Михаил Серёгин

Руководитель центра информационной безопасности Университета Иннополис

- Обеспечение безопасности государственных информационных систем в период с 2011 по 2021 гг.
- С 2021 г. возглавляю ЦИБ Университета Иннополис. Специализация центра: пентесты, аудит ПДн / КИИ, расследование инцидентов, повышение осведомлённости, обучение сотрудников.
- Проведено более 50 обучающих курсов по ИБ

ЧТО МОЖЕТ ПОЙТИ НЕ ТАК?

РАЗБОР РЕАЛЬНЫХ ИНЦИДЕНТОВ ПОСЛЕДНИХ ЛЕТ

Случай 1: звонок

Вводные:

- Время действия – до распространения телефонных мошенников
- Крупная компания с широкой сетью филиалов
- По ИБ – всё хорошо
- Недавно был сменён основной банк
- Сотруднице бухгалтерии поступает звонок…

Случай 1: звонок

Выводы:

- Классика соц. инженерии про «самое слабое место любой системы»
- Повод задуматься: а как у нас дела с этим? Сотрудники хотя бы знают про фишинг, вишинг, квишинг и пр.?

Случай 2: фин. организация

Вводные:

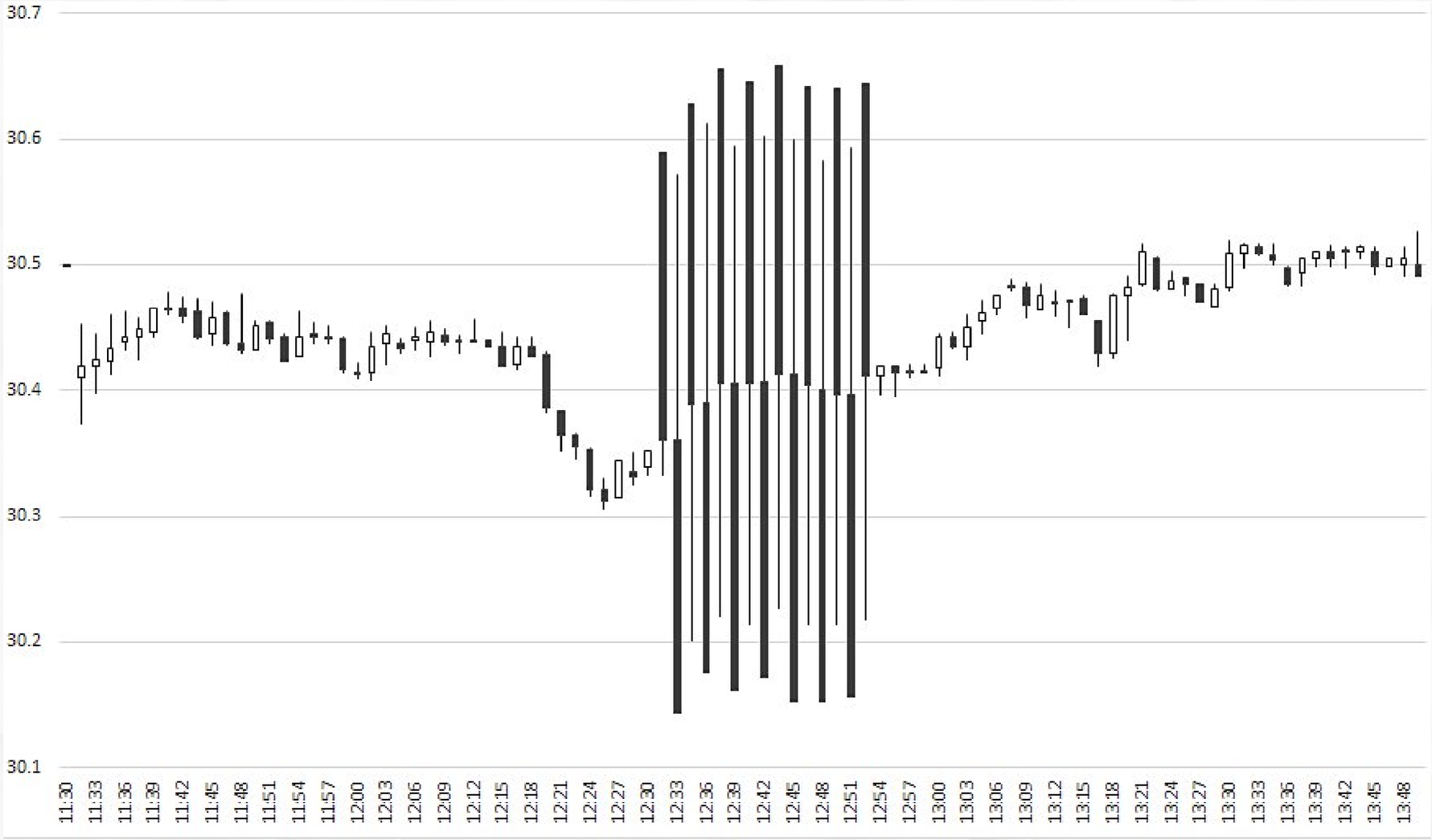
- Финансовая организация, имеющая все лицензии, и прошедшая аудиты
- По практической ИБ – всё не очень
- Есть сотрудник, отвечающий за торговлю на бирже
- Время действия ≈ 2016

Случай 2: фин. организация

Короткая викторина:

- Операционная система: Windows XP
- Права сотрудника: Администраторские
- Браузер: IE
- Токен цифровой подписи: Не вынимался
- Антивирус: Обновлён

Случай 2: фин. организация



Случай 2: фин. организация

Выводы:

- Орг. меры и прочие атрибуты «бумажной» безопасности – это хорошо, но про практическую забывать не стоит

Случай 3: пост в Интернете

[redacted] Russian Defense Contractor | Classified Docs + Logins | ATW | Part 1

by [redacted] - January 19, 2022 at 08:23 AM

Pages (3): 1 2 3 Next »

GOD User

GOD

Posts	339
Threads	112
Joined	Oct 2021
Reputation	2,892

January 19, 2022 at 08:23 AM This post was last modified: January 19, 2022 at 03:10 PM by AgainstTheWest. Edited 1 time in total. *Edit Reason: Adc*
Mirror

Operation Ruble

[redacted]

