КОД ИБ

ТЮМЕНЬ

ШТАБНЫЕ КИБЕРУЧЕНИЯ

04 апреля 2024

Тюмень

ВЛАДИМИР МАКАРОВ

Руководитель направления ИБ

Кошелек

Коротко о себе

- 10+ лет практического опыта работы в области ИБ
- 5+ лет опыта руководства подразделениями ИБ
- **ISO/IEC 27001 Lead Auditor**
- **Certified Ethical Hacker (CEH)**
- Аудитор по ГОСТ Р 57580 (АБИСС)
- Руководитель направления ИБ в компании «Кошелек»

Кошелек — приложение, с которым покупают

12 млн

Человек каждый день пользуются Кошельком

230

Сотрудников в штате

414+ млн

Карт выпущено и добавлено в приложении

525 тонн

Оцифрованного пластика

Кошелёк

Зачем проводятся киберучения

- Разработка или проверка работоспособности планов реагирования на инциденты ИБ
- Симуляция последствий инцидентов для возможности проведения адекватной оценки рисков ИБ
- Формирование у специалистов понимания серьезности инцидентов ИБ

ИНЦИДЕНТ № 1

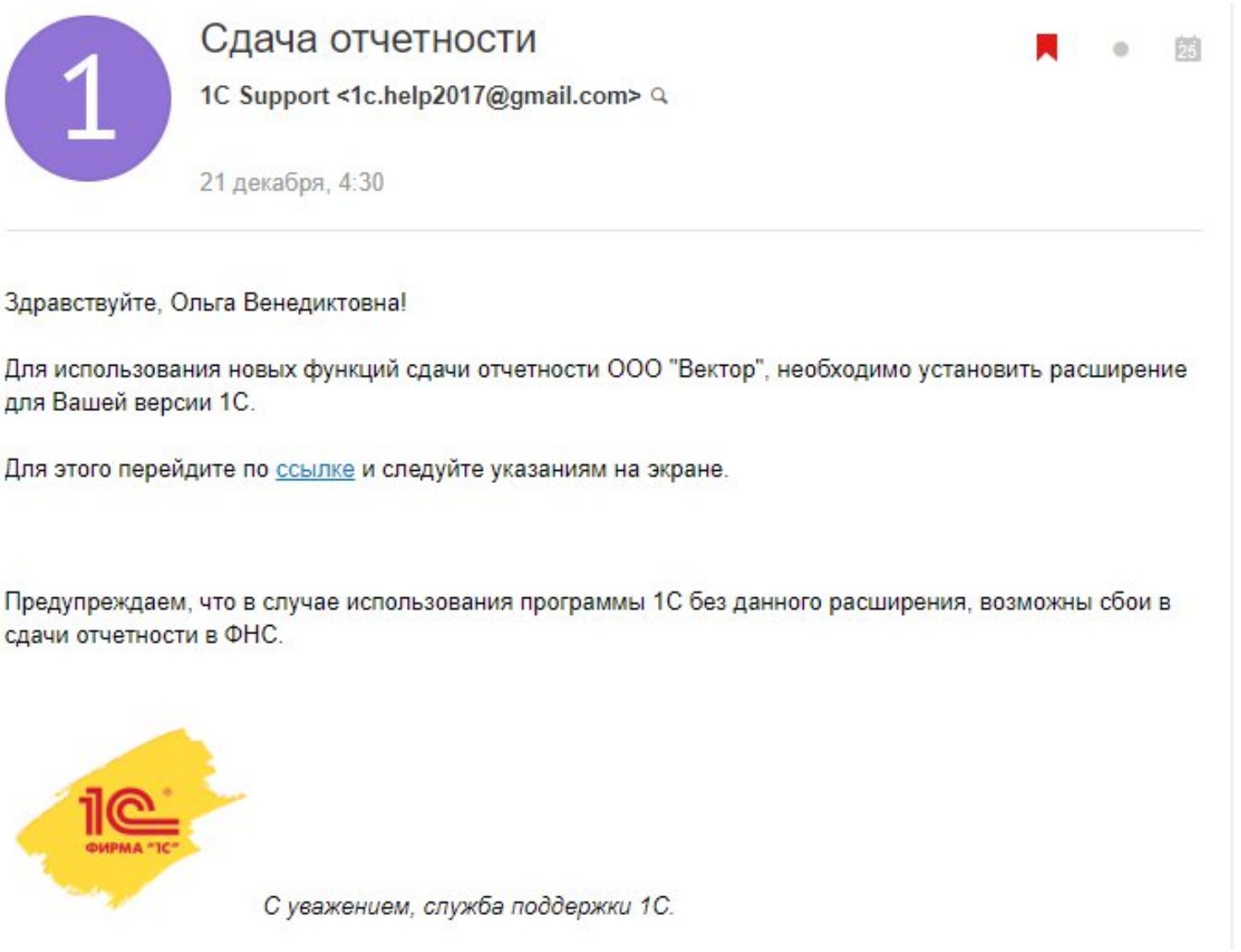
ФИШИНГ 80 УРОВНЯ

Наша компания ООО «Инновация сервис»

- Компания оказывает аутсорсинг IT услуг
- Штат 150+ человек
- Внедрена СУИБ
- Имеется отдел ИБ

Инцидент № 1

К вам утром приходит сотрудник и сообщает, что получил вот такое письмо:



Сдача отчетности

1С Support <1c.help2017@gmail.com>

21 декабря, 4:30

Здравствуйте, Ольга Венедиктовна!

Для использования новых функций сдачи отчетности ООО "Вектор", необходимо установить расширение для Вашей версии 1С.

Для этого перейдите по ссылке и следуйте указаниям на экране.

