

ИСПДн или ГИС? и другие актуальные вопросы защиты информации

Андрей Березов

Руководитель департамента защиты информации

ООО «Информационный центр»

(423) 240-48-66 доб. 401

and@ic-dv.ru

Законопроект ID: 01/05/02- 16/00046644

- из-за размытости определения «государственная информационная система» многие государственные органы отказывались признавать свои системы ГИС и, соответственно, организовывать защиту информации по приказу ФСТЭК № 17;
- законопроект разработан ФСТЭК и призван устранить это недоразумение.

Основные мысли из пояснительной записки к законопроекту:

- на данный момент зарегистрировано 339 федеральных ГИС и около 1200 региональных, это очень мало;
- проблема заключается не в том, что системы не относят к государственным, а в том что их владельцы не проектируют и не реализуют систему защиты информации;

Основные мысли из пояснительной записки к законопроекту:

- кроме этого, государственные органы и госкорпорации зачастую поручают обработку конфиденциальной информации коммерческим центрам обработки данных, в которых не реализуется или реализована не в соответствии с требованиями ФСТЭК система защиты информации;

Основные мысли из пояснительной записки к законопроекту:

- как результат – в 80% информационных систем возможна реализация угроз нарушителями, не обладающими какими-либо специальными средствами и знаниями;
- соответственно к защите информации в госорганах, госкорпорациях и организациях, обрабатывающих ГИР должны быть единые требования.

Законопроект ID: 01/05/02- 16/00046644

Ожидалось, что ФСТЭК изменит определение «ГИС», но регулятор решил сделать по-другому: унифицировать требования для ГИС, ИС гос органов, ИС госкорпораций и ИС коммерческих организаций, обрабатывающих государственный информационный ресурс.

Законопроект ID: 01/05/02- 16/00046644

Вносит в 149-ФЗ обязанность операторов ИС:

- назначать лиц, ответственных за защиту информации;
- издавать внутренние документы по защите информации;
- планировать разработку, внедрение поддержание и совершенствование мер защиты информации;
- осуществление внутреннего контроля;
- ознакомление работников с документами по ЗИ;
- **информирование ФСТЭК и ФСБ об инцидентах информационной безопасности.**


Информирование сотрудников

- рядовые сотрудники являются неотъемлемым звеном процессов ИБ;
- большинство всех заражений вредоносным ПО осуществляется по каналам электронной почты;
- сотрудники не осведомлены об уязвимостях почтового протокола и о методах социальной инженерии.

Отправка фальшивого e-mail с помощью PHP-функции mail()

```
$headers = 'From: Федеральная налоговая  
служба <no-reply@nalog.ru>' . "\r\n" .  
        'Reply-To: no-reply@nalog.ru' .  
        "\r\n";  
mail($to, $subject, $message, $headers);  
  
$headers = 'From: Google <no-  
reply@accounts.google.com>' . "\r\n" .  
        'Reply-To: no-  
reply@accounts.google.com' . "\r\n";  
mail($to, $subject, $message, $headers);
```

Отправка фальшивого e-mail с общедоступного сервиса


 We will never ever send you junk email, or give your email address away to anyone. We hate spam at least as much as you do - maybe more (and that's why this page can't be used by spammers to send bulk email or any other funny stuff).

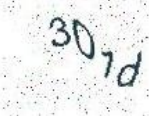
To:

From:

