

Державна кібербезпека ≠ Кібербезпека держави Уроки #FRD

State Cybersecurity ≠ Cybersecurity of the State
Lessons of #FRD

Костянтин Корсун, Бережа Сек'юріті, директор та співзасновник
Kostiantyn Korsun, Berezha Security, Co-founder & CEO

NoNameCon, May 16, 2019, Kyiv, Ukraine

Structure

- ▶ What is Responsible Disclosure and history of FuckResponsibleDisclosure (#FRD);
- ▶ #FRD Paradox: I'm not a doctor, I'm a pain.
- ▶ The Story in Pictures: first splashes of #FRD, #FRD reaction, #FRD participants;
- ▶ Behavioral models during the #FRD: from a hate to a love;
- ▶ National Cybersecurity System: what we've got and how much we paid;
- ▶ #FRD efficiency: results of 23 Top Ukrainian Experts polling;
- ▶ Conclusions

Intro



Cybersecurity is important.
Do you agree?

Cybersecurity is a most important
thing? Do you agree?

There is no Cybersecurity System
in whole Ukraine.
Trust me.

What we actually have as a System?



Ally

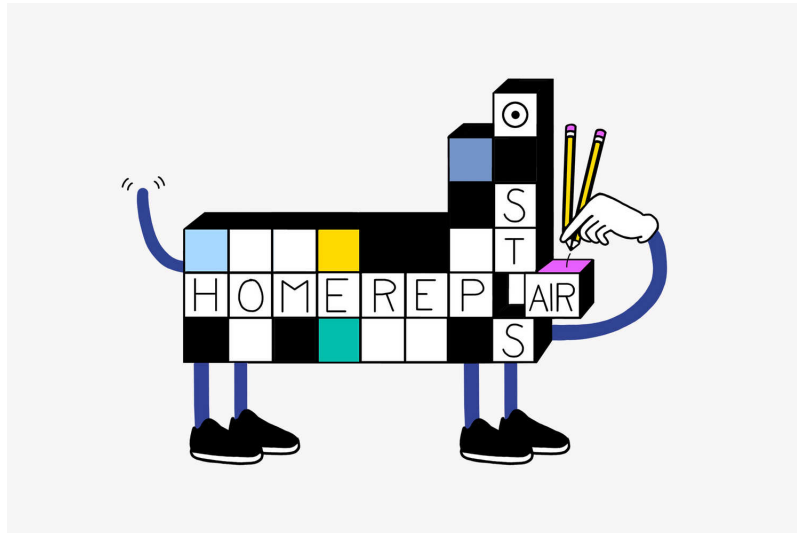


ЦВК



#FRD Paradox

- ▶ There is No System, any evidences?
- ▶ In October 2017 group of activists set up something under hashtag #FuckResponsibleDisclosure, (#FRD)
- ▶ Зневажаю_Відповідальне_Розкриття
- ▶ What those three words under the same # mean?



#FRD Paradox

- ▶ **Responsible Disclosure:** a vulnerability is revealed to an owner, in a nonpublic way

Shortcoming: low efficiency

- ▶ **Full Disclosure, Irresponsible Disclosure:** a vulnerability is revealed to everyone, in a public way.

Shortcoming : exploitation possibility, in fact assisting offender

Bruce Schneier: "Full disclosure - the practice of making the details of security vulnerabilities public - is a damned good idea. Public scrutiny is the only reliable way to improve security, while secrecy only makes us less secure"

https://www.schneier.com/essays/archives/2007/01/schneier_full_disclo.html





#FRD Paradox

- ▶ #FRD important difference (and similarity):
 - public vulnerability statement BUT
 - no exploitation possibilities, like open disk share (exception: XSS);
- ▶ Motivation: improvement of cybersecurity level at critical infrastructure objects AND public limelight through resonance;
- ▶ #FRD activists: no problems' solving, no service ;
- ▶ #FRD activists: only point on problems, laughing on officials' ignorance and critical infrastructure objects' owners incompetence;
- ▶ I'm not a doctor, I'm just a pain.

#FRD Paradox

How legal #FRD is?

How moral #FRD is?



The Story in Pictures

- ▶ When #FRD started: October 6, 2017 with water supply company and energy company;
- ▶ CERT-UA
- ▶ Енергоатом (Energoatom, nuclear energy company): open access to local network;
- ▶ Regional water supply company: : open access to local network;
- ▶ КиївЕнерго (KyivEnergo, energy company): open access to local network;
- ▶ Фінмоніторинг (Financial Monitoring Authority): archaic web site containing plenty of vulnerabilities





Sean Brian Townsend

October 6, 2017 · Kyiv · 🌐

...

Пока аппарат Рады готовит к публикации текст закона 2126а, хочу поговорить о критической инфраструктуре и субъектах её защищающих. Я уже рассказывал эту историю, но не лишним будет рассказать её еще раз. Один из наших хакеров "брутил дедики" (или на мусорском: осуществлял несанкционированный доступ к охраняемой законом информации путём подбора пароля пользователя через телекоммуникационную сеть "Интернет") и зацепил "предприятие критической инфраструктуры" - водоканал, стало ...

[Continue Reading](#)

[See Translation](#)

A	B	C	D	E	F	G	H	I	J	K	L
DILNY	GR	OS_RAH	NAME	NVUL	BUD	KVAR	DO_OPL	OPLAT	SAL_KIN	POG_SUM	POG_KIN
15	3					2	22.880	0.000	214.690	0.000	
15	3						-64.350	100.000	1,356.760	0.000	
15	3					1	15.250	0.000	1,315.960	0.000	
15	3					3	59.930	0.000	622.910	0.000	
15	3						120.050	200.000	329.730	63.590	03/2012
17	3					1	45.760	50.000	288.810	0.000	
8	3						1,195.880	0.000	981.020	12.810	04/2002
1	3					1	1,291.670	0.000	1,313.810	0.000	
1	3						120.050	0.000	1,404.340	0.000	
1	3					1	59.930	0.000	222.040	0.000	
1	3					1	120.050	0.000	236.220	0.000	
1	3					2	60.020	0.000	1,997.460	0.000	
1	3					2	90.030	0.000	1,291.110	0.000	
1	3					3	34.300	0.000	237.180	9.000	11/2008
1	1					2	90.030	400.000	248.050	21.000	01/2002
1	3					3	30.010	0.000	749.860	0.000	
17	3						15.250	0.000	485.080	25.000	11/2011
14	3						3.820	0.000	207.150		
17	3						34.320	100.000	281.410		
17	3						11.440	0.000	1,120.480		

● Chat (16)



Sean Brian Townsend

October 9, 2017 · Kyiv · 🌐



Добро пожаловать в CERT-UA? #FuckResponsibleDisclosure

The State Service for Special Communication and Information Protection

Пароль я не проверял. Замерим время реакции на инцидент.

(Пароль от почтового ящика группы быстрого реагирования на киберугрозы ДССЗІ из-за ошибки был доступен прямо у них на сайте. Это всё что вам нужно знать о гос. спец. связи. Нет, это не учебная тревога. Ваш кэп.)

[See Translation](#)

```
cert.gov.ua/wp-content/themes/cert/ver

$real_ip = GetRealIp();

if (chk_crypt($_POST['code'])) {
    $config = array();
    $config['smtp_username'] = 'ipguard@cert.gov.ua';
    $config['smtp_port'] = '25';
    $config['smtp_host'] = 'mail3.dsszzi.gov.ua';
    $config['smtp_password'] = 'welc0me2cert';
    $config['smtp_debug'] = true;
    $config['smtp_charset'] = 'UTF-8';
    $config['smtp_from'] = 'CERT-WEB';

    $to = "cert@cert.gov.ua";
    $subject = "ПОВІДОМЛЕННЯ З САЙТУ CERT";
    $incident_date = date("Y-m-d H:i:s");
    $message="Тип інциденту:&nbsp;{$_POST['theme']}<br/><br/>
    Контактна інформація:&nbsp;{$_POST['text_contact']} <br/><br/>
    Дата та час виявлення несанкціонованих дій:&nbsp;{$incident_date}<br /><br/>
    Опис несанкціонованих дій:<br /> {$_POST['text_message']}<br/><br/>
    IP:&nbsp;{$real_ip}<br/><br/>
    User-agent:&nbsp;{$_SERVER['HTTP_USER_AGENT']}";

    // $headers = 'Content-type: text/html; charset="utf-8" . "\r\n";
    // $headers .= 'From: CERT-WEB <ipguard@cert.gov.ua> . "\r\n";
```




Сергей Агашков [https](#) тоже нет

Like · Reply · 27 mins



Nikita Nazarenko Ну кароч:

```
"if (chk_crypt($_POST['code'])) {  
    $config = array();  
    $config['smtp_username'] = 'ipguard@cert.gov.ua';  
    $config['smtp_port'] = '25';  
    $config['smtp_host'] = 'mail3.dsszzi.gov.ua';  
    $config['smtp_password'] = 'welc0me2cert';  
    $config['smtp_debug'] = true;  
    $config['smtp_charset'] = 'UTF-8';  
    $config['smtp_from'] = 'CERT-WEB';"
```

```
#include <iostream>  
  
using namespace std;  
  
int main()  
{  
    cout << "Hello world!" << endl;  
    return 0;  
}
```



Like · Reply · 4 · 26 mins



Sean Brian Townsend added 7 new photos — with Jeoffrey Dahmer and Andrii Pertsukh.

November 27, 2017 · Kyiv · 🌐



Енергоатом жаловался на то, что "малоизвестная группа провокаторов" публикует документы без номеров и подписей. С радостью идём вам навстречу. Провоцируем ответственное отношение к работе с 2014 года. Сервер 2004 года ещё дышит, а? Это утечка из офиса, не со станции конечно же, что не делает её менее важной. [#FuckResponsibleDisclosure](#)

Документы - доказательство утечки из локальной сети. Неважно как. Важно, что внутренние документы текут.

И еще раз. Дело не в документах, как таковых, а в том что они подтверждают, что длительное время существовал доступ в локальную сеть. Контрактор, говорите, не важно, говорите, ну-ну... Хотелось бы увидеть не только извинения и закрытые дыры, но и подробный публичный отчёт о работе над ошибками. Извините, но эту пилюлю вам придется съесть. Можете начать уже в среду на конференции "Роль и место спец. служб в защите критической инфраструктуры".

P.S. Донецкая и Черниговская ОДА по-прежнему стоят нараспашку. По донецкой россияне лазят, а Черниговскую только пальцем ткни - всё потечёт. Как будто бы нет войны.

[See Translation](#)



МІНІСТЕРСТВО ЕНЕРГЕТИКИ ТА ВУГІЛНОЇ ПРОМИСЛОВОСТІ УКРАЇНИ
ЕНЕРГО АТОМ

НАЦІОНАЛЬНА АТОМНА
ЕНЕРГОГЕНЕРУЮЧА
КОМПАНІЯ



МІНІСТЕРСТВО ПАЛИВА ТА ЕНЕРГЕТИКИ УКРАЇНИ
ЕНЕРГО АТОМ

НАЦІОН
ЕНЕРГО

● Chat (24)



Sean Brian Townsend is with Jeffrey Dahmer and Andrii Pertsukh.