Hello all, ATW here again.
In light of the recent attacks on the country of Ukraine by pro-Russian groups, we'll be returning the fa
On top of this, as soon as we posted the old version, we received several death threats to take it down
took it down. We're now releasing all the data.
BTFO

Today, we are releasing a large collection of internal files from the following companies / state-owned

[redacted] Russian Defense Contractor | Classified Docs + Logins | ATW | Part 2

by Asuna - January 19, 2022 at 08:37 PM

~~Asuna~~

CCP Leader

Posts	434
Threads	76
Joined	Jan 2021
Reputation	1,762

1 YEAR OF SERVICE

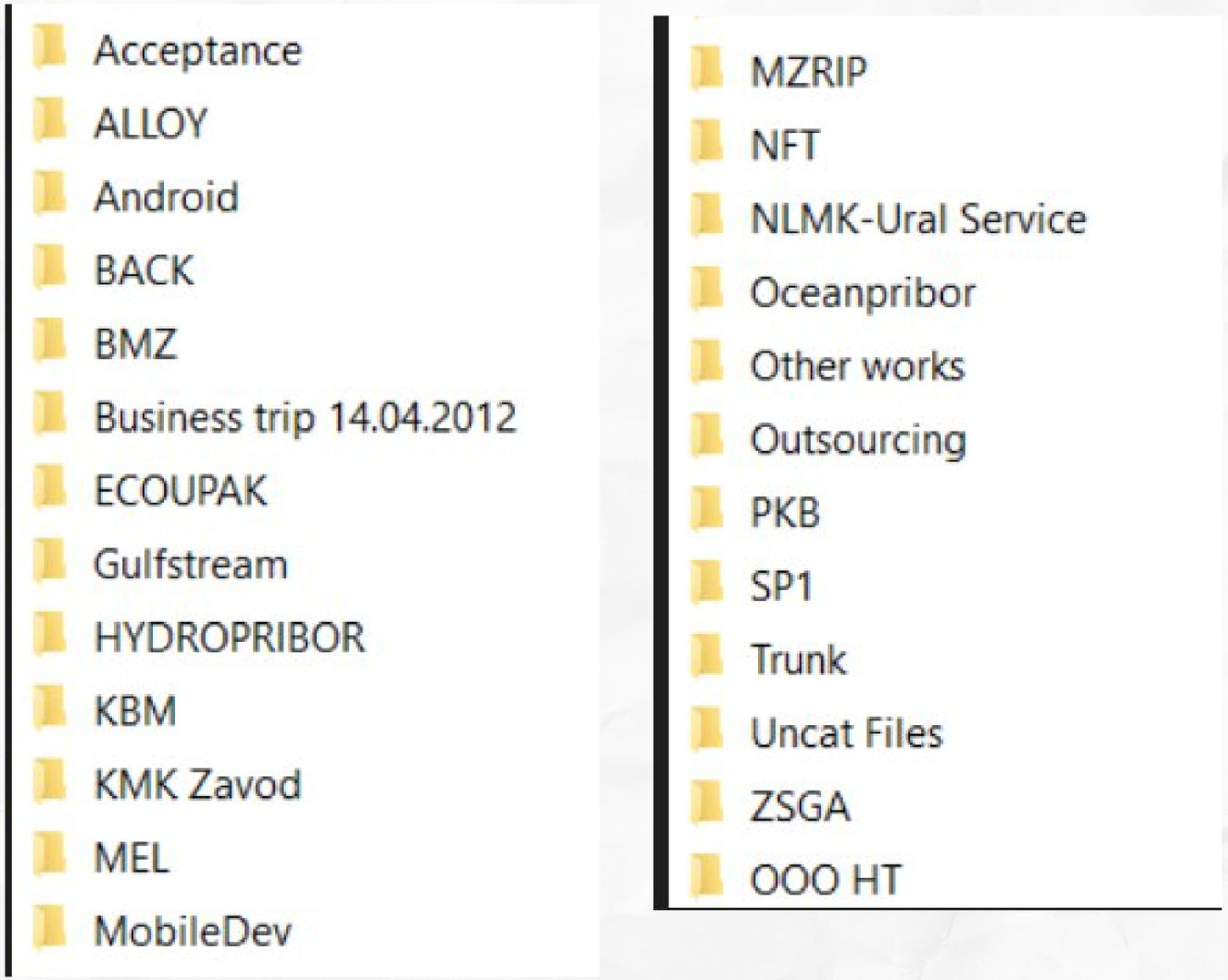
January 19, 2022 at 08:37 PM

Operation Ruble

[redacted]

Hello all ^_^
Asuna with ATW here. Today, we're releasing the 2nd part to the Russian defense contrac
Please refer back to the first part for information on the companies / agencies exposed i
Link

- NPO Splav - https://en.wikipedia.org/wiki/NPO_Splav
- Novolipetsk Steel - https://en.wikipedia.org/wiki/Novolipetsk_Steel
- NPO Mashinostroyeniya - https://en.wikipedia.org/wiki/NPO_Mashinostroyeniya
- Oceanpribor - https://loexpo.crplo.ru/en/machinery/oceanpribor
- Murom Plant of Radio Metering Equipment
- KB Mashinostroyeniya - https://en.wikipedia.org/wiki/KB_Mashinostroyeniya
- HYDROPRIBOR - https://www.altusintel.com/public-yy4xg5/
- [redacted] Mechanical Plant - https://b[redacted]/?lang=e
- GULFSTREAM - https://gulfstream-mnp.ru/


Acceptance
ALLOY
Android
BACK
BMZ
Business trip 14.04.2012
ECOUPAK
Gulfstream
HYDROPRIBOR
KBM
KMK Zavod
MEL
MobileDev
MZRIP
NFT
NLMK-Ural Service
Oceanpribor
Other works
Outsourcing
PKB
SP1
Trunk
Uncat Files
ZSGA
OOO HT

[redacted] для возможности ее работы с [redacted]

11/01/2019 05:34 pm - Ольга Капарулина

Status:	Закрыта	**Start date:**	11/01/2019
Priority:	Нормальный	**Due date:**	11/08/2019
Assignee:	Григорий Буйко	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:		**Spent time:**	8.00 hours
Ревизия SVN:		**Вид задачи:**	Разработка
Вопрос в QT:			

Description

ГОЛЬФСТРИМ в опытной эксплуатации на [redacted]
У них используется ЛОЦМАН 2018 SP1.
Необходимо пропатчить БД ЛОЦМАН для возможности ее работы с текущей версией ГОЛЬФСТРИМ.