Предупреждаем, что в случае использования программы 1С без данного расширения, возможны сбои в сдачи отчетности в ФНС.

С уважением, служба поддержки 1С.

Какие риски несет инцидент?

РИСКИ:

1) Утечка информации

2) IP адрес

3) ПО

4) Сбор информации о типовой системе пользователя

5) Потеря домена

6) Шифрование

Наши действия?

Действия:

1) Опросить сотрудников: случилось ли что-то после этого?

2) Блокировка по служебным заголовкам

3) Предупредить сотрудников об атаке!!!

4) Принять решение об уведомлении НКЦКИ

5) Блокировка файла (поиск индикатора)

6) Инициировать смену паролей

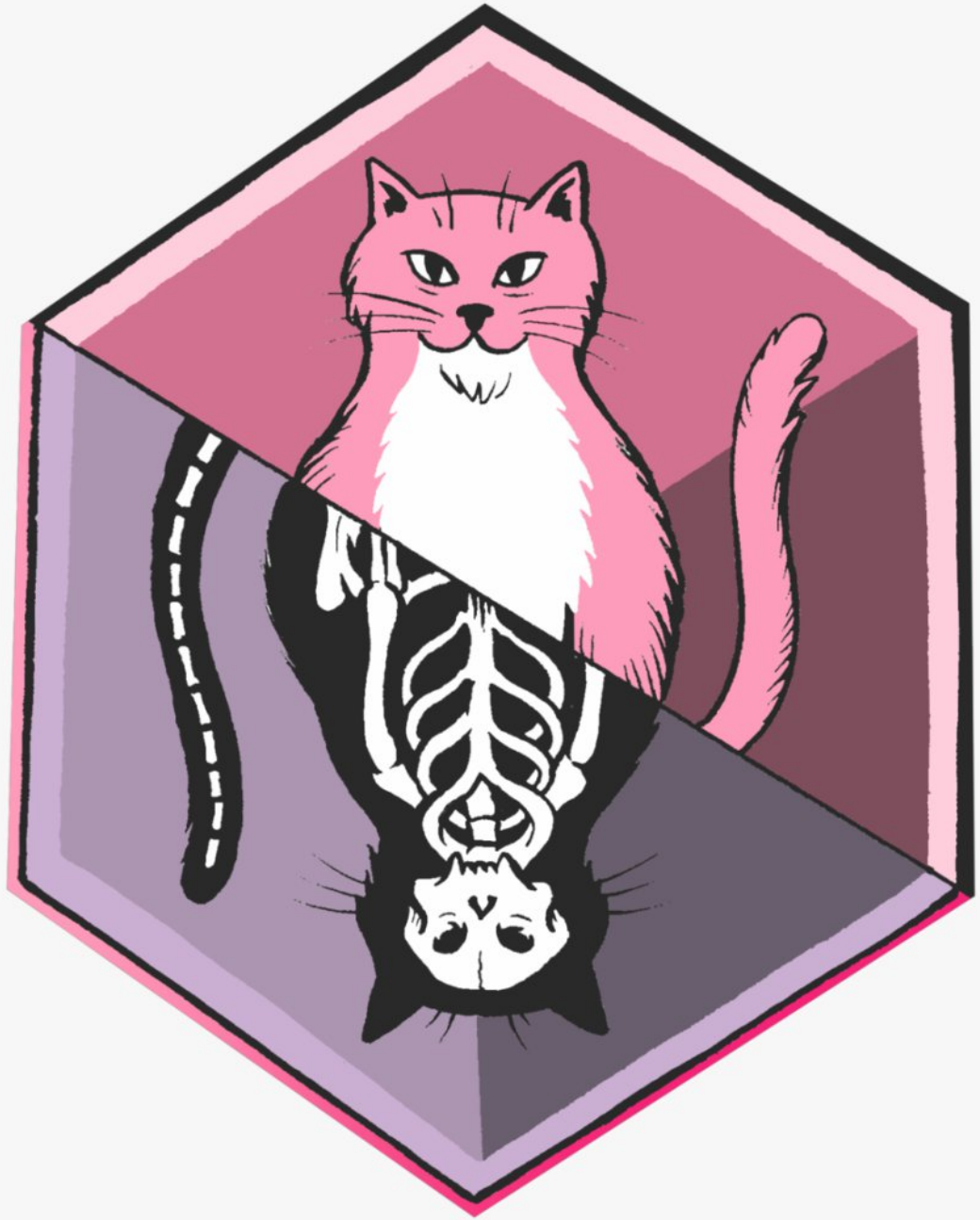
Вы заходите в антиспам систему на почтовом сервере и видите там более 1000 различных детектов за прошедшие сутки