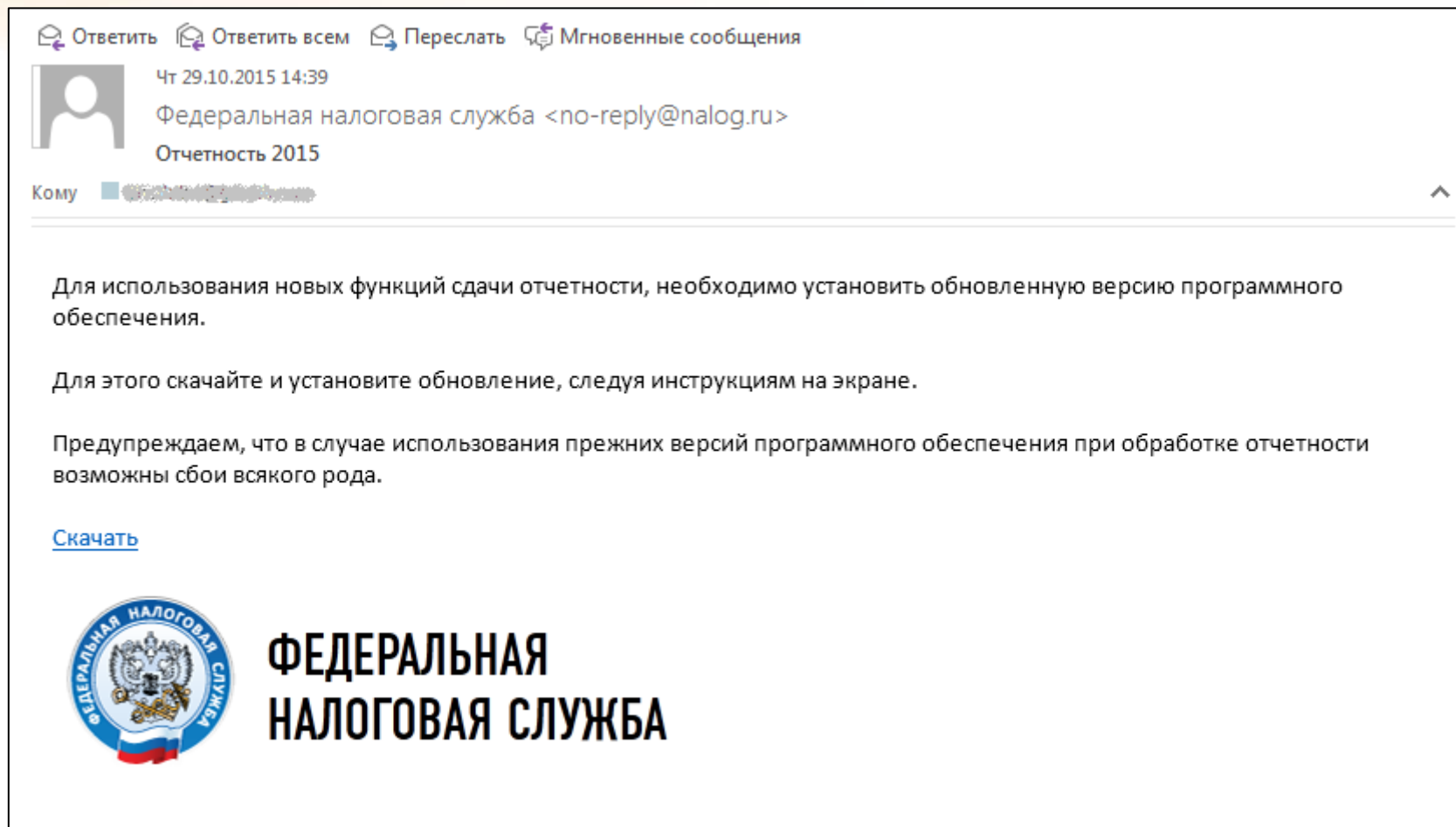
Subject:

Message:

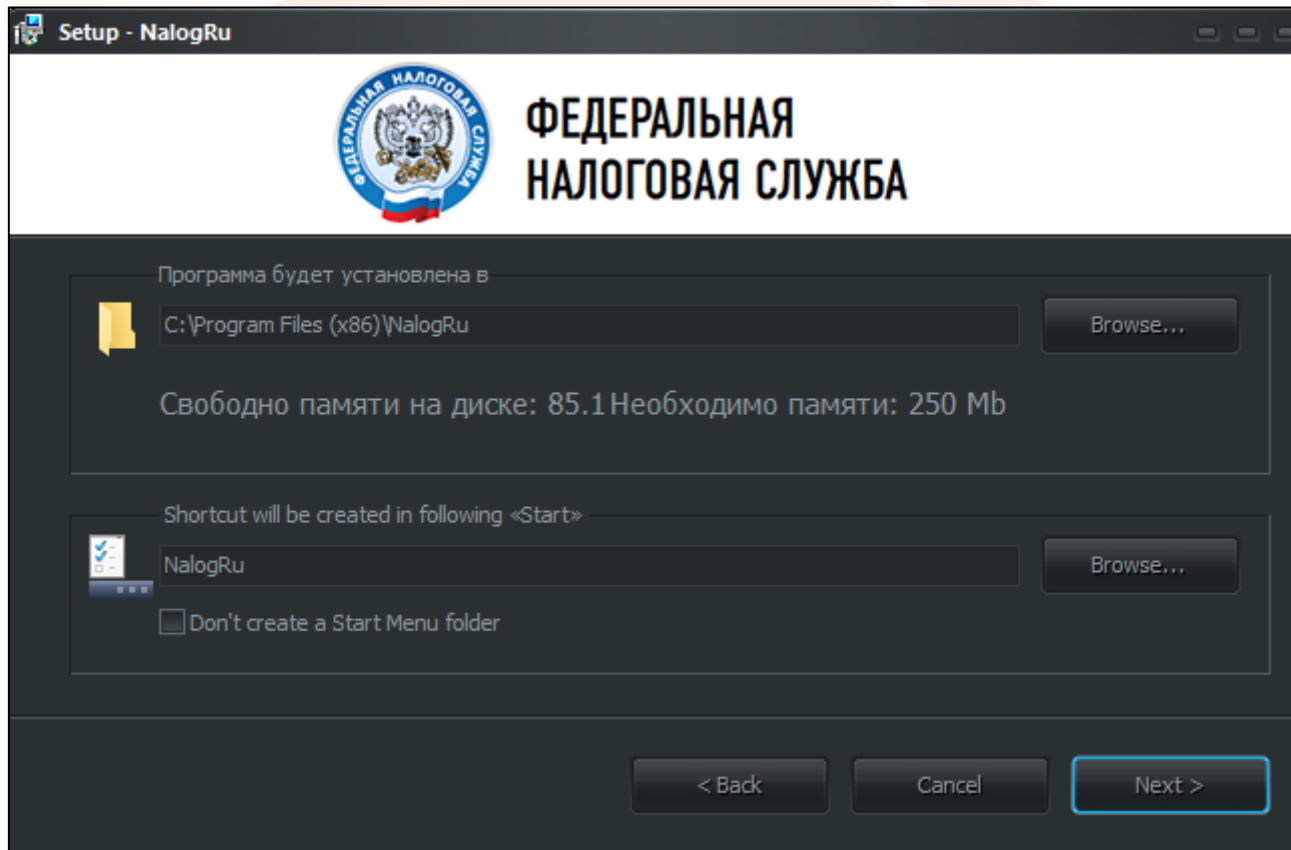


Security:  Please enter the code in the box to the left ([why?](#))

Пример фишингового письма



Установка троянского ПО «от налоговой»