Ссылка на базу: https://cloud.mail.ru/public/5i7P/4rcAwmE4m

History

#1 - 11/13/2019 12:46 pm - Илья Хармац

- Project changed from Прочие работы to [redacted]

#2 - 12/17/2019 01:20 pm - Григорий Буйко

- Status changed from Новая to Выполнена

- Assignee changed from Григорий Буйко to Илья Хармац

- % Done changed from 0 to 100

#3 - 01/10/2020 08:49 am - Илья Хармац

- Status changed from Выполнена to Закрыта

- Assignee changed from Илья Хармац to Григорий Буйко

[redacted] для возможности ее работы с [redacted]

11/01/2019 05:34 pm - Ольга Капарулина

Status:	Закрыта	**Start date:**	11/01/2019
Priority:	Нормальный	**Due date:**	11/08/2019
Assignee:	Григорий Буйко	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:		**Spent time:**	8.00 hours
Ревизия SVN:		**Вид задачи:**	Разработка
Вопрос в QT:			

Description

ГОЛЬФСТРИМ в опытной эксплуатации на [redacted]
У них используется ЛОЦМАН 2018 SP1.
Необходимо пропатчить БД ЛОЦМАН для возможности ее работы с тек

Ссылка на базу: https://cloud.mail.ru/public/5i7P/4rcAwmE4m

Ссылка на базу: https://cloud.mail.ru/public/5i7P/4rcAwmE4m

History

#1 - 11/13/2019 12:46 pm - Илья Хармац

- Project changed from Прочие работы to [redacted]

#2 - 12/17/2019 01:20 pm - Григорий Буйко

- Status changed from Новая to Выполнена

- Assignee changed from Григорий Буйко to Илья Хармац

- % Done changed from 0 to 100

#3 - 01/10/2020 08:49 am - Илья Хармац

- Status changed from Выполнена to Закрыта

- Assignee changed from Илья Хармац to Григорий Буйко

DC8044 F33d

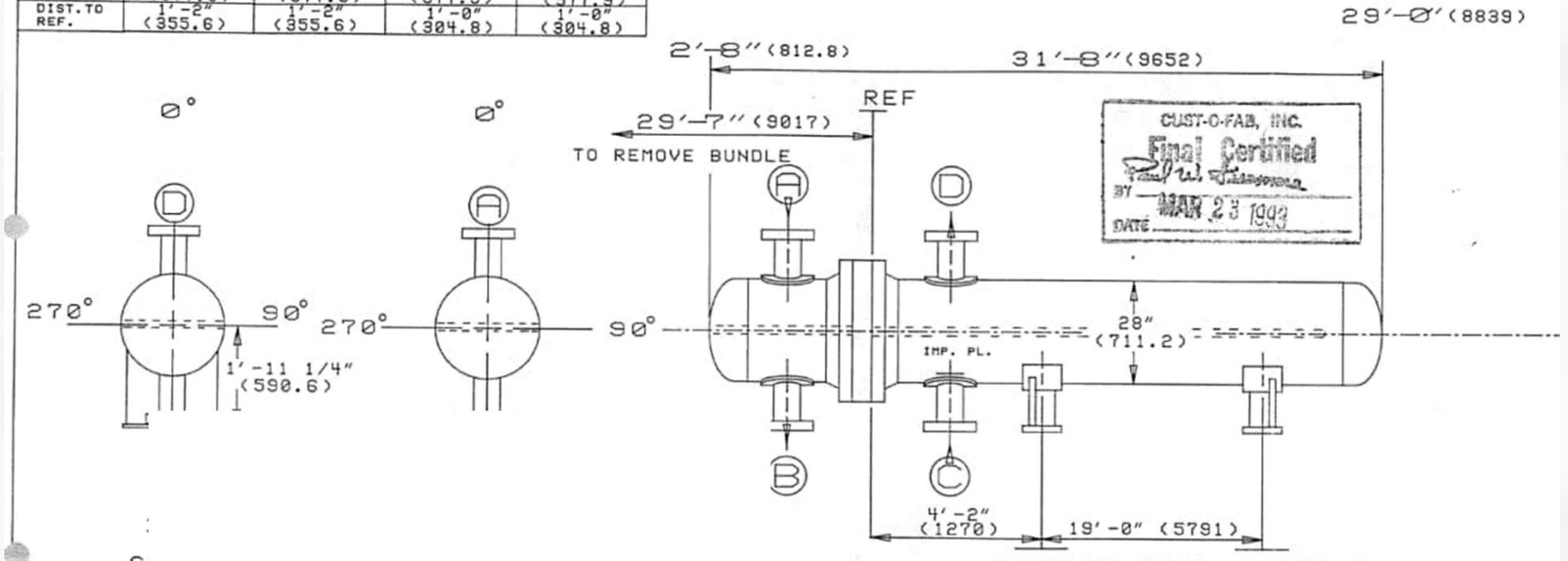
В продолжение темы слива [redacted] (российский концерн, объединяющий предприятия, разрабатывающие и выпускающие вооружения для противовоздушной обороны и противоракетной обороны), который хакеры недавно опубликовали на площадке Рейдфорумс.

Наши камунити мемберы решили провести исследование и проанализировали файлы из опубликованного на Рейдфорумс архива (прежде всего, заинтересовали дампы тикетов Редмайна). В результате исследования обнаружены несколько ссылок на некий диск мейл.ру, где был размещен в открытом доступе (!) архив с файликом. Посмотрев этот файлик, наши кибер-космобольцы обнаружили бекап базы mssql, с примерным размером 67ГБ. В обнаруженной базе, кроме прочего, находилась табличка, в которой лежали блобы с файлами.

Написав за пару часов парсер и заполучив файлики, исследователи обнаружили ТЫСЯЧИ всевозможных чертежей, относящихся к заводам по нефтепереработке, военно-промышленному комплексу, скан-копии служебных документов с подписями и много много другой занимательной информации, контакты сотрудников крупных предприятий, спецификации закупок и черт ногу сломит что еще. Энтузиасты структурировали обнаруженную информацию и предоставляют в удобочитаемом виде.