November 22, 2017 · Kyiv · 🌐

Третий вопрос по кибербезопасности. Совсем простой. Жить хотите?
#FuckResponsibleDisclosure

See Translation

Интернет ОКВП "Дніпро-Кіровоград"						
Место установки	Тип модема	Номер телефона	IP адрес	Login	Parol	Тип связи
Диспетчер						
Шибер						
Водозабор						
Врезка "Победа"						
Перекачная						
Берёзовка - расход						
Задвижка "Рогатая"						
Водозабор эл.сч.						
Коневы 2						
МИОС						



Sean Brian Townsend is with Jeoffrey Dahmer and Andrii Pertsukh.

November 22, 2017 · Kyiv · 🌐



Еще один вопрос. Кто-нибудь извлёк урок из Black Energy, или подождём еще один blackout или диверсию? #FuckResponsibleDisclosure

See Translation

**СТРУКТУРНИЙ ВІДОКРЕМЛЕНИЙ ПІДРОЗДІЛ «КИЇВСЬКІ ТЕЦ»
ПУБЛІЧНОГО АКЦІОНЕРНОГО ТОВАРИСТВА
«КИЇВЕНЕРГО»**

01013, м. Київ, вул. Промислова, 4, телефон 207-87-08, 207-87-30, факс (044) 207-87-55
svpktec@kievenergo.com.ua

14.03.2016 № 028/1/21/11/997

На _____

Директору
ДП «ЕНЕРГОРЕМОНТ»
ПАТ «КИЇВЕНЕРГОРЕМОНТ»
Горобцю Є.В.
04071 м. Київ, пров. Електриків, 15
Тел/ факс (044) 425-84-50

Шановний Євгене Володимировичу!

Згідно з Вашими пропозиції конкурсних торгів на закупівлю: «33.12.1 Ремонтуння та технічне обслуговування машин загальної призначеності (Ремонт обладнання енергоблоку № 1, ТФУ в складі енергоблоку №1 та загальностанційного обладнання ТЕЦ-6)» та на закупівлю «33.14.1 Ремонтуння та технічне обслуговування іншого електричного устаткування (ремонт основного, допоміжного та загальностанційного електротехнічн



Sean Brian Townsend is with Jeffrey Dahmer and Andrii Pertsukh.

November 17, 2017 · Kyiv · 🌐



Державна служба фінансового моніторингу України не обновлялась 10 (десять) лет. Множественные критические уязвимости. Сайт может быть взломан в любой момент. А может быть уже? Ребята, мне на него дышать страшно, чтобы нечаянно не разломать его на куски.

Пока как в колхозе - всё вокруг общее, а значит - ничьё, пока никто ни за что не отвечает, никакие модные железки и высокие зарплаты ничего не исправят. Увольнять по статье. Привлекать к уголовной ответственности за халатность. Оставшимся повышать зарплату. Вы требуете от граждан "ответственности", а какую ответственность вы готовы взять на себя? Поэтому - [#FuckResponsibleDisclosure](#)

See Translation

www.sdfm.gov.ua/info.php

PHP Version 5.2.6	
System	Windows NT WWW-NEW 5.2 build 3790
Build Date	May 2 2008 18:01:20
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--with-gd=shared" "--with-extra-includes=C:\Program Files (x86)\Microsoft SDK\Include\C:\PROGRA~2\MICROS~2\VC98\ATL\INCLUDE;C:\PROGRA~2\MICROS~2\VC98\INCLUDE;C:\PROGRA~2\MICROS~2\VC98\MFC\INCLUDE" "--with-extra-libs=C:\Program Files (x86)\Microsoft SDKLib\C\PROGRA~2\MICROS~2\VC98\LIB;C:\PROGRA~2\MICROS~2\VC98\MFC\LIB"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded	C:\php\php.ini

The Story in Pictures: KhOR

Херсонська обласна рада (Kherson Regional Public Council): typical example

Problem: open access to internal network disk, without a password



Sean Brian Townsend is with Jeffrey Dahmer and Andrii Pertsukh.

November 15, 2017 · Kyiv · 🌐

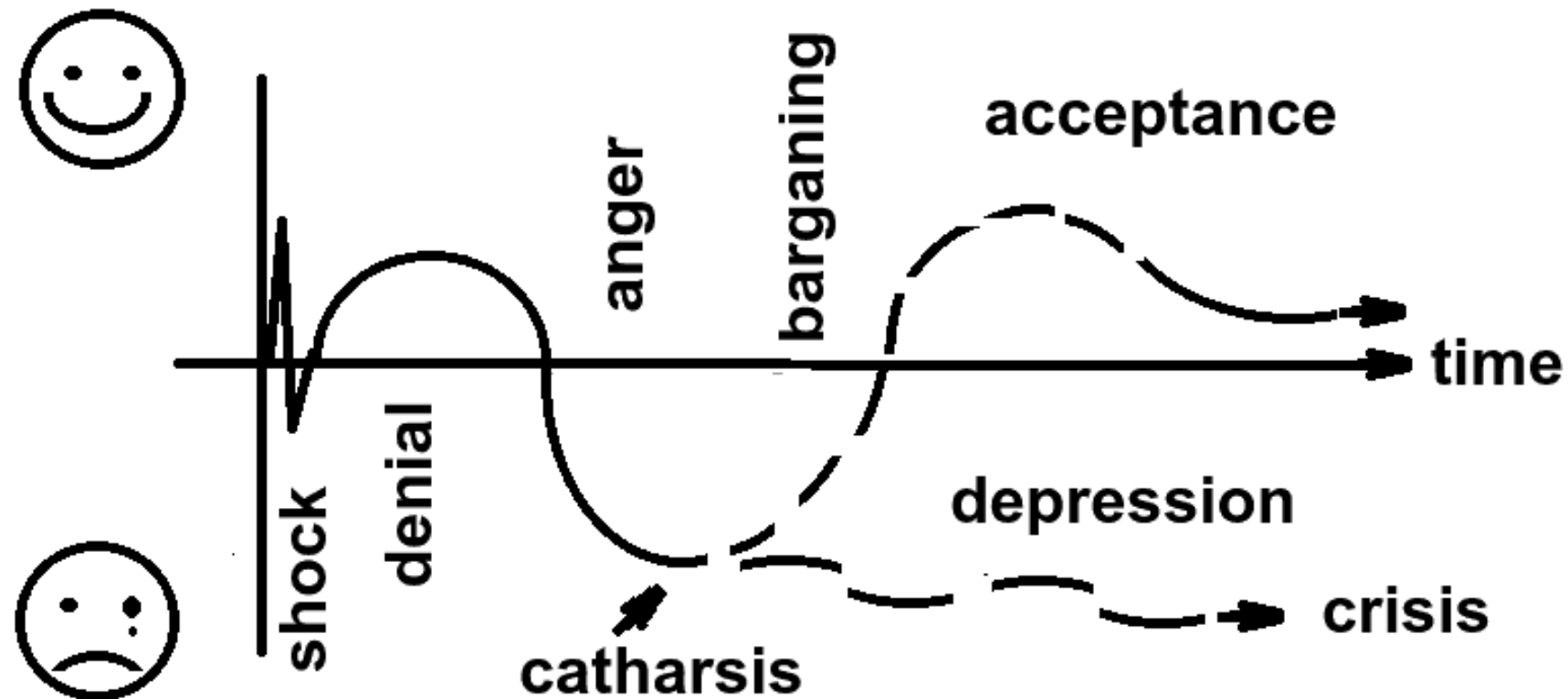
Следующий смертельный номер на конкурсе "Слабоумие и отвага" исполняет системный администратор [Херсонська обласна рада](#) Они решили не мелочиться и расшарить в Интернет общий диск. На запись. Без пароля. С незакрытой уязвимостью. Со всеми своими документами, ведомостями, авиабилетами в Ростов, аудиозаписями заседаний, ключами АЦСК и прочими полезными вещами.

Как и в случае с [Національна академія внутрішніх справ](#), файлы .so - это фрагмент эксплоита [#SambaCry](#) (таже самая уязвимость, что и в нашумевших вымогателях, после которых все били себя пяткой в грудь "никогда вновь!"). И это значит, что сервер областного совета был взломан полностью другими хакерами полгода назад и никому до этого нет дела. [#FuckResponsibleDisclosure](#)

[See Translation](#)

```
sean@localhost:/mnt/ext
File Edit View Search Terminal Help
[root@localhost ext]# mount|grep cifs
//195.230.130.104/share on /mnt/ext type cifs (rw,relatime,vers=default,cache=strict,username=sean,dom
main=,uid=0,noforceuid,gid=0,noforcegid,addr=195.230.130.104,file_mode=0755,dir_mode=0755,nounix,mapp
osix,rsize=1048576,wsiz=1048576,echo_interval=60,actimeo=1)
[root@localhost ext]# ls -al
total 37248004
```


Kübler-Ross model: five stages of a grief



The Story in Pictures: KhOR

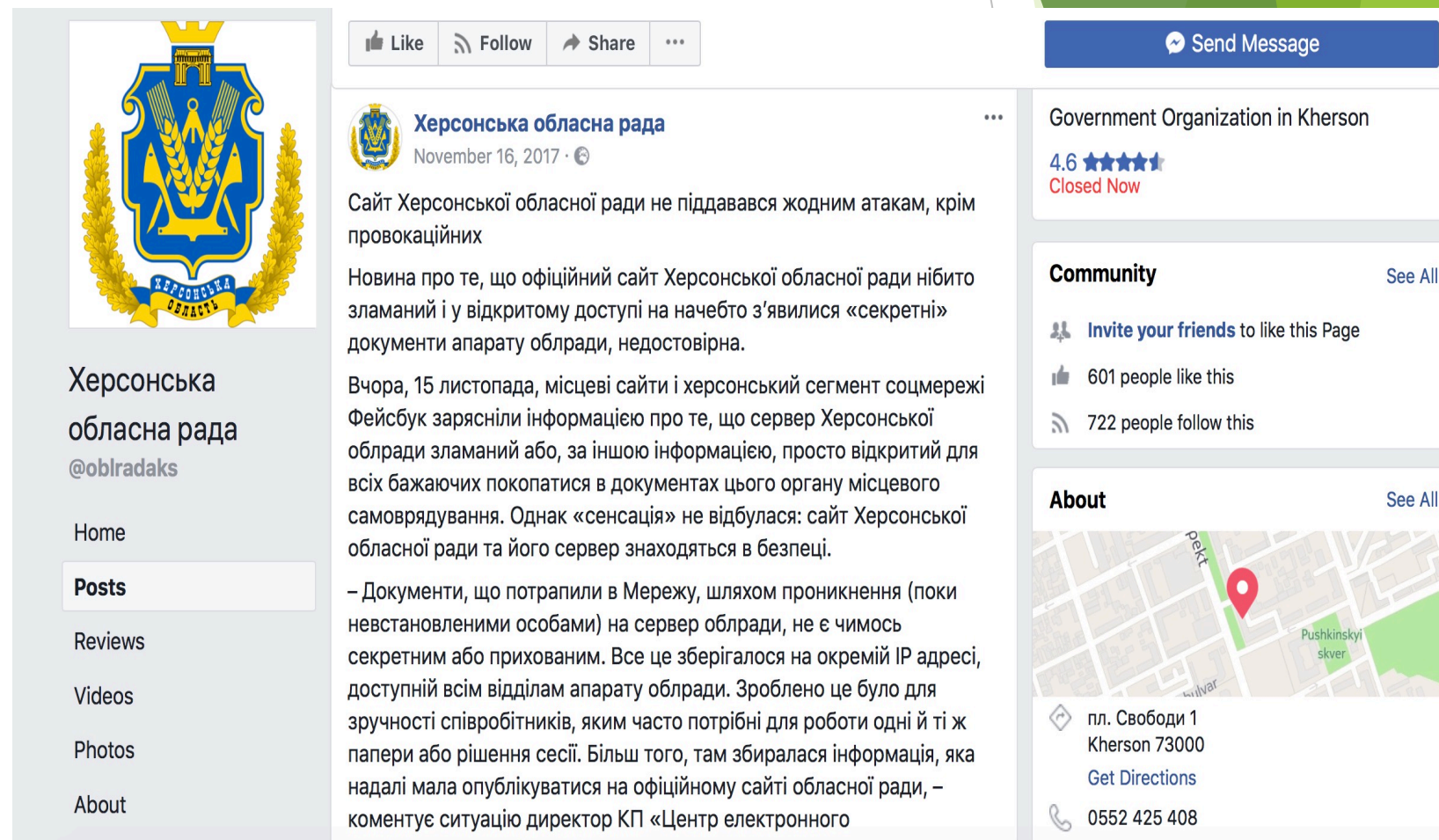
Shock - Denial - Anger:

1) It's just a provocation

2) We haven't been hacked

3) The documents are not secret

4) We complained to the police



The screenshot displays the Facebook profile of the Kherson Regional Council. The profile picture is the official coat of arms of the Kherson Oblast. The page name is "Херсонська обласна рада" with the handle "@oblrads". The post, dated November 16, 2017, contains the following text:

Сайт Херсонської обласної ради не піддавався жодним атакам, крім провокаційних

Новина про те, що офіційний сайт Херсонської обласної ради нібито зламаний і у відкритому доступі на начебто з'явилися «секретні» документи апарату облради, недостовірна.

Вчора, 15 листопада, місцеві сайти і херсонський сегмент соцмережі Фейсбук зарясніли інформацією про те, що сервер Херсонської облради зламаний або, за іншою інформацією, просто відкритий для всіх бажаючих покопатися в документах цього органу місцевого самоврядування. Однак «сенсація» не відбулася: сайт Херсонської обласної ради та його сервер знаходяться в безпеці.

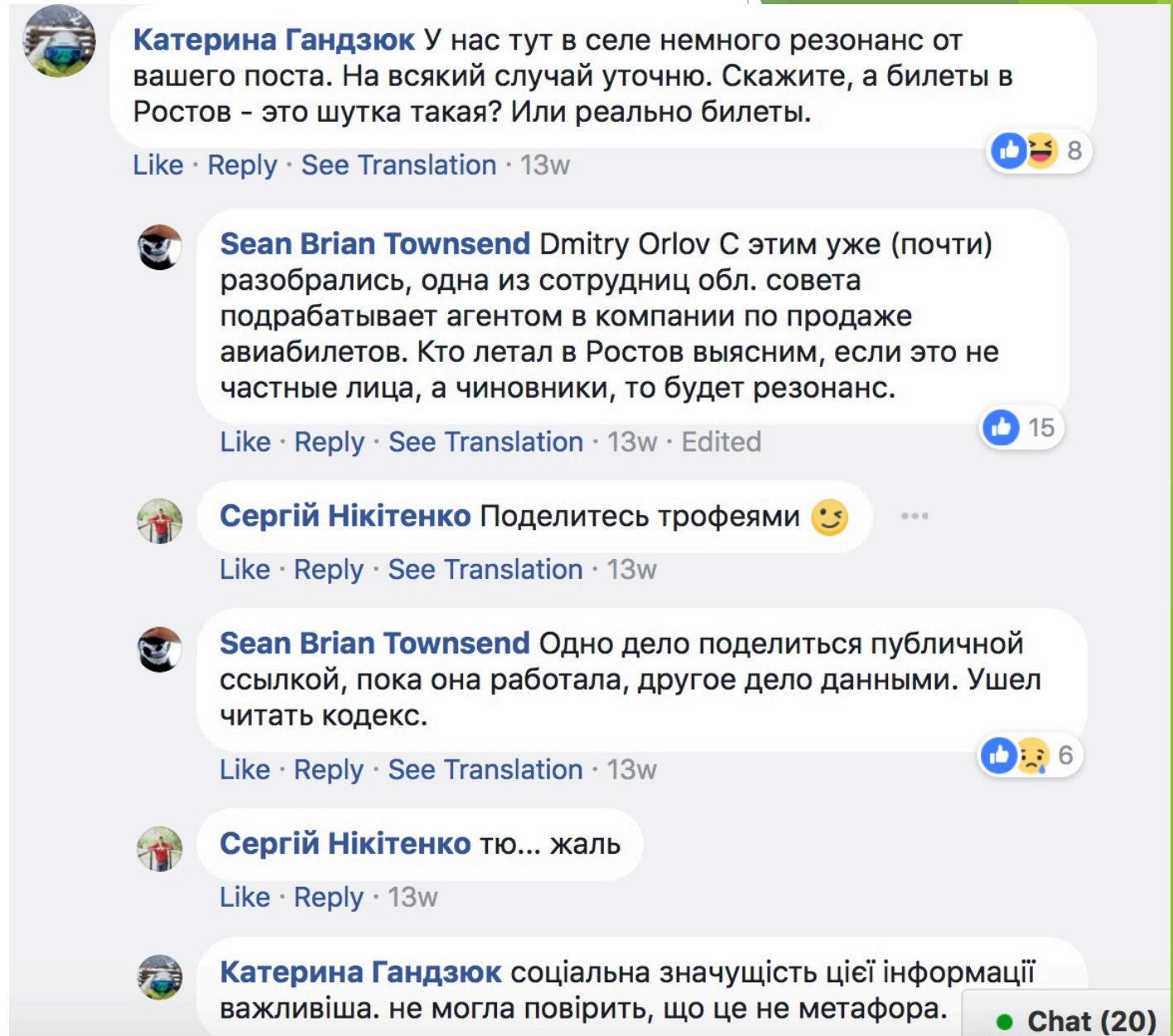
– Документи, що потрапили в Мережу, шляхом проникнення (поки невстановленими особами) на сервер облради, не є чимось секретним або прихованим. Все це зберігалося на окремій IP адресі, доступний всім відділам апарату облради. Зроблено це було для зручності співробітників, яким часто потрібні для роботи одні й ті ж папери або рішення сесії. Більш того, там збиралася інформація, яка надалі мала опублікуватися на офіційному сайті обласної ради, – коментує ситуацію директор КП «Центр електронного

On the right side of the page, there is a "Community" section showing 601 likes and 722 followers, and an "About" section with a map of the council's location at "пл. Свободи 1, Kherson 73000".

The Story in Pictures: KhOR

Bargaining: is it true that....?

Kateryna Handziuk



The screenshot shows a Facebook post with several comments. The comments are in Ukrainian and Russian. The first comment is from Катерина Гандзюк, followed by Sean Brian Townsend, Сергій Нікітенко, and another Sean Brian Townsend. The last comment is from Катерина Гандзюк again. The interface includes like, reply, and translation buttons for each comment, as well as a chat bubble at the bottom right.

Катерина Гандзюк У нас тут в селі немного резонанс от вашего поста. На всякий случай уточню. Скажите, а билеты в Ростов – это шутка такая? Или реально билеты.

Like · Reply · See Translation · 13w 8

Sean Brian Townsend Dmitry Orlov С этим уже (почти) разобрались, одна из сотрудниц обл. совета подрабатывает агентом в компании по продаже авиабилетов. Кто летал в Ростов выясним, если это не частные лица, а чиновники, то будет резонанс.

Like · Reply · See Translation · 13w · Edited 15

Сергій Нікітенко Поделитесь трофеями 😊 ...

Like · Reply · See Translation · 13w

Sean Brian Townsend Одно дело поделиться публичной ссылкой, пока она работала, другое дело данными. Ушел читать кодекс.

Like · Reply · See Translation · 13w 6

Сергій Нікітенко тю... жаль

Like · Reply · 13w

Катерина Гандзюк соціальна значущість цієї інформації важливіша. не могла повірить, що це не метафора.

Chat (20)

The Story in Pictures: KhOR

Depression - Acceptance: ignoring and/or thank you



Галина Ляшевская Не будет никаких обмороков, не переживайте. Будем разбираться и наводить порядок внутри. Спасибо.

Like · Reply · 1y



^ Hide 27 Replies



Sean Brian Townsend Вот это конструктивный подход.

Like · Reply · 1y

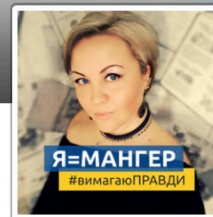
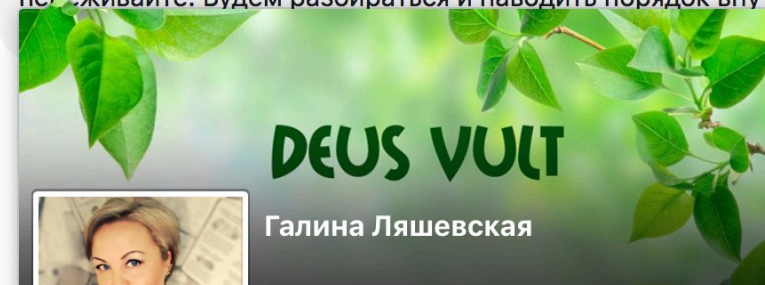


Галина Ляшевская Вам спасибо за вчерашнюю ночную беседу. Действительно, многое встало на свои места, и, кроме благодарности Вам, у меня сегодня нет других эмоций.

Like · Reply · 1y



Галина Ляшевская Не будет никаких обмороков, не переживайте. Будем разбираться и наводить порядок внутри.



Галина Ляшевская

радник Голови at Херсонська обласна рада

November 1, 2016 to present

Lives in Kherson

Add Friend

Follow

Typical #FRD reaction: other option

- 1) We haven't been hacked
- 2) We don't have any critical/secret information
- 3) We complained to the police
- 4) It was customized attack from our competitors



Typical #FRD reaction

Shame on you!

