

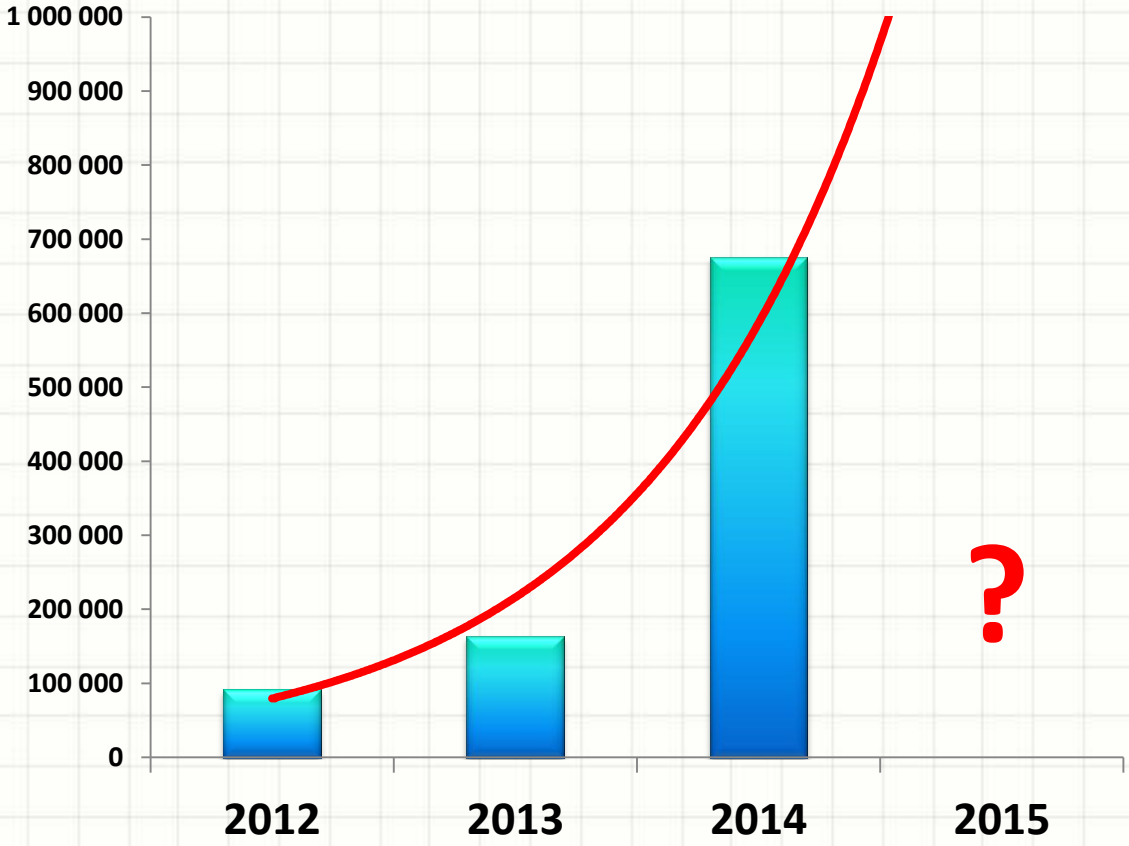
Проблемы верификации и устранения найденных критических уязвимостей систем управления электросетевым комплексом