MARK	A	B	C	D
FLOW	INLET	OUTLET	INLET	OUTLET
SIZE	8" 300	8" 300	8" 300	8" 300
FACING	RF WN	RF WN	RF WN	RF WN
AUX. CONN.				
PROJ. FROM CTR. LINE	1'-10 3/4" (577.9)	1'-10 3/4" (577.9)	1'-10 3/4" (577.9)	1'-10 3/4" (577.9)
DIST. TO REF.	1'-2" (355.6)	1'-2" (355.6)	1'-0" (304.8)	1'-0" (304.8)

NUMBERS IN PARENTHESES ARE MILLIMETERS, UNLESS NOTED.



CUST-O-FAB, INC.
Final Certified
BY
DATE MAR 23 1993

S

ESTIMATED
DRY 15600.
WET 23400.
BUNDLE 8200.

REV	DATE	DESCRIPTION
2	12/8/92	REV.
1	11/6/92	REV.

REVISIONS

GASKET MAT'L DJCHRMNAF
1 SPARE SET GASKETS

PRESSURE AT 100 Deg. F. (-18.8 C)

2-7/8" (22.2) DIA. HOLES
2-7/8" (22.2) X 1 3/4" (SLOTS

FABRICATION REQUIREMENTS	
TEMA CLASS R	
ASME CODE SECTION VIII DIV. ONE, ADDENDA '91	
ASME CODE STAMP IS	REQUIRED
NATIONAL BOARD NO. IS	REQUIRED

HEAT TREAT: CHAN

SPOT XRAY SHELL
FULL XRAY CHANNEL

SEE PAGE 2 FOR PAINTING INSTRUCTIONS.

ALL BOLTHLS. TO STRD'L QS.

