РОСЭНЕРГОАТОМ
ВНИИАЭС

Вопросы
кон^{111}фид$_{000}$енц^{111}иал$_{000}$ьно^{111}сти$_{000}$
в АСУ ТП

2017.05.11, ИПУ РАН

Сидоров Илья

Password:

Cancel

Sign In

ЗАДАЧА

Область задач презентации

РОСЭНЕРГОАТОМ ВНИИАЭС

Вопросы:

- Конфиденциальности нет?
- Конфиденциальность = 0?
- Конфиденциальность не нужна?
- Конфиденциальностью можно пренебречь?

В область задач данной презентации НЕ входят:

- выбор/сравнение/анализ защитных мер.

ТЕОРИЯ

Определение конфиденциальности

РОСЭНЕРГОАТОМ ВНИИАЭС

1

Конфиденциальность информации:

обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

2

Конфиденциальная информация (sensitive information):

информация, требующая защиты.

[1] ФЗ 149-2006, 2006, "Об информации, информационных технологиях и о защите информации";
[2] "Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения". Утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.

Определение конфиденциальности

РОСЭНЕРГОАТОМ ВНИИАЭС

1

2

Конфиденциальность:

свойство, в силу которого информация
не предоставляется и не раскрывается по запросам
не имеющих разрешения лиц, объектов или процессов.

3

4

Confidentiality:

The property that information is
not made available or disclosed to unauthorized individuals,
entities or processes.

[1] IEC 62645:2014, 2014, Edition 1, "Nuclear power plants - Instrumentation and control systems - Requirements for security programmes for computer-based systems".
[2] IEC/PAS 62443-3:2008, 2008, Edition 1, "Security for industrial process measurement and control - Network and system security".
[3] IAEA NSS 17, 2011, "Computer Security at Nuclear Facilities".
[4] IAEA NSS 23-G, 2015, "Implementing Guide. Security of Nuclear Information".

Определение конфиденциальности

РОСЭНЕРГОАТОМ ВНИИАЭС

1

Конфиденциальность данных (data confidentiality):
Свойство, гарантирующее, что информация не стала доступна или раскрыта любым неавторизованным субъектам системы, включая неавторизованных лиц, структуры или процессы.

2

Конфиденциальность (confidentiality):
Гарантия того, что информация не будет раскрыта неавторизованным лицам, процессам или устройствам.

[1] ГОСТ Р 56205-2014, 2015, “Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели”.
[2] IEC/TS 62443-1-1:2009, 2009, Edition 1, "Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models"

Определение конфиденциальности

РОСЭНЕРГОАТОМ ВНИИАЭС

1

Конфиденциальность информации:
Свойство безопасности информации,
при котором доступ к ней осуществляют только субъекты доступа, имеющие на него право.

2

Конфиденциальность информации (confidentiality):
Состояние информации,
при котором доступ к ней осуществляют только субъекты, имеющие на него право.

[1] ФСТЭК, 2014, “Методический документ. Меры защиты информации в государственных информационных системах”.
[2] Р 50.1.056-2005, 2006, “Техническая защита информации. Основные термины и определения”.

Определение конфиденциальности

РОСЭНЕРГОАТОМ ВНИИАЭС

1

2

3

Конфиденциальность (confidentiality):

Сохранение авторизованных ограничений на доступ и раскрытие информации, включая средства защиты неприкосновенности частной жизни и проприетарной информации.