BUT

Probably the problem needs to be solved



VS



Most prominent #FRD cases

43 most prominent cases

(from most important)

State and public authorities: 27

- ▶ Центральна виборча комісія
- ▶ Державний реєстр виборців
- ▶ Міністерство оборони України
- ▶ Генеральна прокуратура України
- ▶ РНБО
- ▶ Міністерство юстиції України
- ▶ Міністерство охорони здоров'я
- ▶ Міністерство внутрішніх справ України
- ▶ Міністерство енергетики та вугільної промисловості України

Most prominent #FRD cases

- ▶ Білоцерківський відділ поліції Національної поліції
- ▶ Державна регуляторна служба України
- ▶ Конституційна комісія при Президентові України
- ▶ Державна служба України з лікарських засобів та контролю за наркотиками
- ▶ Державна служба статистики України
- ▶ НКРЕП (Національна комісія, що здійснює державне регулювання у сферах енергетики та комунальних послуг)
- ▶ Державна служба фінансового моніторингу України

Most prominent #FRD cases

- ▶ Судова влада України
- ▶ Волинська ОДА
- ▶ Донецька ОДА
- ▶ Чернігівська ОДА
- ▶ Херсонська обласна рада
- ▶ Черкаська обласна рада
- ▶ районні державні адміністрації Хмельницької та Харківської областей

Most prominent #FRD cases

Critical infrastructure objects:

- ▶ Енергоатом
- ▶ Південно-Українська АЕС
- ▶ Укрпошта
- ▶ Укренерго
- ▶ Укрзалізниця
- ▶ Київпастрас
- ▶ Водоканал «Дніпро-Кіровоград»
- ▶ Київенерго
- ▶ ПАО «Завод Маяк»
- ▶ Державна фірма «Укрінмаш» («Укроборонпром»)
- ▶ КБ «Південне»
- ▶ Комунальний концерн «Центр комунального сервісу»
- ▶ Львівська залізниця

Most prominent #FRD cases

Приватні компанії:

- ▶ Метінвест
- ▶ Київстар
- ▶ велика аудиторська компанія



← → ↺ 🏠 <https://www.gp.gov.ua/ua/news/povistky.html?fp=10> Повістка



ГЕНЕРАЛЬНА ПРОКУРАТУРА УКРАЇНИ

PROSECUTOR GENERAL'S OFFICE OF UKRAINE



КОНТАКТИ

ПРИЗНАЧЕННЯ

ОРГАНИ ПРОКУРОРСЬКОГО САМОВРЯДУВАННЯ І КДКП

СТАТИСТИЧНА ІНФОРМАЦІЯ ПРО СТАН ЗЛОЧИННОСТІ ТА РЕЗУЛЬТАТИ ПРОКУРОРСЬКО-СЛІДЧОЇ ДІЯЛЬНОСТІ

ОЧИЩЕННЯ ВЛАДИ

ЗАПОБІГАННЯ ТА ПРОТИДІЯ КОРУПЦІЇ

ЗАБЕЗПЕЧЕННЯ ДОСТУПУ ДО ПУБЛІЧНОЇ ІНФОРМАЦІЇ

ЄДИНИЙ РЕЕСТР ДОСУДОВИХ РОЗСЛІДУВАНЬ

ТАЄМНА ПЕРЕВІРКА ДОБРОЧЕСНОСТІ

Повістка про виклик Медведчука В. В.

Повістка про виклик Коломойского І. В.

Генеральна прокуратура : XSS



Sean Brian Townsend

3 hrs · 🌐

А вы говорите, что #XSS фиговая уязвимость. (Необходимый disclaimer ни одна Prosecutor General's Office of Ukraine не пострадала) А ведь уже было такое, и если мне не изменяет память, даже обещались что-нибудь сделать со своим дырявым сайтом. #FRD

👍 🤔 😱 76

15 Comments

4 Shares



Like



Comment



Share

View 1 more comment



Mykola Stasiuk а що по датах тих повісток?

Like · Reply · 3h

🤔 1



Sean Brian Townsend replied · 1 Reply 3



Write a comment...





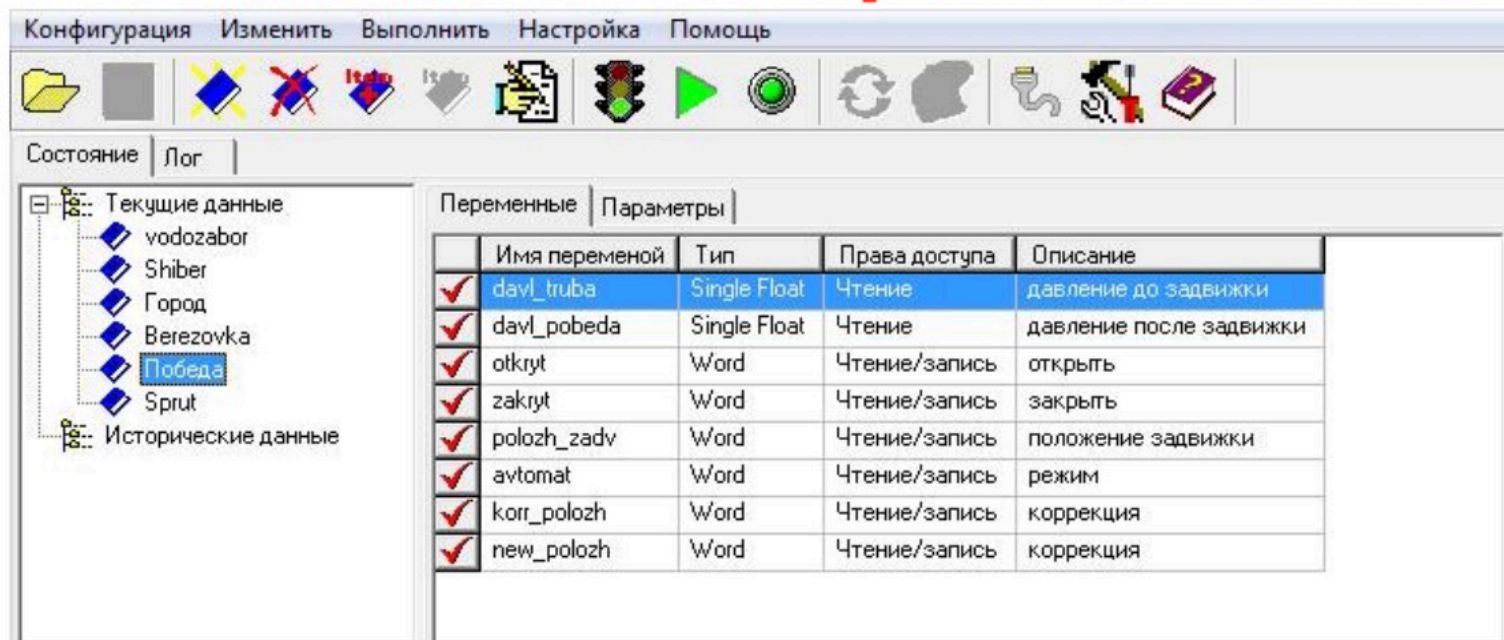
Sean Brian Townsend is with Jeffrey Dahmer and Andrii Pertsukh.

November 22, 2017 · Kyiv · 🌐

Чтобы расставить точки над "i", по поводу АЭС, ТЭЦ и водоканалов. Вы понимаете, что на картинке управление "технологической системой" элемента "критической инфраструктуры"? Технологической. Не бухгалтерией и не архивом переписки. Трубы, давление, задвижки - вот это всё. Клик! И нет воды. #FuckResponsibleDisclosure

See Translation

Водоканал: open network





Sean Brian Townsend is with Jeffrey Dahmer and Andrii Pertsukh.

November 17, 2017 · Kyiv · 🌐

Державна служба фінансового моніторингу України не обновлялась 10 (десять) лет. Множественные критические уязвимости. Сайт может быть взломан в любой момент. А может быть уже? Ребята, мне на него дышать страшно, чтобы нечаянно не разломать его на куски.

Пока как в колхозе - всё вокруг общее, а значит - ничьё, пока никто ни за что не отвечает, никакие модные железки и высокие зарплаты ничего не исправят. Увольнять по статье. Привлекать к уголовной ответственности за халатность. Оставшимся повышать зарплату. Вы требуете от граждан "ответственности", а какую ответственность вы готовы взять на себя? Поэтому - [#FuckResponsibleDisclosure](#)

See Translation

www.sdfm.gov.ua/info.php

sdfm.gov.ua

PHP Version 5.2.6

System	Windows NT WWW-NEW 5.2 build 3790
Build Date	May 2 2008 18:01:20
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--with-gd=shared" "--with-extra-includes=C:\Program Files (x86)\Microsoft SDK\Include;C:\PROGRA~2\MICROS~2\VC98\ATL\INCLUDE;C:\PROGRA~2\MICROS~2\VC98\INCLUDE;C:\PROGRA~2\MICROS~2\VC98\MFC\INCLUDE" "--with-extra-libs=C:\Program Files (x86)\Microsoft SDK\Lib;C:\PROGRA~2\MICROS~2\VC98\Lib;C:\PROGRA~2\MICROS~2\VC98\MFC\Lib"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded	C:\php\php.ini



Sean Brian Townsend

2 mins · 🌐

Я хотел бы спросить у парней из Державна служба статистики України, что думают о скриптах на сайте переписи населения (у нас же пробная намечается, не так ли) ваши парни? #XSS Пруф: <http://archive.fo/HqCte> #FuckResponsibleDisclosure



database.ukrcensus.gov.ua/STATBANK_LVIV/Dialog/Footnote.asp?File=19M0304_03.px&path=../Database/19DEMOGR/03/04/&ti=</title>

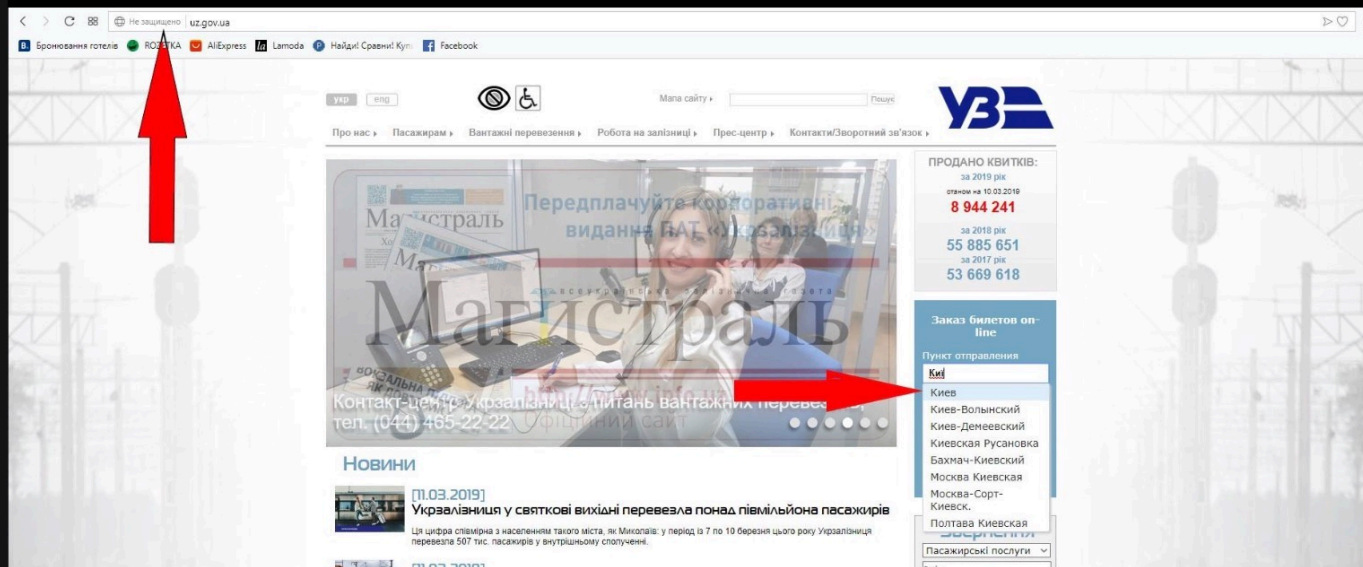
Зростання виробництва говнокода в Україні



Державна
служба
статистики:
XSS



Укрзалізниця: no https



Андрей Перевезий

2 hrs · 🌐

Ну что наш маленький #паровозикоблачко продолжает путь. Уважаемая [Укрзалізниця - Ukrzaliznytsia](#), вы повторяете подвиг МВС України и отказываетесь от https? Я так понимаю, что это тренд нынешнего сезона. Так же обратил внимание на интересный момент, в украинской версии сайта, почему то можно купить билеты только в города, названия которых написано русским языком. К чему бы это? #RFD



You and 5 others

1 Comment



Like



Comment



Share



Kir Vaznitcky Ну, у УЗ по обоим протоколам хоть отдается, хотя переадресацию не мешало бы конечно. У МВС совсем плохо.



