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

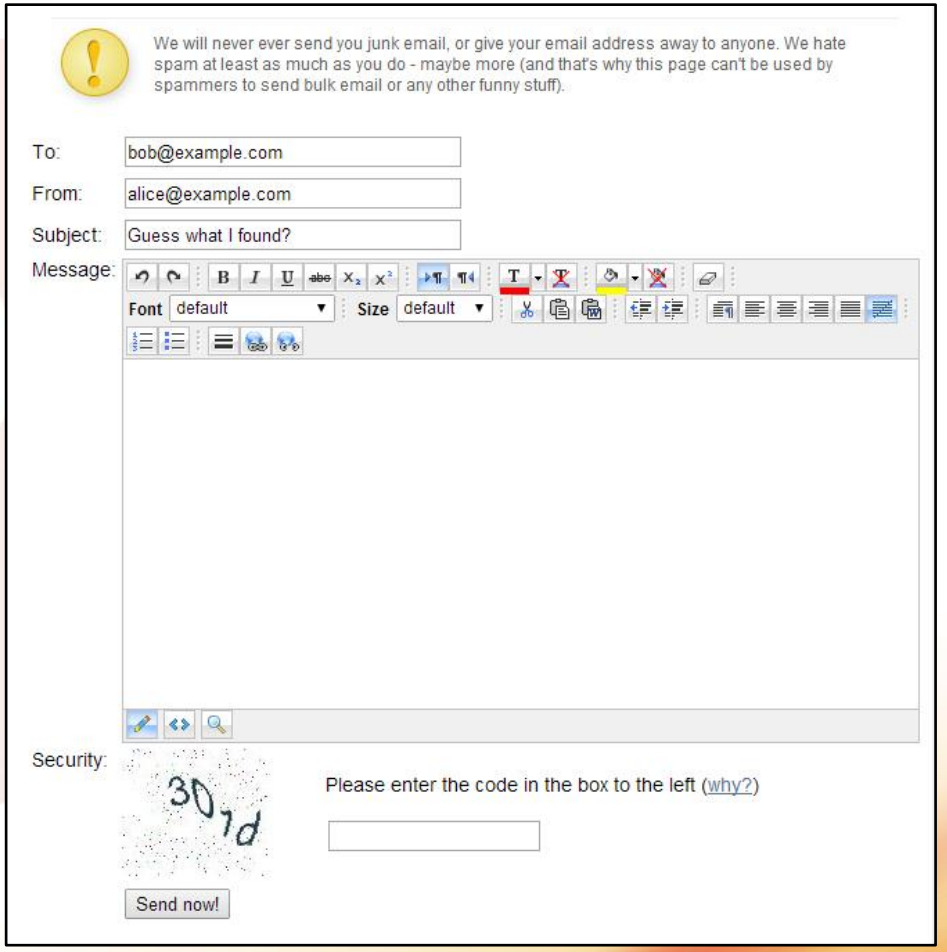
- рядовые сотрудники являются неотъемлемым звеном процессов ИБ;
- большинство всех заражений вредоносным ПО осуществляется по каналам электронной почты;
- сотрудники не осведомлены об уязвимостях почтового протокола и о методах социальной инженерии.

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



Пример фишингового письма

Ответить Ответить всем Переслать Мгновенные сообщения

Чт 29.10.2015 14:39

Федеральная налоговая служба <no-reply@nalog.ru>

Отчетность 2015

Кому [redacted]

Для использования новых функций сдачи отчетности, необходимо установить обновленную версию программного обеспечения.