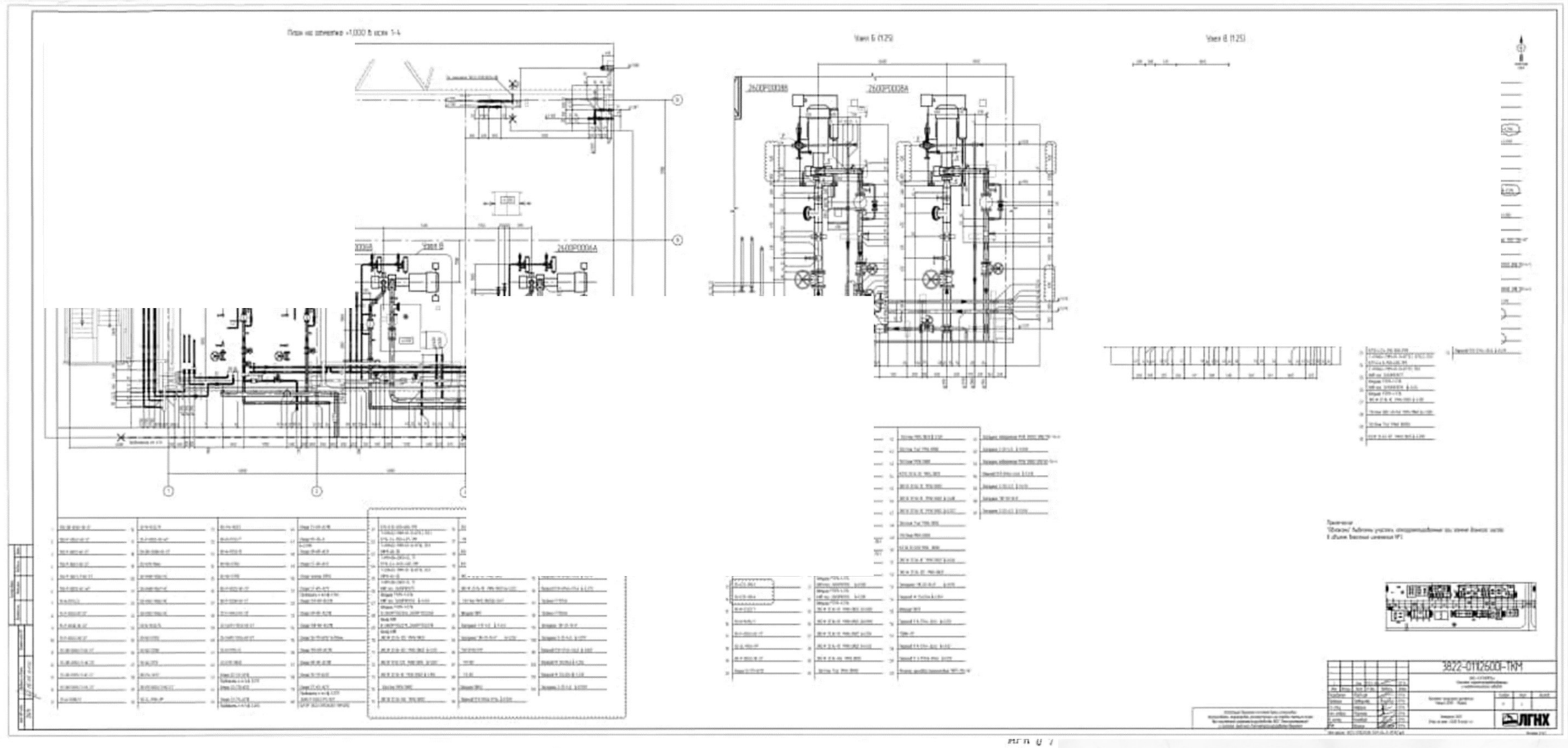
CUST-O-FAB,
SAND SPRINGS, OKL

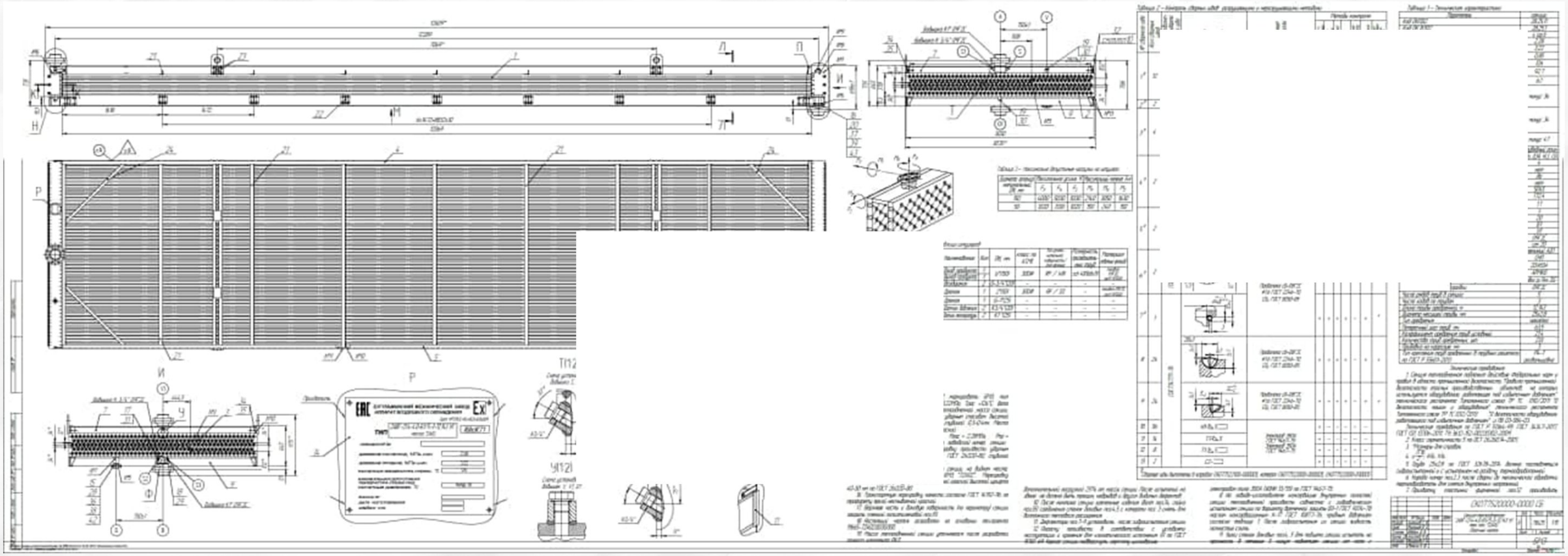
CUSTOMER: PETROFAC, INC
P.O. NO: 20157-0568

SCALE: NONE	DIMENSIONAL OUTLINE	DRAW
DATE: 10/13/92		CHEC

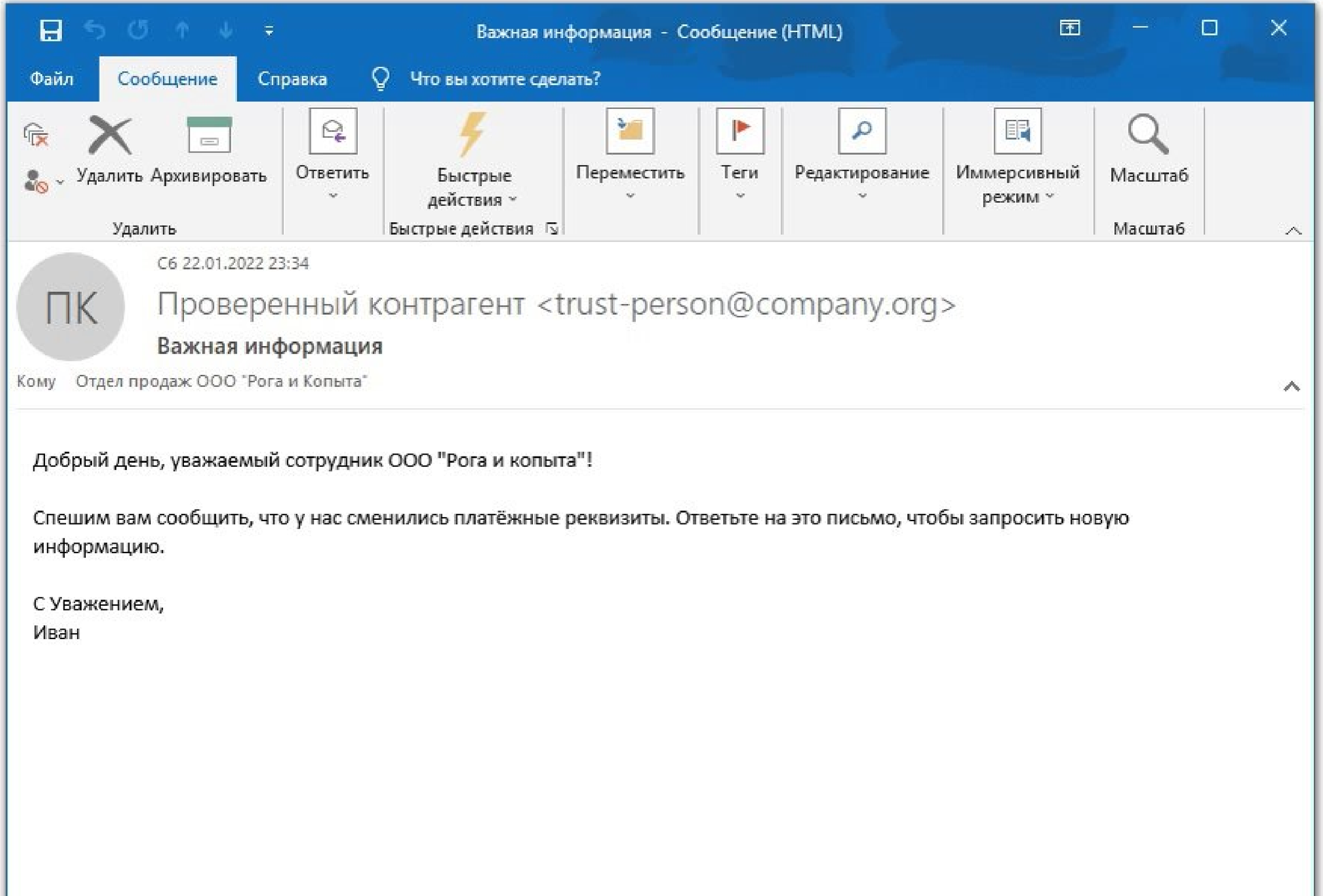
TAG NO: E-201
SERVICE: REFORMER FEED / EFFL. EXC
SIZE: 27-336 BFU (685.8-8534.4)
DWG. NO. 92-673