Write a comment...



pF18d4kQw0AJ5Nj5t0jFvIDIGk1480ouMMkqpeELKz/p;vUZXNDXAdK9CZ2uJhW4
62wzJKYDJBmQnL0JYpPjHv/kvbc17FqtKh0ffAwH/E74FA4YvPPYjvP9AZvFvZg
p7JZHkWDu05jNXMRlppqzUdz2-Bz8050zKf80g06/CEnA2kUuM14AgA4w9As
qnnqHq04DzYntUj614y6VgKsQRkp7z5bDz2KNSzm2rYtVLv3W3QRARdCzELQID
AQK802ABDCB/TAd8NgVQ40FEqG0t2510smbZuA03VwhtvXpvnErAUwgc06GALUd
Iw5SwCBwAu0Tos150mbZuA03VwhtvXpvnErAwhgZ6Krg2swgZgcA4J8NBWYX
A1VBMRAwDQvDUQYIEwdn3j3hW51MQ0wCvDUYQW6K6m21MRUuEwYDVQKEXd
12F7Jhaxk3YXkxEjAQgNBv8ASTCUDJTMtTFZJvJESMBAGAL1EAxMJR01PQyIM
vk11M5K6wY3K0ZInvcNAQkBFhp2XZhrbgi1Q6XulnJhaxk3YXkhuH8Zpd315Y1Z
AlaG6/wK7+MwAGAL1UvEQFMAB4B8DQY3K0ZInvcNAQkBF8QADggEBCzadC1Df
0+X2218jrcQv51J3k8nWUvYzNSZpRnRwFDeP+KUEVSFE5SASe1+gH0rVYf
mC1BzSDQKc1Kx7p2bUwXtW+CS0E9rH2z51quuoYkU1to+MnL2KgrwQ40t016m
H16+ygV7YeJqesR18k8Yks2Aas5F8YjMAvJ1dEbA18Vgh/0tPgTmcmHzd4
r49D30j1J1J;QcNaf8915L21P0211TSrYmuqR4Q12051m4T5B3u0v4V4GM
8qLmUwK6vCv6Z4Y7THfK/eMu04+0JvR/3jAy4xeW0jdHMEAxLulZRdPAhGwgKr
umTVCl4GL9Pcd+=



Sean Brian Townsend's Photos

www.phone.energy.gov.ua/dvig/page.php?db_id=19"><img%20src=http://www.ljplus.ru/img4/s/a/sadistuzhasniy/Hto-zdes.jpg>



Like Comment

Options Send in Messenger



Sean Brian Townsend

1 hr

Укренерго

1

Like

Comment



Write a reply...



Укренерго

Державна регуляторна служба: XSS

www.dkrp.gov.ua/search?k="<script>alert('Регулируем регуляторов');</script>&x=0&y=0&t=

Офіційний сайт

ДЕРЖАВНА РЕГУЛЯТОРНА
СЛУЖБА УКРАЇНИ



РУЙНУЄМО БАР'ЄРИ
ДЛЯ ЧЕСНОГО БІЗНЕСУ В УКРАЇНІ

Регуляторна
політика

Дозвільна система та
ліцензування

Державний нагляд
(контроль)

Дерегуляція

Представництва Служби
у регіонах

Профільні робочі
групи

Гаряча
лінія

Контакти

субота | 25.08.2018

Регулируем регуляторов

OK



Sean Brian Townsend

August 25, 2018 · 🌐

Державна регуляторна служба України #XSS

Служба говорить, що сайт старий. Якщо він не потрібен, то його потрібно вимкнути, якщо потрібен, то починати. Це ще один поширений тип помилки. Коли (не якщо, а коли) буде взломано сервер повністю (з обома сайтами і новим і старим), то буде пізно. "Старі сайти" - чудовий вектор атаки. Ми поставили нову залізну двері, але поруч є стара дерев'яна, закриваючись на ключик. Makes perfect sense. Так що якщо у вас є піддомен або підкаталог "old" - вибирайте прямо зараз, якщо там залишилося щось потрібне, то потім розмістите заново. Або набейте з нього "чучело" (статическу копію)

👍 😂 🤔 327

64 Comments 21 Shares

Like

Comment

Share



Write a comment...



Chat (41)



Alexandr Galushchenko is with Sean Townsend and 38 others. ...

4 hrs · 🌐

Укрпошта: open network

Анонс.

#FuckResponsibleDisclosure

#Укрпошта. Система платежей. Списки клиентов и почтовых отправлений.

Что-то из старого по пенсиям.

Некислый объем на несколько тер. Все четко разложено и готово к применению в незаконных схемах.

И они рассказывают, что у них деньги не воруют 😊)

Есть вопросы? Задавайте.

Имя	Тип	Размер	Дата
ER	Кременчук - 10	STING	каталог_12_11_2018
305	НАП_КАС_20	M_VZ_07	%Thumbs
г.Гриб	КОДЫ УДК		%WinSCP-5.13.4-Setup
TVZ	КЕРНЕЛ	ISE	%Judy-5.70-installer
odbc	Акт_виз_робит		%rc
CONVERT	выгрузка для АРМ БЗ 27022018	Tarif_01_01_2018	%Зависимые Платежи
para	VV	cal	%Monitoring
BASE	VOLA	%	%SR
64	Zavard_online		%Назначение АРМ БЗ 1_0_pdf
SIZE_SINGLE	VVV	ALUT	%domedex35
TrayIcon	velula	2,8	%111
g_PV_01_08_2017	Updater	2,6	%LX-300plus_Driver
FIG	UPDATE	2,5	%FP3530_COM_Server_SETUP_2017_10_10v2_0
36dL4.10.TC8DE.WIN	T_15_09_2017	2,4	%PPrintWIN_Install_2017-12-14_v3.1.4-73_arc
BDN	totalcmd	2,30	%FD Init for Cienra_SETUP_2016_01_26v1_0_0_4
KOMUNAL LOTUS	terror	2,3	%PPAK_TZAT700 COM Server_SETUP_2014_04_03
C	legio	2,2	%PL2303_Profific_DriverInstaller_v1190
C_OLP	TARIFF_19_07_2017	2,1	%rec_3
VZ_CPZ	TARIFF_18_10_2017		%advorka_1358356113_638
Find and Mount	TARIFFS_24_03_2017		%OLBP.FOB
7	STRAH_DDV	10_01_2018	%hh400-handheld-scanner-data-sheet-en-a4
54)	SQL		%Acronis True Image 2018 22.5.1 Build 10649 B6
ГЛОБАЛ 11_2018	SPOOLER	INB	%TeamViewer_Setup
_PFUTSZN	spool	32	%Zebras_2018.1
р по нарахуванню	SoftLine	mev	%up020004
упр	SAWP	464644	%TVP_20_01 - 18.02
левина	BT79HOL35	re_ALL	%464644
	RKD		%233333
	REG		%1111111111111111
укаленики	Kammstein (1995-2011) [AAC]	Mount	%kas_rvt
DOK_20_02_2017	RAD Studio 10.1 Berlin bug hotfix collect		%kas_rvt
IT_OLBP	Print_Font	ication	%TMSR03DPM
ТРА	Posting	ing	%111
инкатура_30_12_2017	POSTACH		%STANDARD_OBR
36i индекс Украины	PLAT		%sc
н кас 2017_29.11.2017	PF	loom	%3281280
КАС_38IT_28_02_2018	PENSION_KDO	ON	%ind_NP_10_01_2018
КАС_13_03_2018	PENSION		%3604200000033-100
инкатура_08_12_2017	OLBP_287	m.inf_x86_neutral_S2342F26d70e83	%Книга REG201801
КАС_09_03_2018	elbp		%Bk_new_Tarif_01_01_2018
КАС_28IT_01_03_2018	Obnov_v52_MF2_15.06.2018		%111111
КАС_38IT	NOMEN_KAS_04_06.2018	KCIR_12_2018	%AKH_VZ
знана кас	nomenklat29092017	89102017	%krupt_nrbp
КАС_06_03_2018	nomenklat1102017	шка (2)	%464618
КАС_06_03_2018	nomenclature_08_05_2017	шка	%FTP_LOG
инчук - 23	nomenclature_07_12_2017	LUTD_650	%_FinWinXP
Имя	Тип	Размер	Дата
Оновлення	xlsx		www.root.rar/wwwroot/onlinepayment/*.*
INDEX_NP	txt		Тип Размер Дата
1910171139521156	dbf		<Папка> 21.08.
			<Папка> 01.08.



Alexandr Galushchenko is with Andrii Pertsukh and 3 others.

3 hrs · 🌐

- Что передать мой король?
- Передай твой король мой пламенный привет)

ЦОФ Октябрська	06.09.2018 10:15	Папка с файлами
ПЭС	06.09.2018 10:15	Папка с файлами
ТЕЦ	06.09.2018 10:15	Папка с файлами
Требования к примечаниям	06.09.2018 10:15	Папка с файлами
ПЕС	06.09.2018 10:14	Папка с файлами
ПАТ ДТЕК Дніпрообленерго	06.09.2018 10:14	Папка с файлами
Павлоградуголь	06.09.2018 10:14	Папка с файлами
Павлоградвугілля	06.09.2018 10:14	Папка с файлами
Павлоград 2012г	06.09.2018 10:14	Папка с файлами
Крыменерго	06.09.2018 10:14	Папка с файлами
Октябрьский	06.09.2018 10:14	Папка с файлами
Отчет ОКТЯБРЬСКА ЦЗФ	06.09.2018 10:14	Папка с файлами
Отчет ЦОФОВ	06.09.2018 10:14	Папка с файлами
Крименерго	06.09.2018 10:14	Папка с файлами
Киевэнерго	06.09.2018 10:14	Папка с файлами
Консультації	06.09.2018 10:14	Папка с файлами
Западенерго	06.09.2018 10:14	Папка с файлами
Київенерго	06.09.2018 10:14	Папка с файлами
ДТЕК Шахта Комсомолец Донбасса	06.09.2018 10:14	Папка с файлами
ДТЭК КРЫМЭНЕРГО	06.09.2018 10:14	Папка с файлами
ДТЕК ЦОФ Октябрська	06.09.2018 10:14	Папка с файлами

Аудиторська
компанія



Sean Brian Townsend added 3 new photos.

5 hrs · Kyiv · 🌐



Дмитрий Орлов прислал свежую порцию "открытых данных" для вечнонеунывающей рубрики [#FuckResponsibleDisclosure](#). В этот раз попался ПАО "Завод Маяк". Там делают стрелковое оружие, завод входит в [Державний концерн "Укроборонпром"](#). И что тут такого? Всего-то чертежи новых оборонных разработок, заказы, договора на поставку комплектующих. Листайте дальше.

Особого цинизма добавляет то, что Укроборонпром является инициатором амбициозных проектов в области безопасности - киберцентра который уже не взлетел и баг-баунти программы, которая ещё не взлетела. Хотел бы попросить господ советников уделить немного внимания собственному концерну, а то и чем черт не шутит потратить пару монеток.