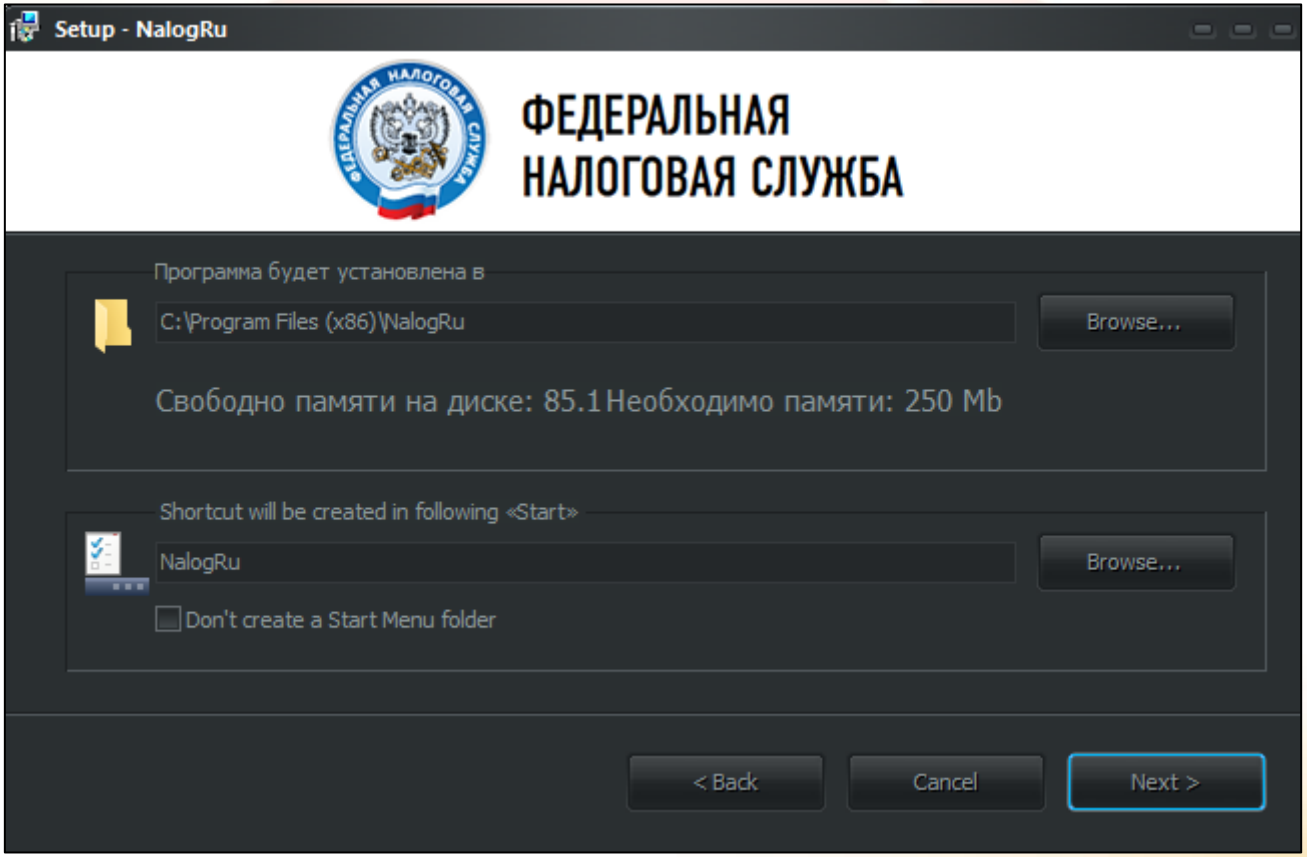
Для этого скачайте и установите обновление, следуя инструкциям на экране.

Предупреждаем, что в случае использования прежних версий программного обеспечения при обработке отчетности возможны сбои всякого рода.