к.т.н., М.В. НИКАНДРОВ

iGRIDS
Интеллектуальные Сети

Рост количества атак на АСУ ТП

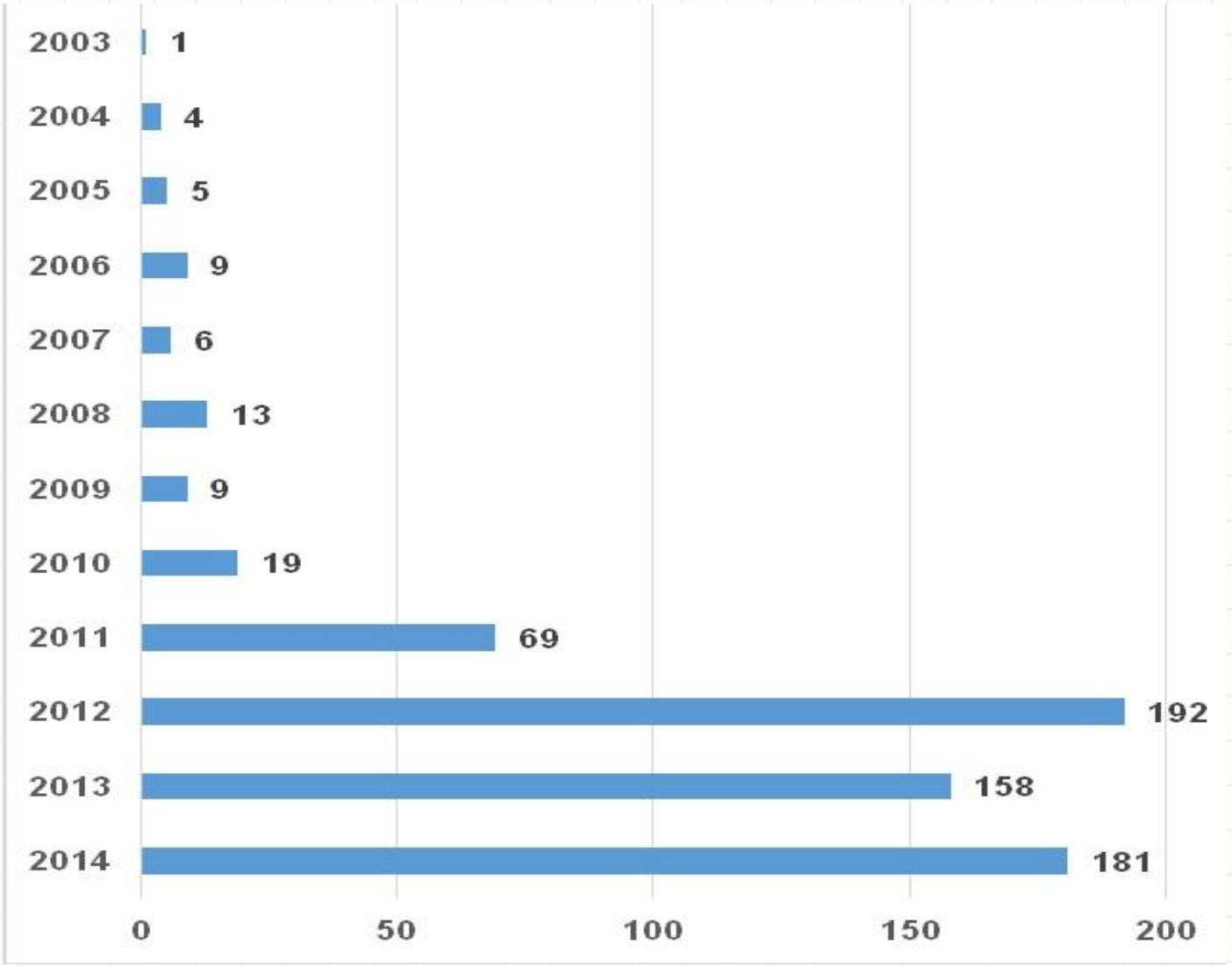
4-х кратный рост количества атак на АСУ ТП в 2014 г.



Отчет «2015 Dell Security Annual Threat Report»

https://software.dell.com/docs/2015-dell-security-annual-threat-report-white-paper-15657.pdf

Рост количества найденных уязвимостей



Отчет Positive Technologies «Безопасность промышленных систем в цифрах» 2015 г.

ProductCERT Security Advisories

Siemens ProductCERT is the central team for responding to potential security incidents and vulnerabilities related to Siemens products, solutions and services. In the following, Siemens security advisories and bulletins issued by ProductCERT are listed.

2015

- SSA-720081 (Last Update 2015-09-01): IP Forwarding in RUGGEDCOM ROS-based Devices
- SSA-134003 (Last Update 2015-08-27): Web Vulnerability in S7-1200
- SSA-504631 (Last Update 2015-08-04): Incorrect Certificate Validation in COMPAS Mobile App
- SSA-267489 (Last Update 2015-07-21): Vulnerability in Android App Sm@rtClient
- SSA-396873 (Last Update 2015-07-21): TLS Vulnerability in Ruggedcom ROS- and ROX-based Devices
- SSA-732541 (Last Update 2015-07-17): Denial-of-Service Vulnerability in SIPROTEC 4
- SSA-632547 (Last Update 2015-07-14): Authentication Bypass Vulnerability in SICAM MIC
- SSA-142512 (Last Update 2015-06-25): Cross-Site Scripting Vulnerability in Climatix BACnet/IP Communication Module
- SSA-311412 (Last Update 2015-05-04): Incorrect Certificate Verification in Android App HomeControl for Room Automation
- SSA-237894 (Last Update 2015-09-28): Vulnerability in SIMATIC PCS 7
- SSA-487246 (Last Update 2015-08-27): Vulnerabilities in SIMATIC HMI Devices
- SSA-994726 (Last Update 2015-04-22): GHOST Vulnerability in Siemens Industrial Products
- SSA-335471 (Last Update 2015-03-05): Denial-of-Service Vulnerability in SPC Controller Series
- SSA-451236 (Last Update 2015-04-22): Vulnerability in SIMATIC ProSave, SIMATIC CFC, SIMATIC STEP 7, SIMOTION Scout, and STARTER
- SSA-987029 (Last Update 2015-03-05): Denial-of-Service Vulnerability in S7-300
- SSA-185226 (Last Update 2015-03-05): Vulnerabilities in App SPCanywhere
- SSA-749212 (Last Update 2015-03-05): NTP Vulnerabilities in SINUMERIK Controllers
- SSA-315836 (Last Update 2015-08-27): Vulnerabilities in SIMATIC STEP 7 (TIA Portal) V12 and V13
- SSA-543623 (Last Update 2015-02-13): Vulnerabilities in SIMATIC WinCC (TIA Portal) V13
- SSA-234789 (Last Update 2015-02-13): Vulnerabilities in SIMATIC STEP 7 (TIA Portal) V13
- SSA-753139 (Last Update 2015-02-03): Vulnerabilities in Ruggedcom WIN Products
- SSA-954136 (Last Update 2015-02-02): User Impersonation Vulnerability in SCALANCE X-200IRT Switch Family
- SSA-597212 (Last Update 2015-01-21): Web Vulnerability in SIMATIC S7-1200
- SSA-321046 (Last Update 2015-01-19): Denial-of-Service Vulnerabilities in SCALANCE X-300/X408 Switch Family
- SSA-671683 (Last Update 2015-03-05): NTP Vulnerabilities in Ruggedcom ROX-based Devices
- SSA-311299 (Last Update 2015-01-13): Vulnerabilities in iOS App SIMATIC WinCC Sm@rtClient