Средний месячный показатель по вредоносным письмам – не более 100 в месяц

Кошелёк

ИНЦИДЕНТ № 2

УТЕЧКА ШРЁДИНГЕРА



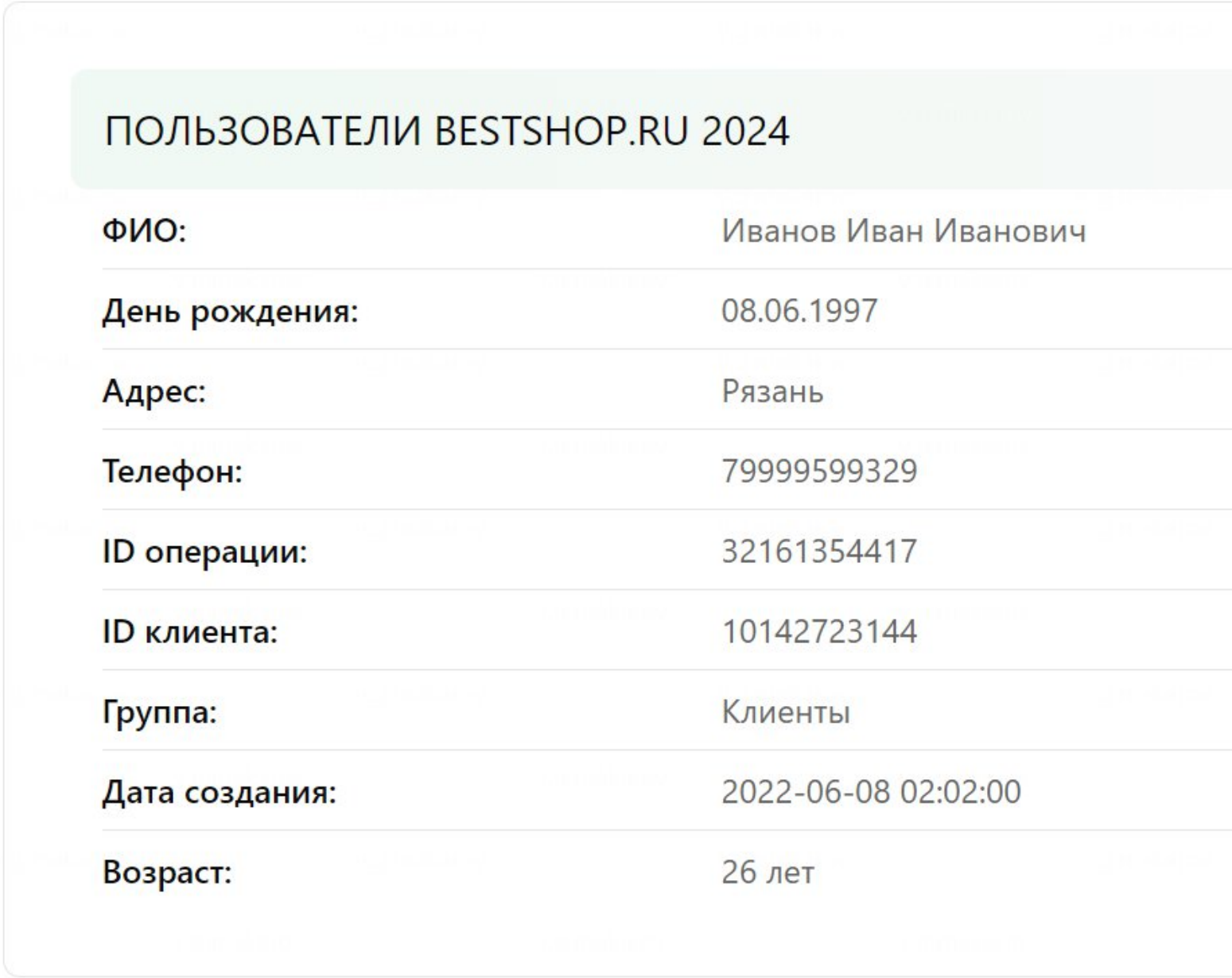
Кошелёк

Наша компания ООО «Интернет трейд»

- Компания e-commerce
- Штат 200+ человек
- Внедрена СУИБ
- Имеется отдел ИБ
- Внедрен процесс AppSec
- Сайт защищен WAF и от DDoS
- Ваш сайт bestshop.ru
- Ваш магазин имеет много маркетинговых акций с другими компаниями

Инцидент № 2

К вам приходит сотрудник и сообщает, что пытался «пробить» знакомую через «Глаз Бога» и там увидел:



ПОЛЬЗОВАТЕЛИ BESTSHOP.RU 2024

ФИО:	Иванов Иван Иванович
День рождения:	08.06.1997
Адрес:	Рязань
Телефон:	79999599329
ID операции:	32161354417
ID клиента:	10142723144
Группа:	Клиенты
Дата создания:	2022-06-08 02:02:00
Возраст:	26 лет

Какие риски несет инцидент?

РИСКИ:

1) Репутационные

2) Утечка ПДн

3) Финансовые

4) Судебные

5) Внимание регулятора

Наши действия?

Действия:

1) Проверить действительно ли была утечка по актуальным ID (Взломали ли наши системы?)