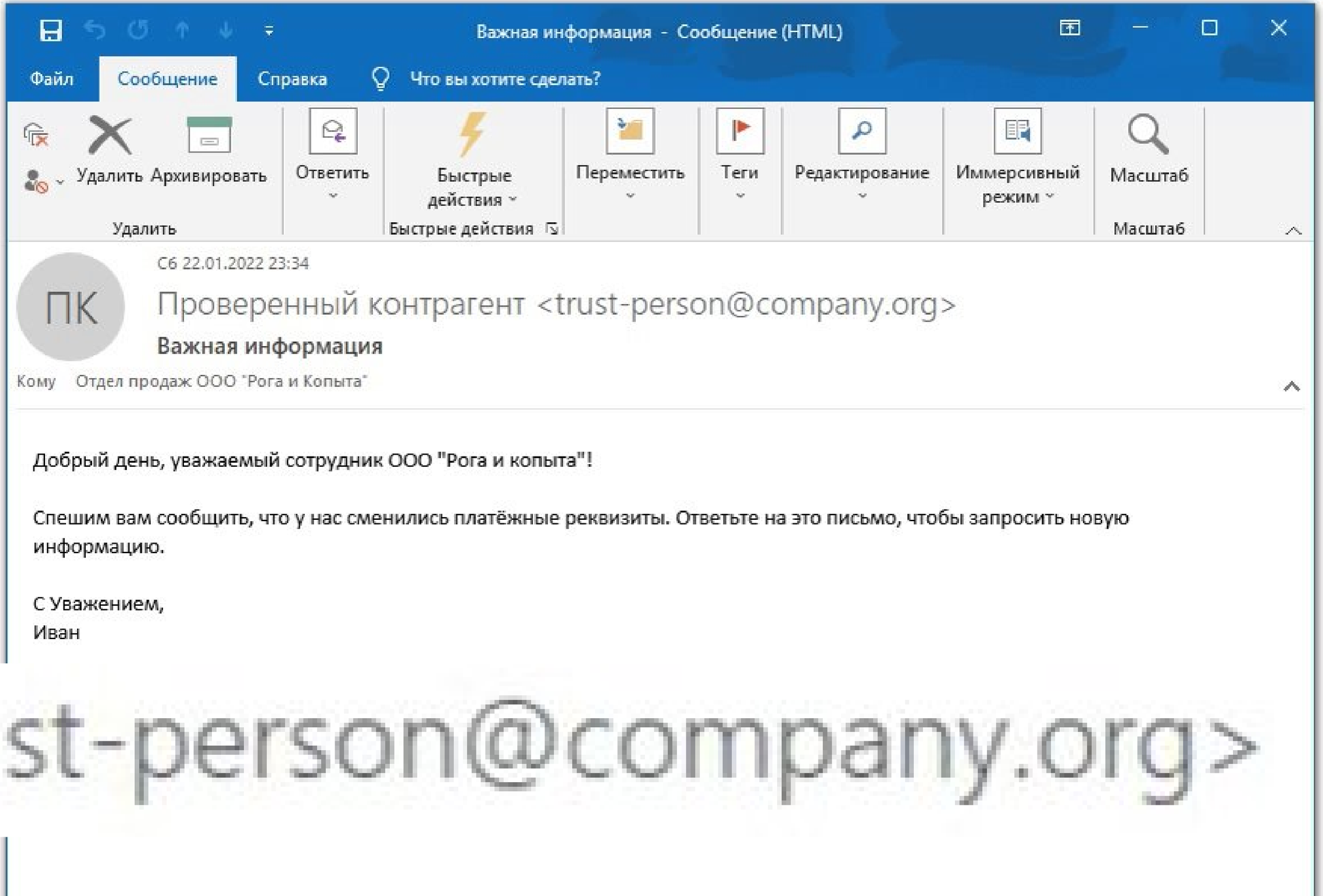
APR 0 7


План на отметке +1,000 В. оси 1-4
Узел 5 (1:25)
Узел 6 (1:25)
2600P1008B
2600P1008A
2600P1006A
Примечания
3822-01102600-ТКМ