Электроэнергетика на «передовой»

Половина найденных уязвимостей относится к автоматизации электроэнергетического оборудования

Что делать с уязвимостями ?

1. Поиск уязвимостей
2. Верификация и тестирование
3. Устранение

Поиск уязвимостей

1. Международные и национальные банки данных угроз и уязвимостей

2. Поиск уязвимостей, тестирование, honey pot, CTF…

3. Bug Bounty

4. Обязать проводить тестирование

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

Верификация и тестирование

Испытательные полигоны

KEMA

Евросоюз, лаборатория в Нидерландах
«The KEMA Laboratories Flex Power Grid Lab»

США, Национальная лаборатория в Айдахо, Idaho National Laboratory
«National SCADA Test Bed Program»

Проблемы устранения уязвимостей

1. Нельзя вывести оборудование из эксплуатации
2. Устранять некем
3. Возможно повреждение оборудование
4. Иногда, устранить невозможно

Устранение выявленных критических уязвимостей

Какие варианты действий возможны для устранения опасных уязвимостей, тех, которые потенциально могут привести к снижению общей надежности и потери части функционала

№	Вариант действий	Результаты опроса
1	Ничего не делать, блокировать распространение информации об уязвимости	0%
2	Уязвимость не устранять, минимизировать эксплуатацию данной уязвимости средствами системы кибернетической защиты	56%
4	Обязать производителя оборудования (поставщика, эксплуатацию) устранить найденные уязвимости во время очередных регламентных работ на объектах	33%
5	Обязать производителя оборудования (поставщика, эксплуатацию) устранить найденные уязвимости в строго регламентированные сроки, оборудование выводить из работы внепланово	11%

Устранение выявленных критических уязвимостей

Какие варианты действий возможны для устранения критических уязвимостей, тех, которые потенциально могут привести к неприемлемому ущербу

№	Вариант действий	Результаты опроса
1	Ничего не делать, блокировать распространение информации об уязвимости	0%
2	Уязвимость не устранять, минимизировать эксплуатацию данной уязвимости средствами системы кибернетической защиты	36%
3	Информирование организации, рассылка циркуляров в целях не допущения в закупках нового оборудования с известными уязвимостями	8%
4	Обязать производителя оборудования (поставщика, эксплуатацию) устранить найденные уязвимости во время очередных регламентных работ на объектах	15%
5	Обязать производителя оборудования (поставщика, эксплуатацию) устранить найденные уязвимости в строго регламентированные сроки, оборудование выводить из работы внепланово	15%
6	Провести превентивные меры, возможно, разумная деградация системы и утрата части функционала, обязать производителя (поставщика, эксплуатацию) устранить найденные уязвимости в строго регламентированные сроки	29%

Выводы

- Необходимы полигоны испытаний и лаборатории по проведения тестов на не декларируемые возможности с учетом кибер-физических моделей
- В большинстве случаев устранить уязвимости на работающих объектах проблематично, следует направить усилия на недопущение на объекты оборудования с уязвимостями, для этого ввести обязательное тестирование оборудования и другие мероприятия снижающие вероятность поставки на объекты не проверенного оборудования
- Необходимо внедрять объектовые системы кибернетической защиты

Спасибо за внимание!

iGRIDS
Интеллектуальные Сети

ООО «Интеллектуальные Сети»
Никандров Максим
nikandrov@igrids.ru