А пока все данные переданы [The S](#)

[See Translation](#)

**Завод «Маяк»:
open network**

Вводные

Заводу «Маяк» необходимы стволы для производства стволов с целью установки в собственные винтовки. Заводу «Маяк» также может потребоваться локализация производственного процесса в собственной компании в последующие годы.

Заводу «Маяк» необходимо начать получать стволы в сентябре.



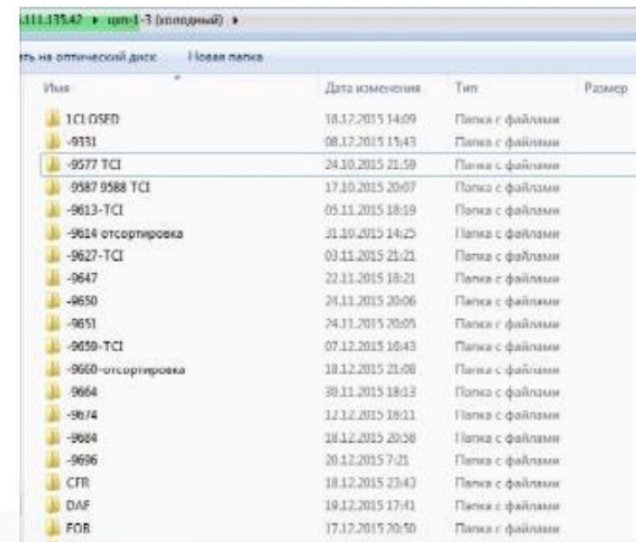
Sean Brian Townsend added 2 new photos — with Jeffrey Dahmer and Andrii Pertsikh.

November 22, 2017 · Kyiv · 🌐



Часто в ответ на [#FuckResponsibleDisclosure](#) мы получаем комментарии, что всё - из-за низких зарплат в государственном секторе. Я думаю, что в [Метінвест](#) зарплаты выше, но деньги пофигизм не лечат. В самом деле, зачем хакерам металлургический завод? [ОАО «Запорожсталь»](#) Очень скучно, очень. Лучше сразу стать сельскохозяйственной сверхдержавой. (И если вы не знали, сельское хозяйство - это тоже хайтек на самом деле)

See Translation **Метінвест, Запорожсталь**



Имя	Дата изменения	Тип	Размер
TCI OSD	18.12.2015 14:09	Папка с файлами	
-9131	08.12.2015 15:43	Папка с файлами	
-9577 TCI	24.10.2015 21:59	Папка с файлами	
9587 9588 TCI	17.10.2015 20:07	Папка с файлами	
-9613-TCI	05.11.2015 18:19	Папка с файлами	
-9614 отсортировка	31.10.2015 14:25	Папка с файлами	
-9627-TCI	03.11.2015 21:21	Папка с файлами	
-9647	22.11.2015 18:21	Папка с файлами	
-9650	24.11.2015 20:06	Папка с файлами	
-9651	24.11.2015 20:05	Папка с файлами	
-9659-TCI	07.12.2015 16:43	Папка с файлами	
-9660-отсортировка	18.12.2015 21:08	Папка с файлами	
9664	30.11.2015 18:13	Папка с файлами	
-9674	12.12.2015 18:11	Папка с файлами	
-9684	18.12.2015 20:58	Папка с файлами	
-9696	20.12.2015 7:21	Папка с файлами	
CGI	18.12.2015 23:43	Папка с файлами	
DAF	19.12.2015 17:41	Папка с файлами	
FOR	17.12.2015 20:50	Папка с файлами	





Андрей Перевезий is with Sean Townsend and 5 others.

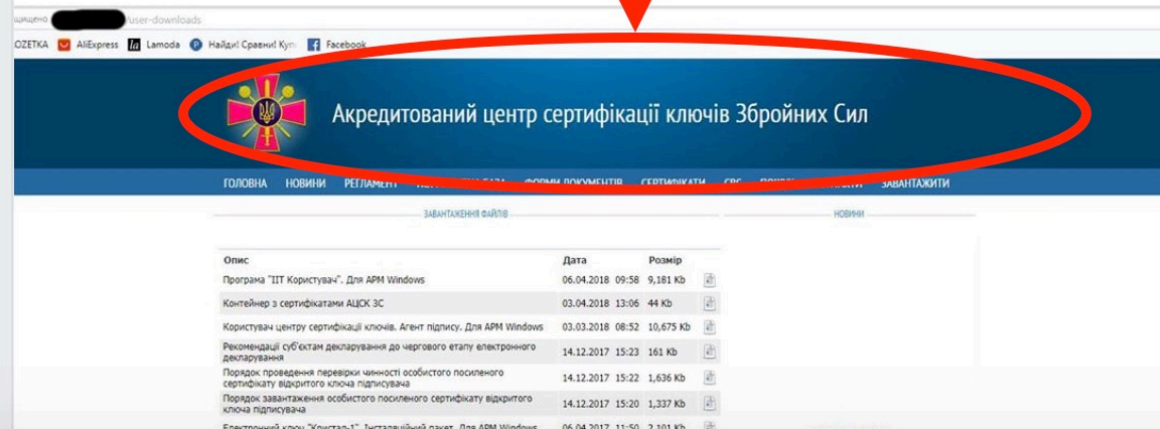
9 hrs · 🌐

Когда я показал, то что сейчас опубликовано Andrii Pertsyukh сказал только одно слово б...дь. Предлагаю всем ознакомиться с инсталями электронных ключей, которые используются в Мин Обороны. Информация находится в открытом доступе (честно сложно комментировать причины), но это как бы фигня. Уважаемые коллеги, комьюнити, давайте скинемся Мин Обороны на <https://>, по баксу с профиля, лет на 10 Comodo купим))))

На самом деле, вопрос, зачем это выкладывать в открытом доступе у меня до сих пор висит, тем более выкладывать pdf, где написан локальный IP системы "Дніпро" Сергій Дяченко может я чего то не знаю?

Міністерство оборони:
#паровозикоблачко #RFD

P.S. Ну и если кто то хочет почитать почту, тоже милости просим.





Sean Brian Townsend

October 14, 2017 · Kyiv · 🌐

...

Зайчики из МВД, которые оставили сетевой диск без пароля в Интернет – это [Національна академія внутрішніх справ](#). Прекрасных людей и замечательных специалистов мне показал один из френдов (Я упомяну по имени, если захочешь. Я тебе еще об этом не говорил, но ты блестяще работаешь! 😊)

Я сейчас объясню что нарисовано на картинке. Во-первых, это просто виндовая шара, и вы могли бы подключить её тоже, если бы знали IP. Во-вторых, на ней мы видим несколько дампов баз данных – полный список машин из внутренней сети, база сайта (вместе с паролями), список студентов (285 офицеров до полковников включительно)

Интереснее всего файлы .SO – это огрызок от эксплоита [#SambaCry](#). Сервер многократно был взломан другими хакерами за последние полгода. После Непети и всех предупреждений! И наконец, на картинке этого нет, но сервер так же отдаёт список рабочих групп, включая бухгалтерию и комендатуру.

[Andrii Pertsukh](#) уже написал в [CERT-UA](#), а я в [The Security Service of Ukraine](#). Не знаю, кто добрался туда быстрее, но сегодня "сервис" потух. Я вот что хочу спросить. Ребята из Академии, я уже могу публиковать хеши ваших паролей, имена и адреса машин? Вы же приготовились? У вас я слышал специальные "чемоданчики" есть?

Disclaimer. Внимание! Трюк выполнен опытным каскадером. |

● Chat (19)

A	B	C	D	E	F	G	H	I	K	L
			УКРІНМАШ							
MF/MIM	Название детали	№	Имя файла	Цена детали	Цена пресс-формы	Цена механической обработки	Стоимость режущих инструментов для обработки детали	Уточнение размеров на чертеже (SI - ДА, NO - НЕТ)	Срок изготовления формы	Срок изготовления образцов
-		1	.. №034 Bend "П01.00.00.001 Гнеток".							
-		2	.. №035 Feed Lever Axis "П01.00.00.002 Ось Рычага Подачи".							
MF	S-3408	3	.. №037 Receiver Base "П01.00.00.005 Основание Приемника".							
-		4	.. №038 Limiter Of Contactor "П01.00.00.006 Ограничитель Замыкателя							
MIM	S-3373	5	.. №040 Recharge Handle "П01.02.00.001 Рукоятка Перезаряджания".							
-		6	.. №041 Sleeve "П01.02.00.003 Втулка".							
-		7	.. №045 Recharging Arm Base "П01.02.00.009 Основание Р. Перезар."							
MIM	S-3374	8	.. №048 Reflector "П01.02.01.009 Отражатель".							
MIM	S-3375	9	.. №058 Feed Lever Base "П01.02.01.106 Основание Рычага Подачи".							
MIM	s-3318	10	.. №059 Feed Lever Base "П01.02.01.107 Основание Рычага Подачи".							
MIM	S-3386	11	.. №063 Rusk "П01.02.01.202 Сухарь".							
MF	S-3315	12	.. №067 Frame "П01.03.01.001 Рама".							
-		13	.. №069 Rod "П01.03.01.004 Шток".							
MIM	S-3376	14	.. №071 Extractor "П01.03.01.006 Извлекатель".							
MF	S-3316	15	.. №072 Shutter "П01.03.02.001 Затвор".							
MIM	S-3377	16	.. №073 Hammer "П01.03.02.002 Ударник".							
MIM	S-3319	17	.. №074 Ejector "П01.03.02.003 Выбрасыватель".							
-		18	.. №076 Ejector Shaft "П01.03.02.005 Ось Выбрасывателя".							
-		19	.. №077 Ejector Shaft Pin "П01.03.02.006 Штифт Оси Выбрасывателя".							
		20	.. №081 Shaft Nut "П01.04.00.004 Гайка Стенжня".							

Укрінмаш:
open network

Минэнергоуголь Украины

ГП «НАЭК «Энергоатом»

ОП «Южно-Украинская АЭС»

Химический цех

УТВЕРЖДАЮ

Главный инженер

_____ Н.А. Феофен-
тов

" 26 " 04 2017 г.

АКТ №АК 3.0014.6712 от 20.04.2017г.
по результатам контроля коррозионного состояния внутренних поверхностей
парогенераторов 3УВ10-40W1 энергоблока №3 со стороны второго контура
в период останова на ППР-2017

Объект контроля: парогенератор 3УВ10-40W1 энергоблока №3 ОП ЮУ-
АЭС.

Дата проведения: 1.04.2017г.

Рабочие документы:

1. Парогенератор ПГВ-1000 М 1.0001-044ТО. Техническое описание;
2. ГНД 05.11.05.044-99 «Методика определения степени загрязненности поверхностей парогенераторов ПГВ-1000 М со стороны второго контура»;
3. ИН.0.0014.0138 «Коррозионный осмотр технологического оборудования. Инструкция»;
4. МТ.0.0014.0062 «Методы анализа отложений на поверхности технологического оборудования АЭС. Сборник»;
5. ПМ.3.0014.0062 «Рабочая программа коррозионного обследования металла основного и вспомогательного оборудования энергоблока №3 в период ППР-2017г.»

Средства измерения и испытательное оборудование:

1. Колориметр фотоэлектрический КФК-2 зав. № 8702570;
2. Муфельная печь СНОЛ 1,6.2,5.1/11-И2 зав. №.16492;
3. Весы АВГ220WPO, зав. №.650290.