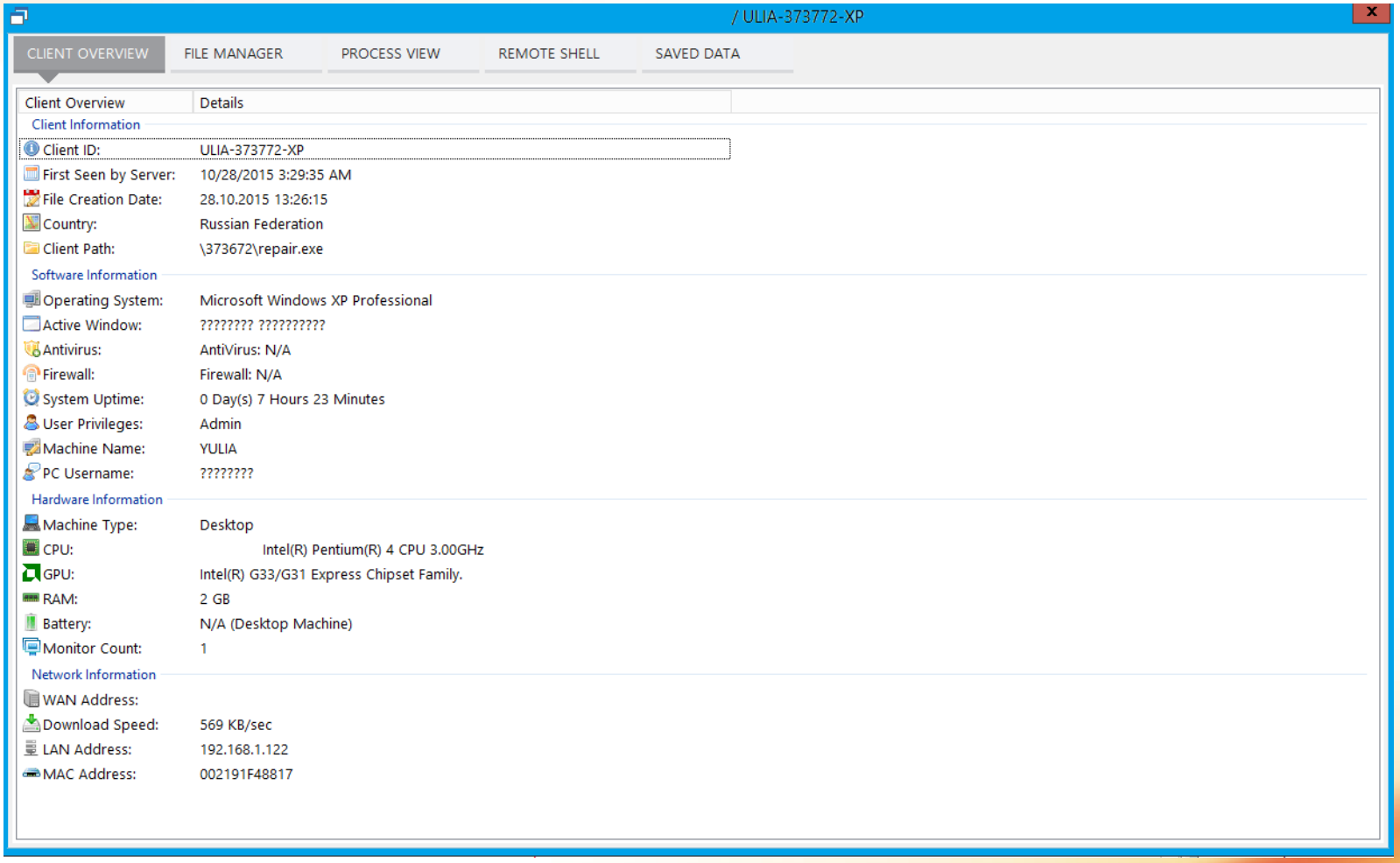
Скачать

ФЕДЕРАЛЬНАЯ НАЛОГОВАЯ СЛУЖБА

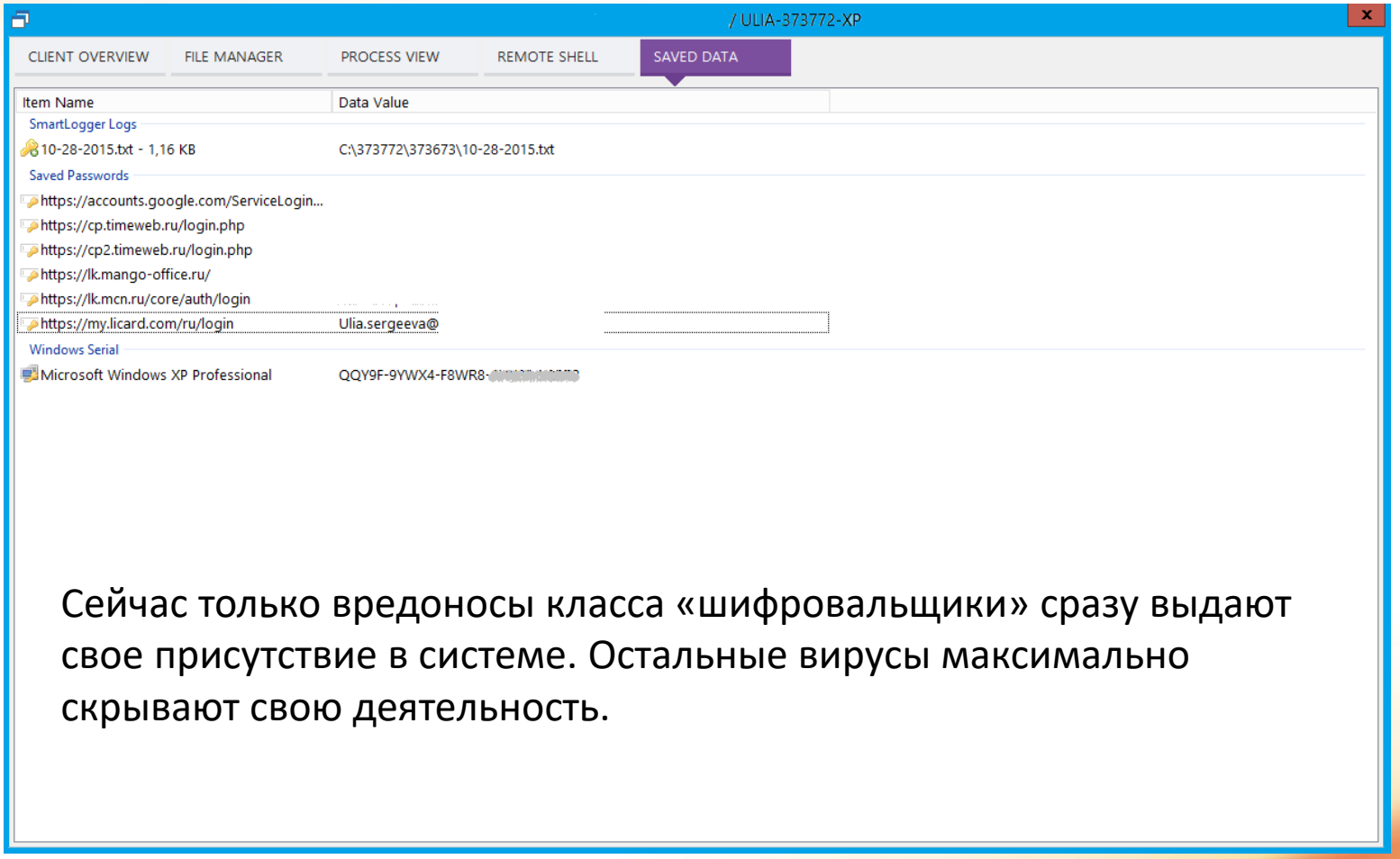
Установка троянского ПО «от налоговой»



Удаленный контроль зараженного компьютера



Удаленный контроль зараженного компьютера



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