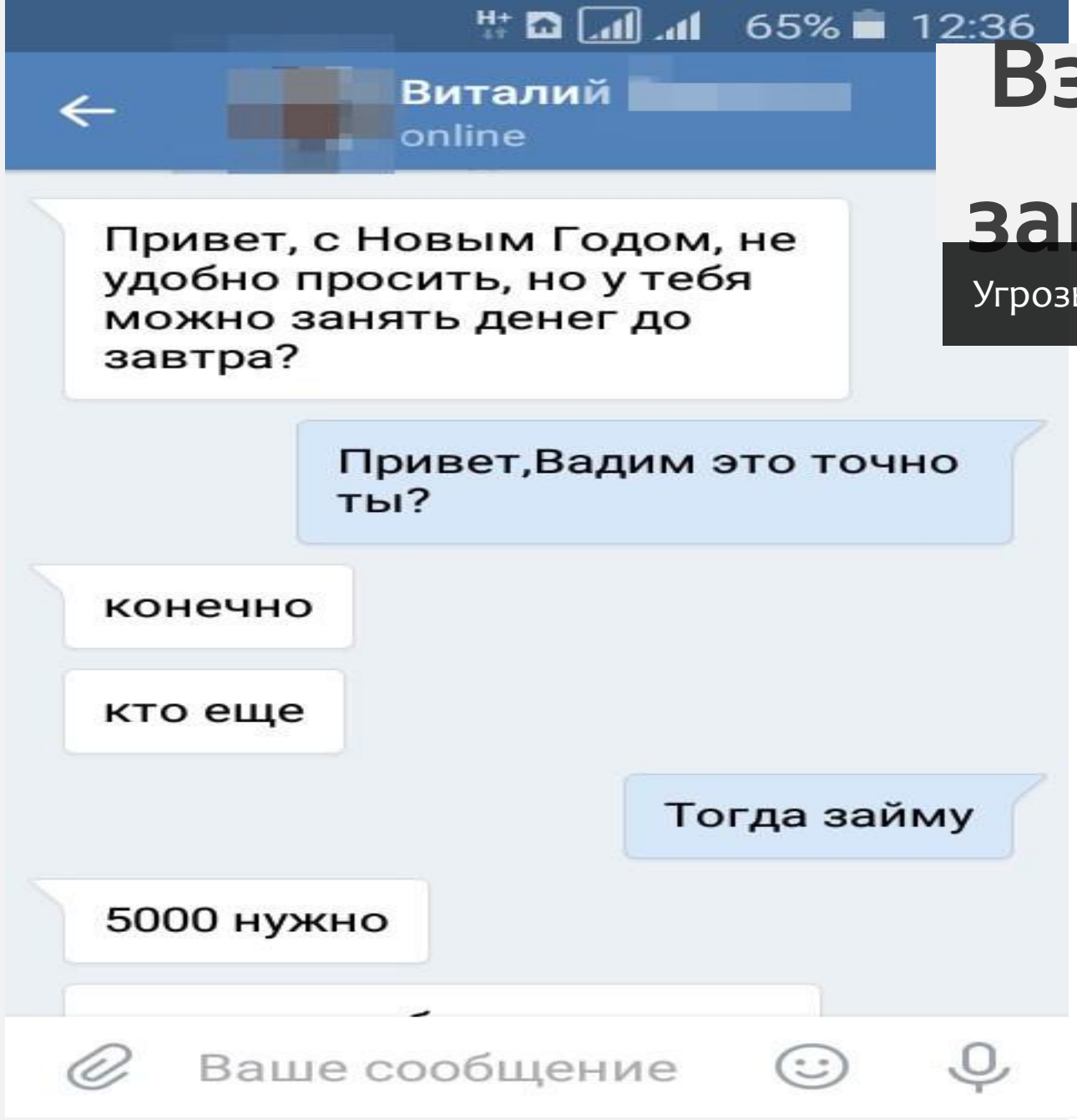
Хищение информации

Фишинговые сайты

Подобного рода нехитрые схемы используются для убеждения человека осуществить ввод какой-то личной информации (логины, пароли, реквизиты банковских карт и т.п.).

Взлом учетных записей

Угрозы



Злоумышленник, рассылает всем виртуальным «друзьям» потерпевшего просьбу под различными предлогами сообщить реквизиты банковской платежной карты. Порой преступники просят просто номер мобильного телефона и либо пытаются похитить со счета телефона деньги или наоборот используют его как промежуточное звено, направляя на этот счет чужие деньги, переводя их затем дальше, чтобы запутать свои следы.

Цифровая безопасность

Базовые правила

- **не устанавливать программное обеспечение из неизвестных источников;**
- **не открывать электронных писем от неизвестных отправителей, не переходить по ссылкам и не запускать вложенные файлы;**
- **использовать наиболее современную версию антивирусного программного обеспечения;**
- **использовать безопасные (сложные) пароли, а также механизмы дополнительной аутентификации;**
- **хранить пароли в тайне даже от близких;**
- **не осуществлять переходов по подозрительным ссылкам и не вводить личную информацию (номера карт, телефонов и т.п.) ни под какими благовидными предлогами.**

Банкоматы

Угрозы использования

Суть скимминга

Технологии кражи данных при непосредственном контакте с банковской картой постоянно совершенствуются. Обычно это происходит так:

- Клиент вставляет карту в картоприемник.
- Вводит ПИН-код
- Устройство считывает номер карты и введенный код.

Затем происходит либо блокирование карты на некоторое время, за которое мошенники успевают перевести деньги с карт-счета, либо собираются данные для создания копии карты, которая потом будет использована в других банкоматах для вывода денег.

Безопасные платежи

Основные правила

- обязательно подпишите карточку и храните в тайне ПИН-код к ней;
- храните карточку в безопасном месте, исключая доступ к ней третьих лиц;
- банки не рассылают писем, SMS-сообщений, электронных сообщений с просьбой подтвердить реквизиты карточки;
- установите лимиты расходования средств;
- обращайте внимание на людей, стоящих за вами в очереди;
- при проведении операции в организациях торговли и сервиса не выпускайте карточку из вида;
- обращайте особое внимание на действия кассира;

Безопасные платежи

Основные правила при использовании карты за границей

- открыть отдельный счет и пополнять его по мере необходимости;
- по возвращении из поездки перевести денежные средства на другой счет;
- использовать карты с чипом (стандарт EMV);
- не использовать сберегательные карточки;
- установить лимиты расходования средств и подключить услуги оповещения о транзакциях;
- при обнаружении пропажи (иных подозрительных случаях) заблокировать карту;
- bспользовать терминалы, расположенные в хорошо освещенных людных местах.