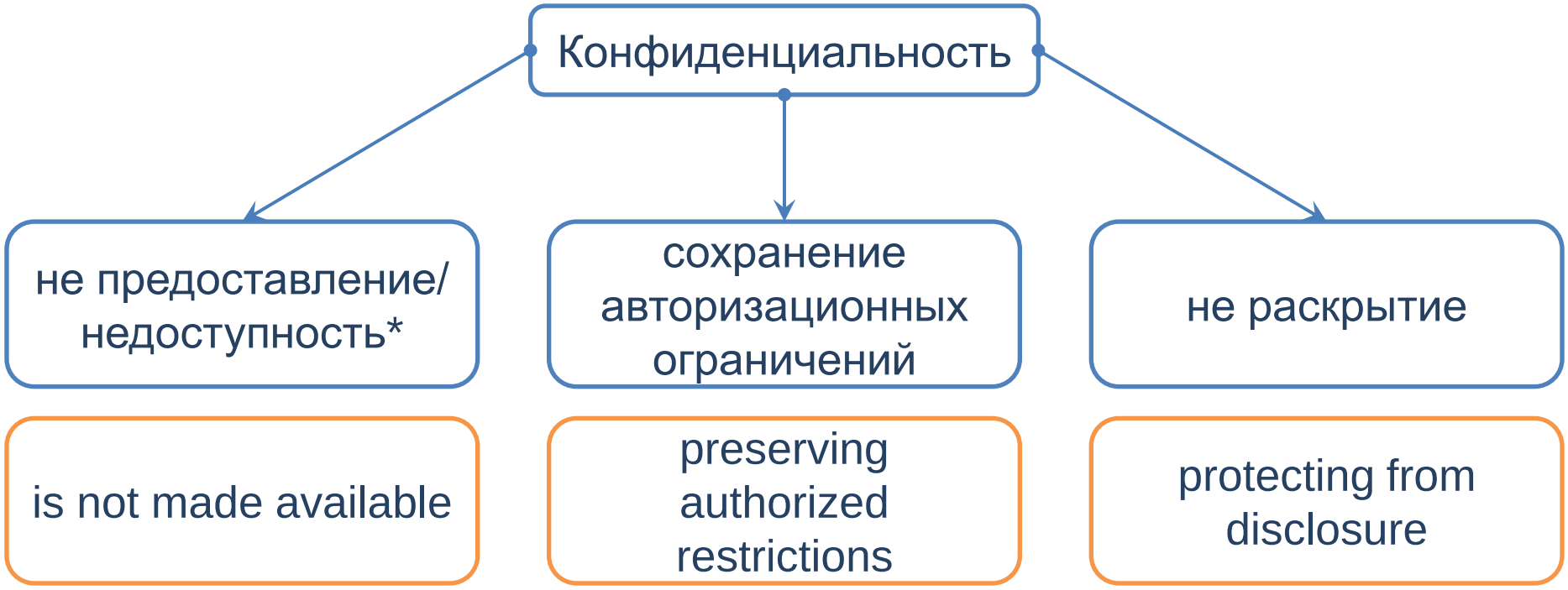
Примечание:

при употреблении в контексте IACS* термин относится к защите данных и информации, относящихся к IACS, от неавторизованного доступа.

[1] ГОСТ Р МЭК 62443-3-3-2016, 2016, Сети промышленной коммуникации. Безопасность сетей и систем. Часть 3-3. Требования к системной безопасности и уровни безопасности.
[2] IEC 62443-3-3:2013, 2013, Edition 1, "Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels".
[3] NIST SP800-82, 2015, Revision 2, "Guide to Industrial Control Systems (ICS) Security".

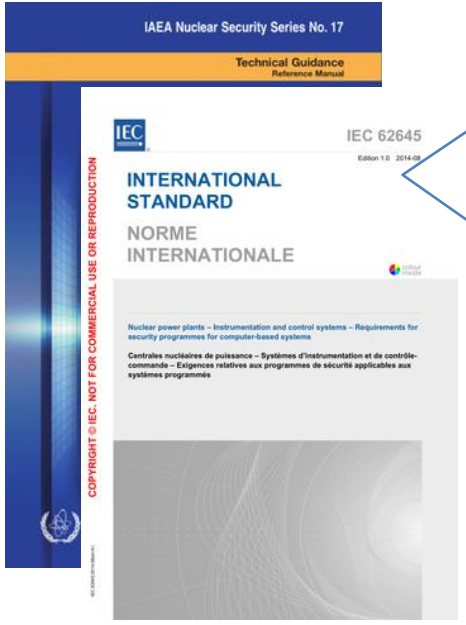
* Сохранён текст оригинала (IACS - industrial automation and control systems, системы промышленной автоматики и контроля).