Выполнен контроль:

1. Коррозионного состояния со стороны второго контура, в доступных местах:
 - поверхности металла корпусов и коллекторов парогенераторов 3УВ10-40W01, с отбором проб отложений;

Most popular vulnerabilities:

- ▶ Open network disk, without password
- ▶ XSS
- ▶ Outdated CMS
- ▶ Web-servers without updates + plenty of vulnerabilities
- ▶ Old web sites' versions on sub-domains .gov.ua
- ▶ SQLi
- ▶ HTTP instead of HTTPS



Outstanding #FRD activists

Sean Brian Townsend

Дмитрий Орлов

Jeoffrey Dahmer

Yehor Papyshev

Andrii Pertsuikh

Kir Vaznitsky

Сергій Дяченко

Aleksandr Galushchenko

Андрей Перевезий

Дякую!

‘National Cybersecurity System’

Seven public authorities are responsible for National Cybersecurity System:

- ▶ РНБО, National Security and Defense Council. coordinator
- ▶ Держспецзв’язку, SSSCIP
- ▶ СБУ, Security Service of Ukraine
- ▶ Кіберполіція, CyberPolice
- ▶ НБУ, National Bank of Ukraine
- ▶ Міністерство оборони/ГШ ЗСУ, Ministry of Defense, General Staff
- ▶ Розвідувальні органи, Intelligence Agencies

Three of them are objects of #FRD

Other ones are potential objects

‘National Cybersecurity System’: money

- ▶ \$125 million per year for SSSCIP
- ▶ SSU: \$17 million
- ▶ CyberPolice: \$700k
- ▶ NBU, MoD, Intel: N/A

Total: ? ? ? ? ?

On National Cybersecurity System in details:

UISGCON14, Костянтин Корсун,
Система кібербезпеки України -
реальність чи міф?

<https://www.youtube.com/watch?v=HerX0DDEaFs&t=9s>

UISGCON14 Костянтин Корсун, Система кібербезпеки України - реальність ...

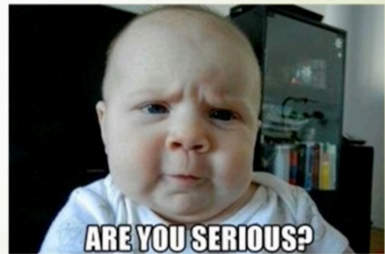
National cybersecurity system: the Plan

План заходів на 2018 рік з реалізації Стратегії кібербезпеки України (Затверджено Розпорядженням КМУ від 11 липня 2018 р. № 481-р)

Планом передбачено 27 пунктів плану, з яких:

- ні про що:	2
- неефективні:	11
- важко виконати/шкідливі:	3
- корупційні:	3
- більш-менш корисні:	10

Positive Efficiency: ~ 37%



UISGCON14
THE BIRTHPLACE OF UKRAINIAN CYBERSECURITY
26 жовтня 2018 / Київ, Україна

10:19 / 51:42

#FRD consequences

Tactical effects:

Resonance in media

Discharges

Budgets for cybersecurity

Growing interest to cybersec industry

Increasing number of professional certificates

Better cooperation of Gov and Private sectors

Is it objective or subjective?

23 Ukrainian cybersecurity Top-experts have been inquired.

#FRD consequences

Who are those 23 experts?

- ▶ 5 work at Gov sector
- ▶ 14 work at Private sector
- ▶ 4 independent experts (freelance, journalist)
- ▶ 8 work at critical infrastructure objects
- ▶ 2 females, 21 males
- ▶ No one is #FRD activist
- ▶ No one from CyberPolice

#FRD consequences

- ▶ 1. *Do you believe that since 2014 cybersecurity level in Ukraine has been increased?*
- ▶ 2. *If so, has #FuckResponsibleDisclosure initiative influenced on it?*
- ▶ 3. *What factors in your opinion have influenced on current cybersecurity level in Ukraine the most?*

1. Чи вважаєте Ви, що протягом останніх років (з 2014 по тепер) рівень *

☐ Так

☐ Ні

☐ Other...

2. Якщо так, то чи вплинула на це ініціатива #FuckResponsibleDisclosure? *

☐ Так

☐ Ні

☐ Other...

3. На Вашу думку, які внутрішні фактори найбільше вплинули на *

Long answer text

#FRD consequences

Question 1: *Do you believe that since 2014 cybersecurity level in Ukraine has been increased?*

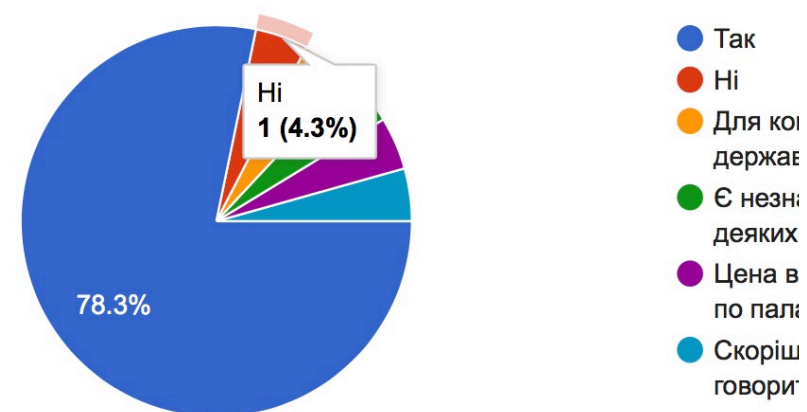
YES: 78,3%

NO: 4,3%

Other: 17,4%

1. Чи вважаєте Ви, що протягом останніх років (з 2014) рівень кібербезпеки України покращився?

23 responses



#FRD consequences

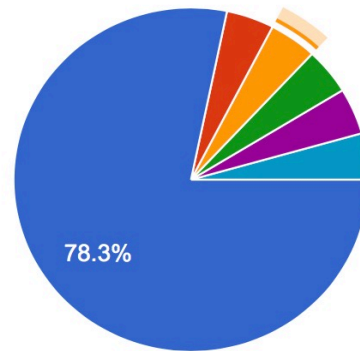
Question 1: *Do you believe that since 2014 cybersecurity level in Ukraine has been increased?*

For commercial sector: Yes

For Governmental sector: don't think so

1. Чи вважаєте Ви, що протягом останніх років (з 2014 по тепер) рівень кібербезпеки України покращився?

23 responses



- Так
- Ні
- Для комерційного сектора - так, для державного - немає відчуття покращення
- Є незначні несистемні зміни у
- Для комерційного сектора - так, для державного - немає відчуття покращення
- Державний сектор середньої температури по палаті... Якщо брати окремі ак...
- Скоріше так, ніж ні. Не можна говорити, що рівень лишився тим...

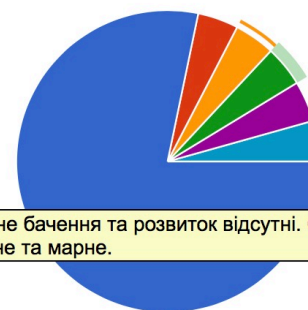
#FRD consequences

Question 1: *Do you believe that since 2014 cybersecurity level in Ukraine has been increased?*

Changes are insignificant,
in some organizations only

1. Чи вважаєте Ви, що протягом останніх років (з 2014 по тепер) рівень кібербезпеки України покращився?

23 responses



Так

Ні

Для комерційного сектора - так, для державного - немає відчуття покращення

Є незначні несистемні зміни у деяких установах. Системне бачення та розвиток відсутні. Оновлення нормативних документів не відбулося. Як і раніше спеціалісти мають обирати між складним вибором: ефективне але незаконне або законне та марне.

Ціна вимір середньої температури

Скоріше так, ніж ні. Не можна говорити, що рівень лишився тим самим

Немає відповіді

#FRD consequences

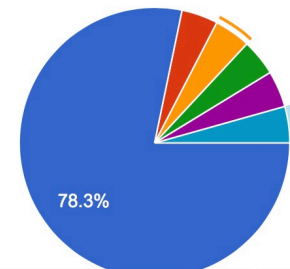
Question 1: *Do you believe that since 2014 cybersecurity level in Ukraine has been increased?*

Rather yes then no.

Cybersecurity level in Governmental/state organization has been increased unessentially

1. Чи вважаєте Ви, що протягом останніх років (з 2014 по тепер) рівень кібербезпеки України покращився?

23 responses



- Так
- Ні
- Для комерційного сектора - так, для державного - немає відчуття покращення
- Є незначні несистемні зміни у деяких установах. Системне бачення відсутнє
- Ціна вимір середньої температури по палаті... Якщо брати окремі акції
- Скоріше так, ніж ні. Не можна говорити, що рівень лишився тим самим, адже багатох "клієнтів смажений півень". Якщо говорити про рівень кібербезпеки держустанов, то, імовірно, він змінився не суттєво, а якщо і покращився, то завдяки "наганяю зверху", а не ініціативі власне держустанов.

Скоріше так, ніж ні. Не можна говорити, що рівень лишився тим самим, адже багатох "клієнтів смажений півень". Якщо говорити про рівень кібербезпеки держустанов, то, імовірно, він змінився не суттєво, а якщо і покращився, то завдяки "наганяю зверху", а не ініціативі власне держустанов.

#FRD consequences

Question 2: *If so, has #FuckResponsibleDisclosure initiative influenced on it?*

Yes: 34,7%

No: 13%

It influenced partially: 21,5%

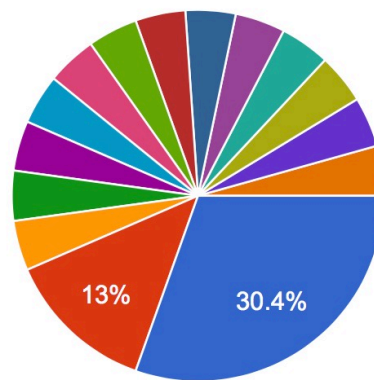
Influence was minor/moderate: 12,9%

I haven't heard on #FRD: 12,9%

I can't say definitely: 5%

2. Якщо так, то чи вплинула на це ініціатива #FuckResponsibleDisclosure?

23 responses



- Так
- Ні
- Внесок #FRD є, але він не такий...
- Не чув
- Вплив був помірний
- Будь яка ініціатива впливає, тому...
- І так, і ні. Деяки компанії, що мал...
- Скоріше - ні, ніж - так. Був певний...

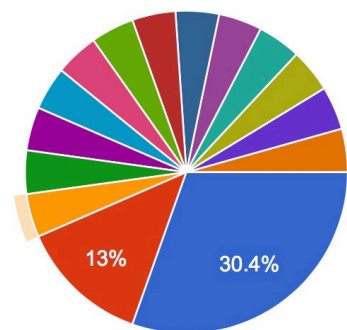
#FRD consequences

Question 2: *If so, has #FuckResponsibleDisclosure initiative influenced on it?*

#FRD contribution was minor

2. Якщо так, то чи вплинула на це ініціатива #FuckResponsibleDisclosure?

23 responses



- Так
 - Ні
 - Внесок #FRD є, але він не такий...
 - Не чув
 - Вплив був повний
 - Будь яка ініціатива впливає, тому...
 - І так, і ні. Деякі компанії, що мал...
 - Скоріше - ні, ніж - так. Був певний...
- Внесок #FRD є, але він не такий суттєвий, як реальних кібератак, особливо, масштабу країни.