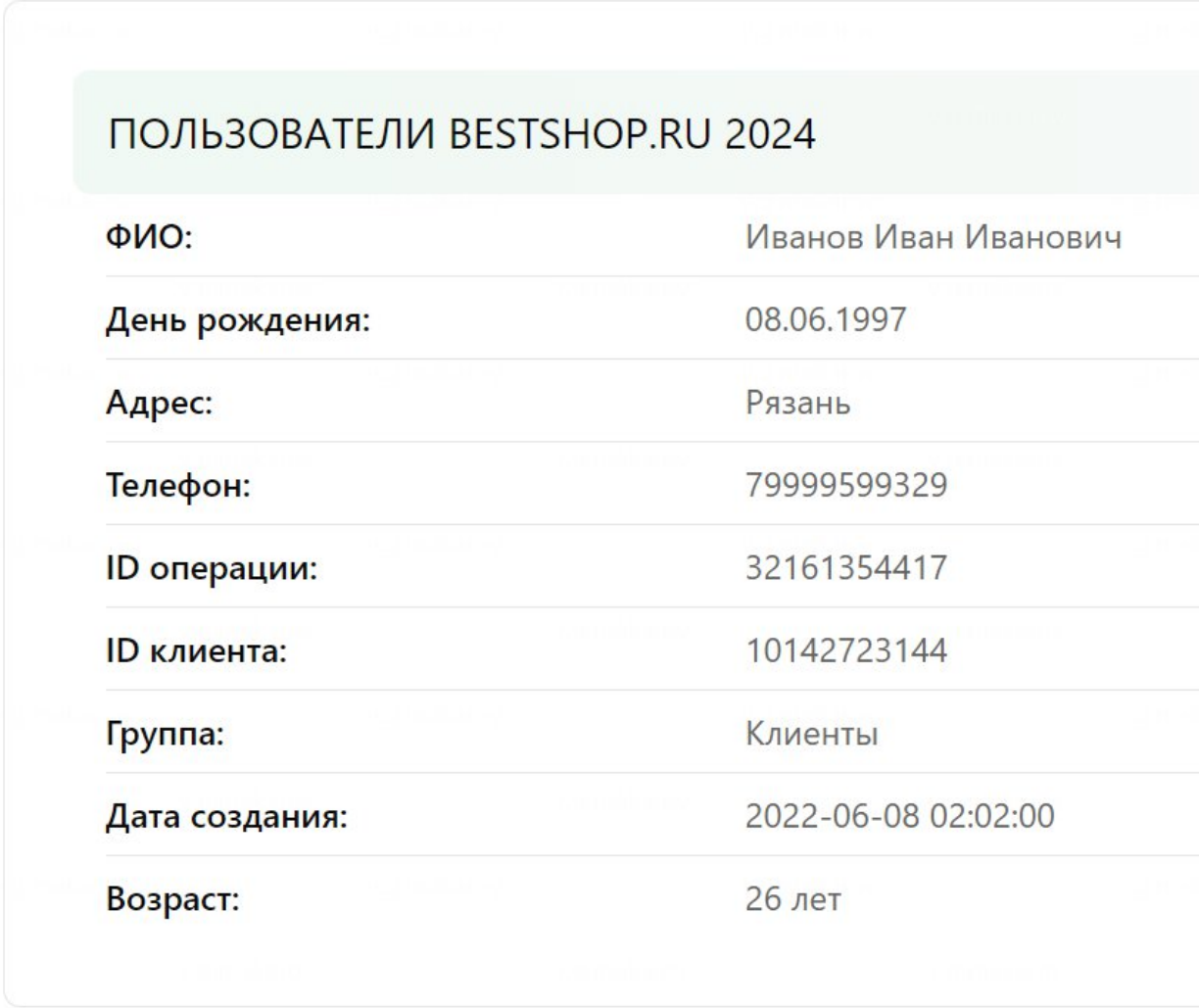
2) Опросили DATA-инженеров

3) Поднять все средства защиты

4) Сверить данные (названия полей, поля ID операции, код клиента)

5) Инициировать встречу с департаментом ИБ партнёра

6) Внести изменения в договор с партнёрами



ПОЛЬЗОВАТЕЛИ BESTSHOP.RU 2024

ФИО:	Иванов Иван Иванович
День рождения:	08.06.1997
Адрес:	Рязань
Телефон:	79999599329
ID операции:	32161354417
ID клиента:	10142723144
Группа:	Клиенты
Дата создания:	2022-06-08 02:02:00
Возраст:	26 лет

Попросив сотрудника выгрузить полный отчет «Глаза Бога» вы замечаете:

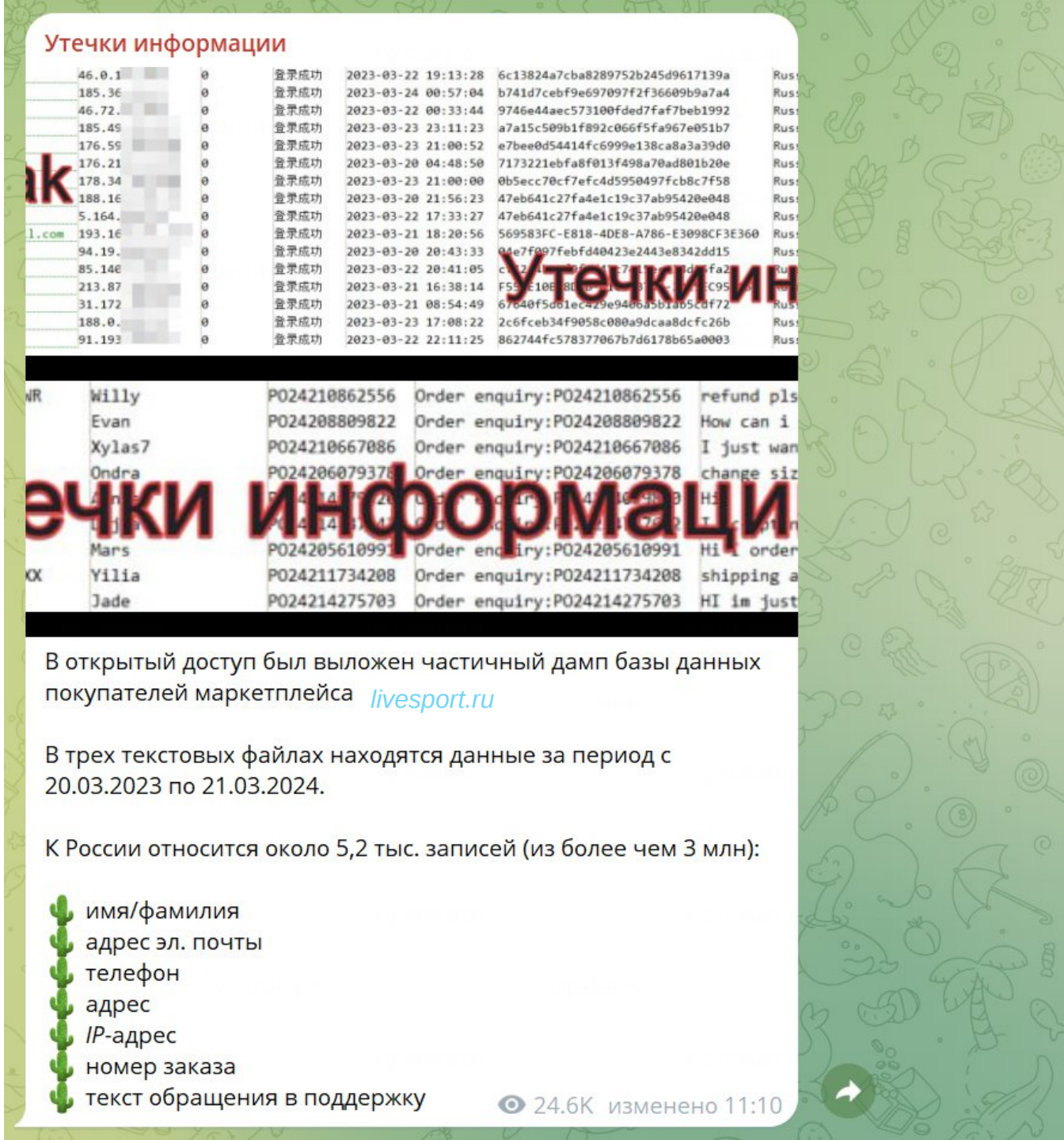
ПОЛЬЗОВАТЕЛИ BESTSHOP.RU 2024

ФИО:	Иванов Иван Иванович
День рождения:	08.06.1997
Адрес:	Рязань
Телефон:	79999599329
ID операции:	32161354417
ID клиента:	10142723144
Группа:	Клиенты
Дата создания:	2022-06-08 02:02:00
Возраст:	26 лет

ПОЛЬЗОВАТЕЛИ LIVESPORT.RU 2024

ФИО:	Иванов Иван Иванович
День рождения:	08.06.1997
Адрес:	Рязань
Телефон:	79999599329
ID операции:	32161354417
ID клиента:	10142723144
Группа:	Клиенты
Дата создания:	2022-06-08 02:02:00
Возраст:	26 лет

Проверив Telegram каналы с утечками вы узнаете что у партнера LiveSport совсем недавно была утечка клиентской базы



Кошелёк

ИНЦИДЕНТ № 3*

ВСЕ ПРОПАЛО МИХАЛЫЧ!