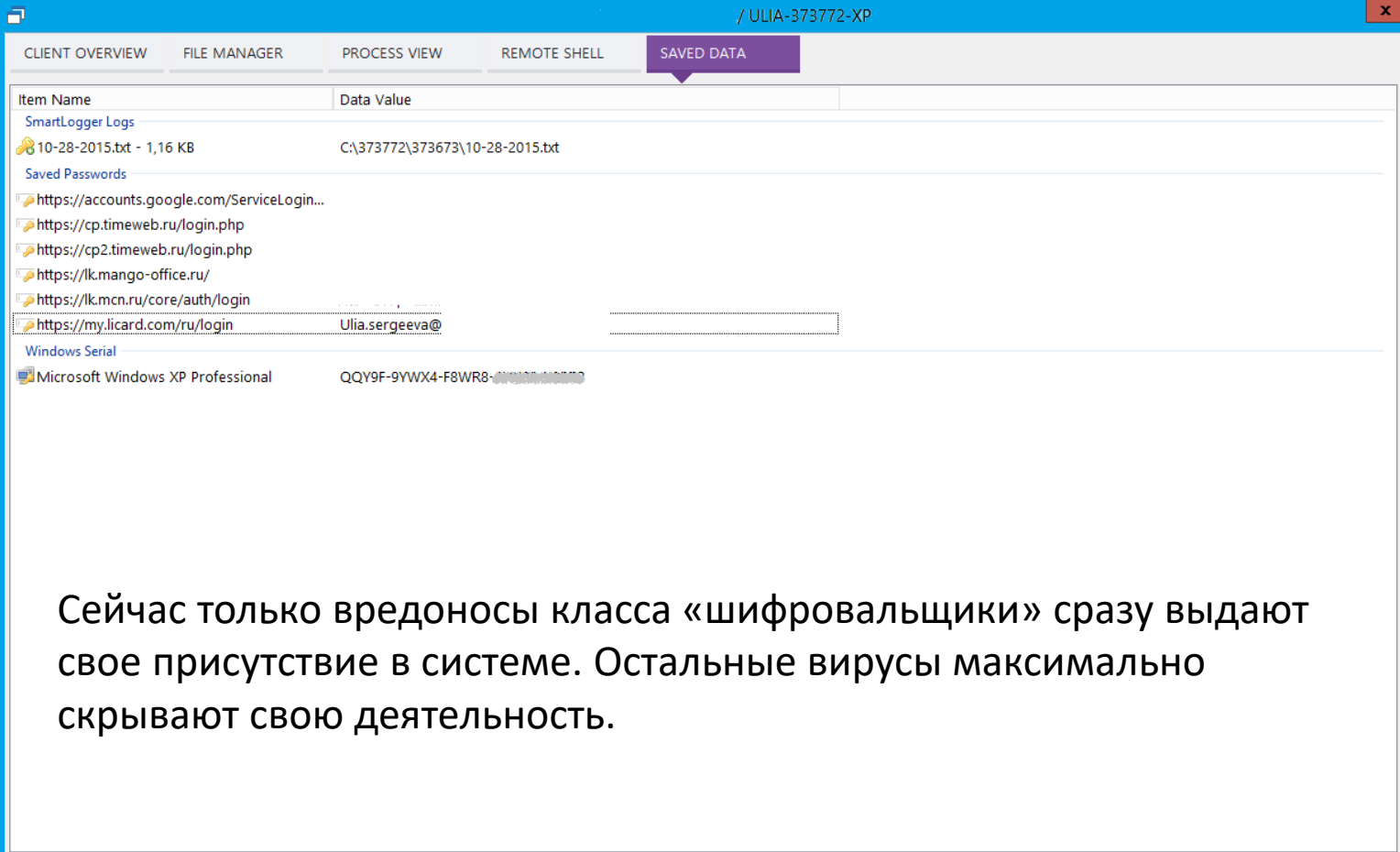


Удаленный контроль зараженного компьютера

The screenshot displays a remote control interface for a client named ULIA-373772-XP. The interface includes a top navigation bar with tabs for CLIENT OVERVIEW, FILE MANAGER, PROCESS VIEW, REMOTE SHELL, and SAVED DATA. The CLIENT OVERVIEW tab is active, showing a detailed overview of the client's information, organized into several sections:

- Client Information:**
 - Client ID: ULIA-373772-XP
 - First Seen by Server: 10/28/2015 3:29:35 AM
 - File Creation Date: 28.10.2015 13:26:15
 - Country: Russian Federation
 - Client Path: \\373672\repair.exe
- Software Information:**
 - Operating System: Microsoft Windows XP Professional
 - Active Window: ????????? ??????????
 - Antivirus: AntiVirus: N/A
 - Firewall: Firewall: N/A
 - System Uptime: 0 Day(s) 7 Hours 23 Minutes
 - User Privileges: Admin
 - Machine Name: YULIA
 - PC Username: ?????????
- Hardware Information:**
 - Machine Type: Desktop
 - CPU: Intel(R) Pentium(R) 4 CPU 3.00GHz
 - GPU: Intel(R) G33/G31 Express Chipset Family.
 - RAM: 2 GB
 - Battery: N/A (Desktop Machine)
 - Monitor Count: 1
- Network Information:**
 - WAN Address:
 - Download Speed: 569 KB/sec
 - LAN Address: 192.168.1.122
 - MAC Address: 002191F48817

Удаленный контроль зараженного компьютера



The screenshot shows a remote control application window titled "/ ULIA-373772-XP". The interface includes a menu bar with options: CLIENT OVERVIEW, FILE MANAGER, PROCESS VIEW, REMOTE SHELL, and SAVED DATA. The SAVED DATA tab is active, displaying a table of saved items:

Item Name	Data Value
SmartLogger Logs	
10-28-2015.txt - 1,16 KB	C:\373772\373673\10-28-2015.txt
Saved Passwords	
https://accounts.google.com/ServiceLogin...	
https://cp.timeweb.ru/login.php	
https://cp2.timeweb.ru/login.php	
https://lk.mango-office.ru/	
https://lk.mcn.ru/core/auth/login	
https://my.licard.com/ru/login	Ulia.sergeeva@
Windows Serial	
Microsoft Windows XP Professional	QQY9F-9YWX4-F8WR8-9W537Y-160793

Below the screenshot, a text box contains the following Russian text:

Сейчас только вредоносы класса «шифровальщики» сразу выдают свое присутствие в системе. Остальные вирусы максимально скрывают свою деятельность.

Благодарю за внимание!

Андрей Березов

Руководитель департамента защиты
информации

ООО «Информационный центр»

(423) 240-48-66 доб. 401

E-mail: and@ic-dv.ru