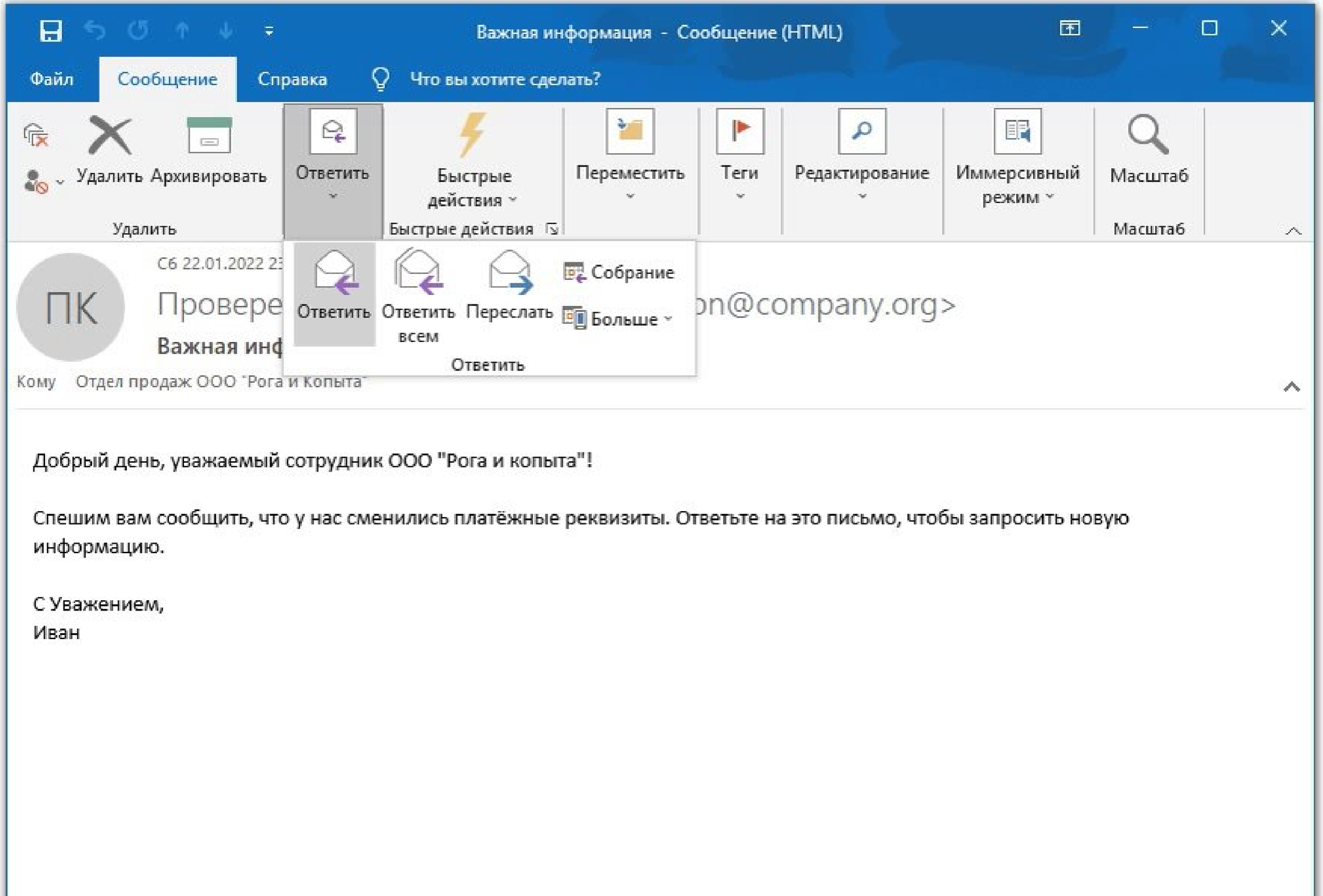


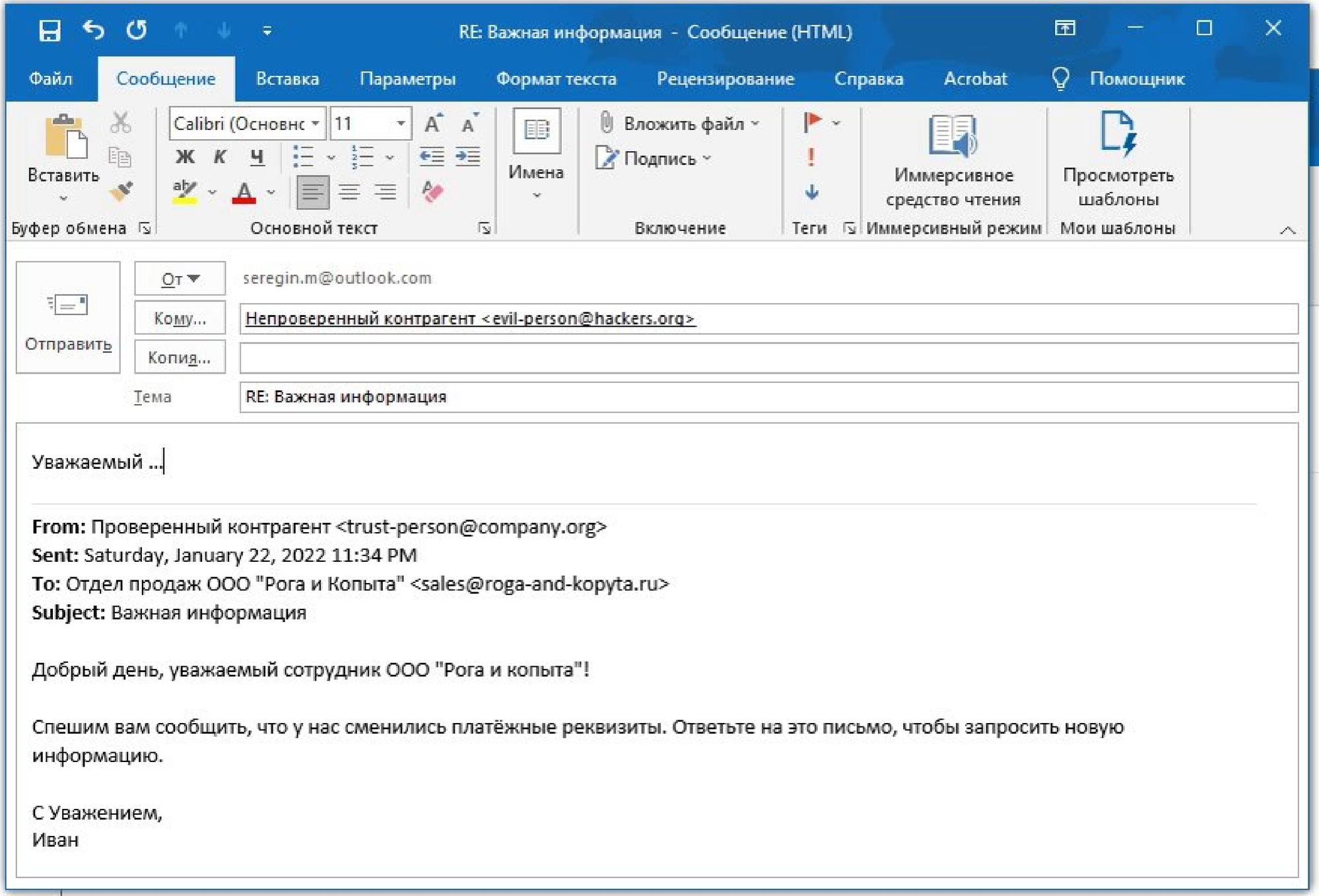
Случай 4: простой почтовый ящик

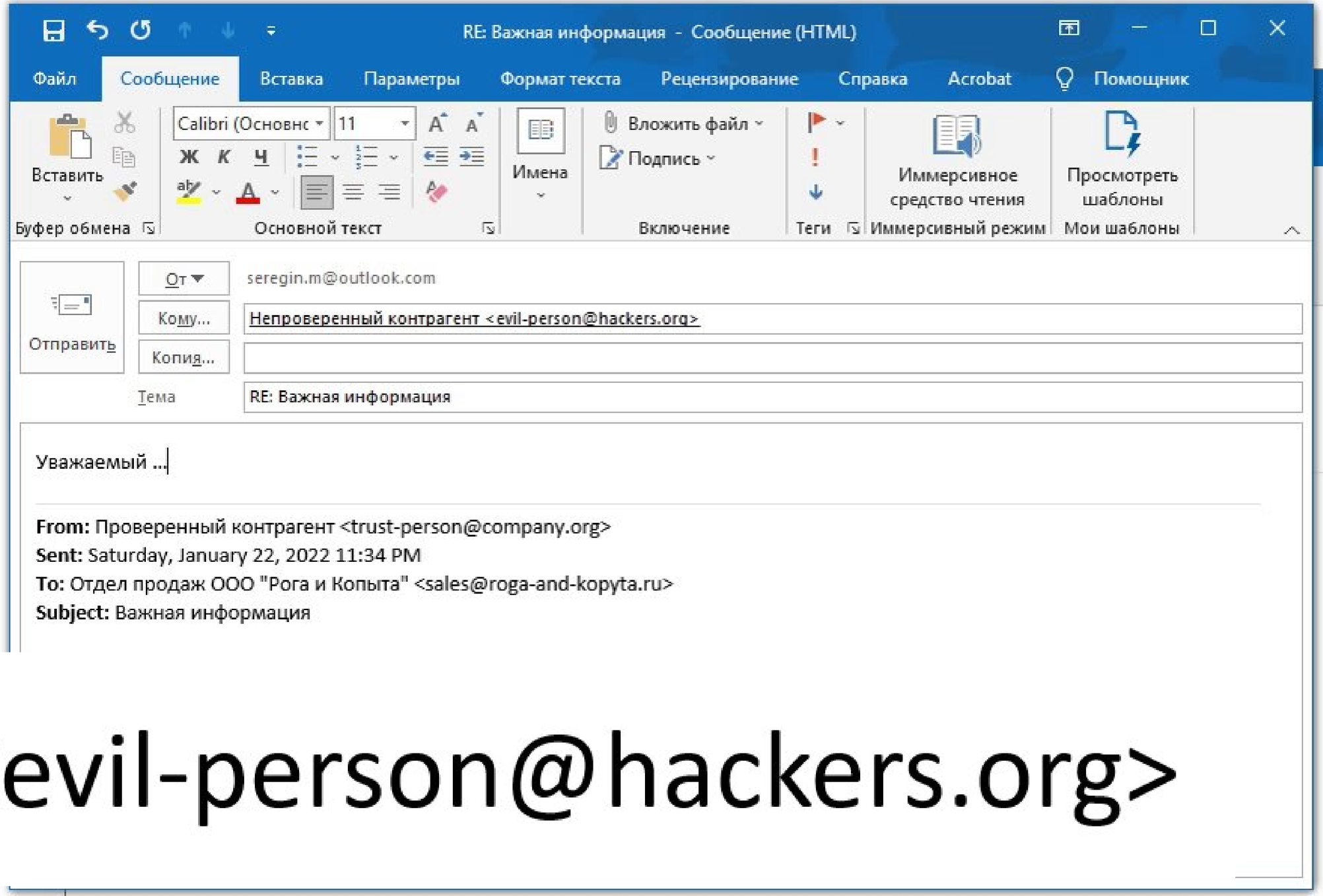

Важная информация - Сообщение (HTML)
Файл
Сообщение
Справка
Что вы хотите сделать?
Удалить
Архивировать
Ответить
Быстрые действия
Переместить
Теги
Редактирование
Иммерсивный режим
Масштаб
Удалить
Быстрые действия
Масштаб
ПК
Сб 22.01.2022 23:34
Проверенный контрагент <trust-person@company.org>
Важная информация
Кому Отдел продаж ООО "Рога и Копыта"
Добрый день, уважаемый сотрудник ООО "Рога и копыта"!
Спешим вам сообщить, что у нас сменились платёжные реквизиты. Ответьте на это письмо, чтобы запросить новую информацию.
С Уважением,
Иван



<trust-person@company.org>


Важная информация - Сообщение (HTML)
Файл
Сообщение
Справка
Что вы хотите сделать?
Удалить
Архивировать
Ответить
Быстрые действия
Переместить
Теги
Редактирование
Иммерсивный режим
Масштаб
Удалить
Быстрые действия
Масштаб
Ответить
Ответить всем
Переслать
Собрание
Больше
Ответить
ПК
Кому
Отдел продаж ООО "Рога и Копыта"
Добрый день, уважаемый сотрудник ООО "Рога и копыта"!
Спешим вам сообщить, что у нас сменились платёжные реквизиты. Ответьте на это письмо, чтобы запросить новую информацию.