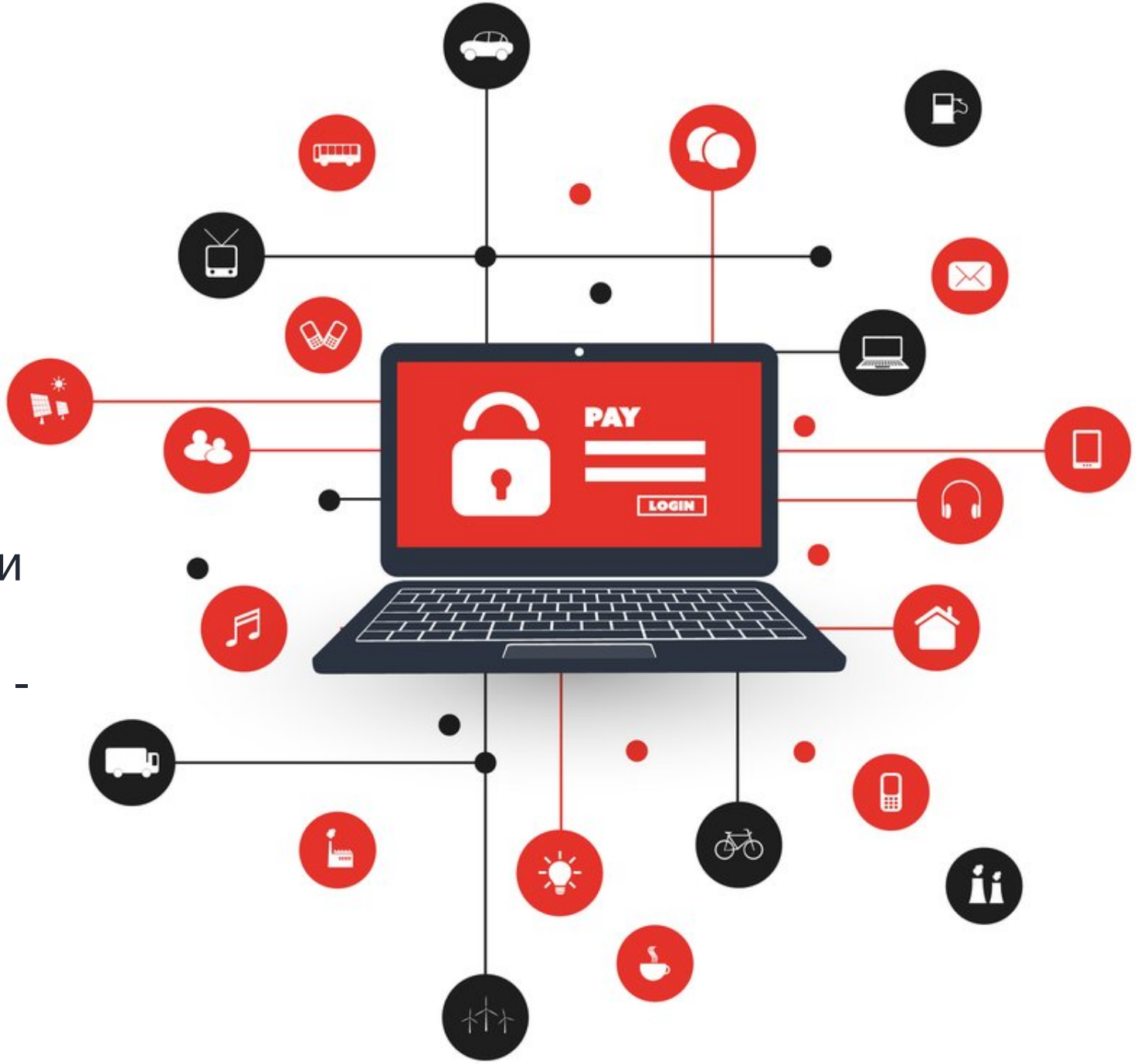
Кошелёк

Наша компания ООО «НеИнновация сервис»

- Компания оказывает аутсорсинг IT услуг
- Штат 150+ человек
- СУИБ не внедрена
- Нет отдела ИБ

Инцидент № 3*

Утро понедельника.
Вы приходите на работу и вдруг видите что вся Windows инфраструктура - зашифрована



Какие риски несет инцидент?

РИСКИ:

1) Целесообразность существования организации

2) Ущерб данных

3) Материальный ущерб

4) Ущерб инфраструктуры

5) Утечка данных

6) Репутационные

7) Угроза атаки на клиентов

8) Невозможность определения доступа к вашей инфраструктуре

Наши действия?

Действия:

1) Предупредить клиентов, оборвать сетевые связи
2) Проверить бэкапы
3) Наличие дешифратора
4) Попросить помощи у вендора
5) Сообщить в соответствующие органы об инциденте
6) Попытаться расшифровать
7) Поиск источника
8) Проверка бэкапов на то, что они не заражены
9) Сканирование на наличие маркеров компрометации
10) Восстановление с бэкапов 2,3 уровня (если они есть)

Макаров Владимир

Спасибо за внимание!