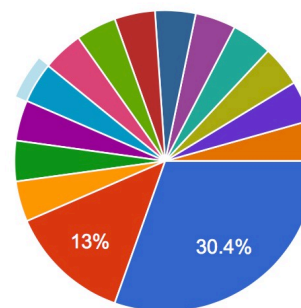
#FRD consequences

Question 2: *If so, has #FuckResponsibleDisclosure initiative influenced on it?*

Any initiative influences but I can't say how strong

2. Якщо так, то чи вплинула на це ініціатива #FuckResponsibleDisclosure?

23 responses



- Так
- Ні
- Внесок #FRD є, але він не такий...
- Не чув
- Вплив був помірний
- Будь яка ініціатива впливає, тому...
- І так, і ні. Деяки компанії, що мал...
- Скоріше ні, ніж так

1/2

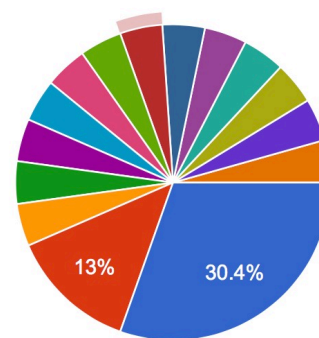
#FRD consequences

Question 2: *If so, has #FuckResponsibleDisclosure initiative influenced on it?*

I can't be sure however probably the initiative influenced on cyber awareness

2. Якщо так, то чи вплинула на це ініціатива #FuckResponsibleDisclosure?

23 responses



Не впевнена, але ця ініціатива вплинула на обізнаність. Будем с...

Не впевнена, але ця ініціатива вплинула на обізнаність. Будем сподіватись, що це трансформується в покращення безпеки:)

Не чув про таке

Як визнає сам Шон, ФРД не зміни...

Так, вплинула. Це гарна ініціатив...

Частково

▲ 2/2 ▼

#FRD consequences

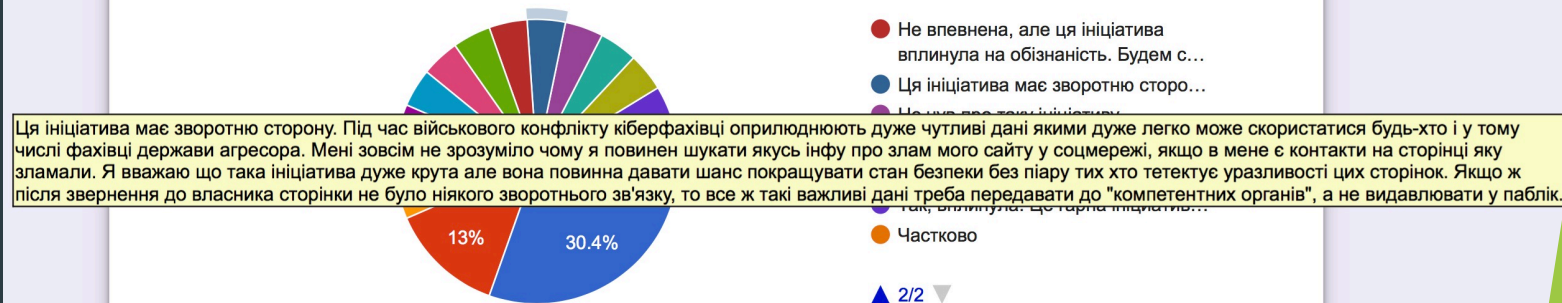
Question 2: *If so, has #FuckResponsibleDisclosure initiative influenced on it?*

The initiative has an opposite side: our country is in war any the adversary could use revealed vulnerabilities.

If an owner of vulnerable resources doesn't response it would be better to let LEs know, not sharing in public.

2. Якщо так, то чи вплинула на це ініціатива #FuckResponsibleDisclosure?

23 responses



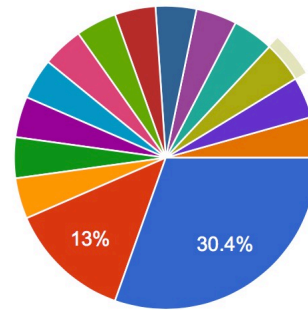
#FRD consequences

Question 2: *If so, has #FuckResponsibleDisclosure initiative influenced on it?*

#FRD's initiative influenced inessentially, and Sean admitted that

2. Якщо так, то чи вплинула на це ініціатива #FuckResponsibleDisclosure?

23 responses



- Не впевнена, але ця ініціатива вплинула на обізнаність. Будем с...
- Ця ініціатива має зворотню сторо...
- Не чув про таку ініціативу
- Не чув про таке
- Як визнає сам Шон, ФРД не зміни...
- Так, вплинула. Це гарна ініціатив...

Як визнає сам Шон, ФРД не змінила на краще ситуацію. Особисто моя думка - вплив цей, попри все, несуттєвий.

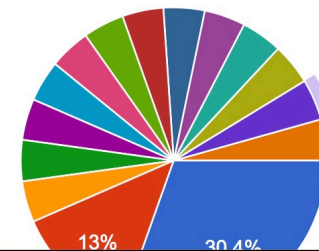
#FRD consequences

Question 2: *If so, has #FuckResponsibleDisclosure initiative influenced on it?*

Yes, #FRD has influenced.
And this initiative must be used in
upcoming Law on Cybersecurity in
Ukraine

2. Якщо так, то чи вплинула на це ініціатива #FuckResponsibleDisclosure?

23 responses



- Не впевнена, але ця ініціатива вплинула на обізнаність. Будем с...
- Ця ініціатива має зворотню сторо...
- Не чув про таку ініціативу
- Не чув про таке
- Як визнає сам Шон, ФРД не зміни...
- Так, вплинула. Це гарна ініціатив...
- Частково

Так, вплинула. Це гарна ініціатива, але шкода, що поки не змогли використати її для "легалізації" відкритих офіційних програм пошуку вразливостей для держ органів на платформах із тисячами спеціалістів, за прикладом США та ЄС. Думаю, існуючим досвідом потрібно буде все ж скористатись при написанні закону про кібербезпеку.

#FRD consequences

3. What factors in your opinion have influenced on current cybersecurity level in Ukraine the most?

NotPetya and most known cyberattacks

Why #FRD occurred?

3. На Вашу думку, які внутрішні фактори найбільше вплинули на поточний стан кібербезпеки України?

23 responses

Підвищення обізнаності збільшення фінансування (переважно у державному секторі).

Активна співпраця із міжнародними партнерами, свіжа Стратегія і Доктрина

відсутність спільної позиції між суб'єктами кіберпростору, застаріла регуляція, відсутність достатньої кількості кадрів для внутрішнього ринку ,

Я бачу вплив тільки зовнішніх факторів. Не бачу внутрішніх нажаль. Навіть FRD дав поштовх для комерції більш ніж для держ установ (ІМНО)

Галузева регуляція, приватно- державне партнерство

Я не бачи системи. Мені здається, що це просто повільна еволюція. Навіть атака Петі Непеті не вплинула на кіберзахист. Під егідою захисту обираються досить безглузді кроки та втілюються у життя.

Впровадження Іт-систем

Патріотизм, небайдужість і набутий останніми роками досвід та професіоналізм окремих як посадовців так і причетних до сфери членів громадського суспільства

кібер-атака на ЦВК в 2014 році та кібер-атака NotPetya 2017 року

атака на обленерго в 2016 році, атака нотПетя в 2017 році

#FRD consequences

3. *What factors in your opinion have influenced on current cybersecurity level in Ukraine the most?*

What #FRD has led to?

Western Partners: not inner factor

3. На Вашу думку, які внутрішні фактори найбільше вплинули на поточний стан кібербезпеки України?

23 responses

З позитивного - складається враження, що коло спеціалістів і співчуваючих розширилось, підтянулись суміжні сфери: юристи наприклад. З негативного і очевидного - бажання витратити кошти на технічні засоби, ніж на навчання спеціалістів.

Я вважаю, що на стан кібербезпеки повинен впливати в першу чергу Голова будь-якої організації. Зараз дуже мало компетентних керівників які усвідомлено роблять кроки у підсиленні кібербезпеки своїх організацій. Якщо казати про те що впливає на стан, то це:

- нормативна база, стандарти. Дуже показова нормативна від НацБанку. На рівні держави дуже повільний розвиток. Багато робиться з боку Держави щодо побудови CSIRTів, але бюрократія все нівелює...;
- спеціалізовані ком'юніті, спеціалізовані конференції (uisgcon, defcon, nonamecon, owaspcn, bsides, idc, pubkey, skynet,...);
- діяльність ентузіастів;
- зрілі організації, які купують послуги вітчизняних компаній і тим самим стимулюють розвиток вітчизняних надавачів послуг без витоку мозку за кордон (статистика clutch).

Бюрократический государственный аппарат

NotPetya

Розуміння, що кібербезпека це не щось віртуальне і далеке. В країні війна і потрібні реальні/комплексні кроки щодо побудови системи кіберзахисту в Україні. Важливе питання просвітництва і популяризації питань кібербезпеки. Заходи починати потрібно майже з дитячого садка!

#FRD consequences

3. What factors in your opinion have influenced on current cybersecurity level in Ukraine the most?

No 'inner factors' or 'can't say' - honest answers

Only one hint at #FRD

3. На Вашу думку, які внутрішні фактори найбільше вплинули на поточний стан кібербезпеки України?

23 responses

NotPetya

Розуміння, що кібербезпека це не щось віртуальне і далеке. В країні війна і потрібні реальні/комплексні кроки щодо побудови системи кіберзахисту в Україні. Важливе питання просвітництва і популяризації питань кібербезпеки. Заходи починати потрібно майже з дитячого садка!

Страх наслідків NotPetya & FRD

Великі гучні інциденти + медійна поширеність теми, а також відомість кремлівських хакерів у країні та світі

Публічне висвітлення недостатнього рівня технічного захисту державних інформаційних ресурсів.

винесення питання про незахищеність держ ресурсів у публічну площину та збільшення фінансування

підвищення фінансування кібербезпеки, підвищення уваги вищого керівництва до цього питання, навчання, підвищення рівня зарплатні спеціалістів, вірус Петя

Важко відповісти.

Євроінтеграція, підтримка Партнерів та їх вимоги. Сподіваюсь це і надалі буде позитивно впливати на розвиток галузі. Людський фактор та залученість спільноти до процесів.

"Петя" (якщо його можна вважати "внутрішнім фактором")

#FRD consequences

So 23 best Ukrainian Cybersecurity experts believe that:

Cybersecurity level in Ukraine has increased:
78,3%

#FRD influenced on that significantly or partially:
56,2%

BUT

#FRD was not a determined factor of that growth



Conclusions

Question to myself:

Main inner driver was marginal and hasn't influenced whole country's cybersecurity significantly?

Massive cyberattacks were a main driver?

#FRD is important initiative, but not enough effective?

Any other idea?



Conclusions

- ▶ #FRD is necessary and helpful
- ▶ #FRD is not enough to influence whole country
- ▶ #FRD needs to be changed; however it wouldn't be #FRD
- ▶ Government should do what #FRD does; but actually they don't.

#FRD is something bright, emotional, scandal, patriotic.

Thank you, #FRD





Have we a
time for
Q&A session?



Thank you!

Please reach me out:
kos@berezhasecurity.com
<https://berezhasecurity.com>