С Уважением,
Иван


RE: Важная информация - Сообщение (HTML)
Файл
Сообщение
Вставка
Параметры
Формат текста
Рецензирование
Справка
Acrobat
Помощник
Вставить
Буфер обмена
Calibri (Основнс
11
Основной текст
Имена
Вложить файл
Подпись
Включение
Теги
Иммерсивное средство чтения
Иммерсивный режим
Просмотреть шаблоны
Мои шаблоны
Отправить
От
seregin.m@outlook.com
Кому...
Непроверенный контрагент <evil-person@hackers.org>
Копия...
Тема
RE: Важная информация
Уважаемый ...
From: Проверенный контрагент <trust-person@company.org>
Sent: Saturday, January 22, 2022 11:34 PM
To: Отдел продаж ООО "Рога и Копыта" <sales@roga-and-kopyta.ru>
Subject: Важная информация
Добрый день, уважаемый сотрудник ООО "Рога и копыта"!
Спешим вам сообщить, что у нас сменились платёжные реквизиты. Ответьте на это письмо, чтобы запросить новую информацию.
С Уважением,
Иван



<evil-person@hackers.org>

Общие выводы

Общие выводы

- Тренируйте персонал (повышение осведомлённости – хорошая внутренняя отчётность и «подсвет» ИБ для руководства)
- Тренируйте себя (киберполигоны – это хорошо)
- Не пренебрегайте подрядными организациями – в одиночку всё делать тяжело

Готов ответить
на ваши вопросы

E-mail:
m.seregin@innopolis.ru
t.me/m_seregin