Определение конфиденциальности



* Недоступность для неавторизованного субъекта

Определение конфиденциальности



Annex D (informative)
Attackers profiles and attack scenarios

…

Depending on the objectives or aims of the attack, the attacker is likely to exploit different system vulnerabilities. Such attacks can lead to:

- unauthorized access to information (loss of confidentiality);

…

[1] IEC 62645:2014, 2014, Edition 1, "Nuclear power plants - Instrumentation and control systems - Requirements for security programmes for computer-based systems"
[2] IAEA Nuclear Security Series No. 17, 2011, Technical Guidance. Reference Manual, "Computer Security at Nuclear Facilities"

Определение конфиденциальности

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 56205— 2014 IEC/TS 62443-1-1:2009

СЕТИ КОММУНИКАЦИОННЫЕ ПРОМЫШЛЕННЫЕ
Защищенность (кибербезопасность) сети и системы

Часть 1-1
Терминология, концептуальные положения и модели

IEC/TS 62443-1-1:2009
Industrial communication networks — Network and system security —
Part 1-1: Terminology, concepts and models
(IDT)

Издание официальное

Москва
Стандартинформ
2014

5.2 Цели безопасности

…

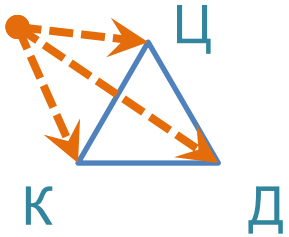
В рамках определенных требований к эксплуатации отдельные компоненты или системы в целом будут иметь иные приоритеты в качестве целей (т.е. значение целостности или доступности может перевесить значение конфиденциальности или наоборот). В результате для достижения целей безопасности организация может быть вынуждена применять другие контрмеры.

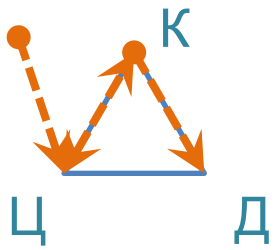
…

Источник: ГОСТ Р 56205-2014 (IEC/TS 62443-1-1:2009), 2014, "Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели".

ПРАКТИКА

Воздействие на конфиденциальность





Воздействие:

- прямое:
  - передача информации по открытым каналам;
  - прямое раскрытие информации.
- опосредованное:
  - одновременное нарушение нескольких свойств информации/данных;
  - последовательное взаимосвязанное нарушение свойств информации/данных.

*Ц, Д, К – целостность, доступность, конфиденциальность.

Описание атаки

Атака может характеризоваться с помощью следующих понятий:

- схема атаки / поверхность атаки / вектор атаки;
- период атаки / фазы атаки.

МАГАТЭ NSS-17 - Фазы атаки

Приложение I. Сценарии атак на системы ядерных установок

…

Хорошо спланированная компьютерная атака состоит из ряда этапов. Эти этапы включают:

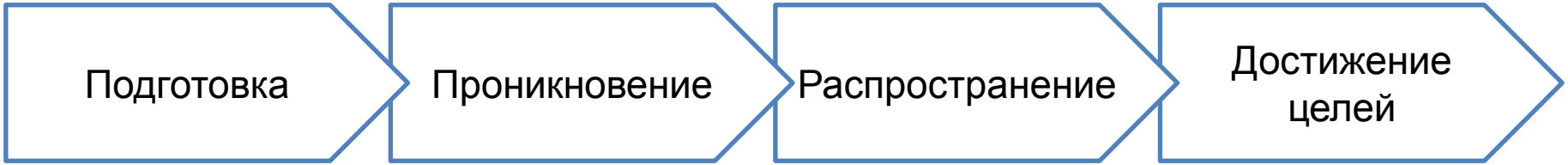
- **определение цели;**
- **изучение обстановки;**
- **доступ к системе**/нарушение ее нормальной работы;
- выполнение атаки;
- сокрытие следов в поддержку отрицания виновности <прим. непричастности>.

…

Источник: Справочное руководство "Компьютерная безопасность на ядерных установках", серия изданий МАГАТЭ по физической ядерной безопасности, № 17, МАГАТЭ, 2012

Фазы целевой атаки

РОСЭНЕРГОАТОМ ВНИИАЭС



- выявление цели
- сбор информации
- разработка стратегии
- создание стенда
- разработка инструментов

- техника обхода стандартных средств защиты
- эксплуатация уязвимостей
- социальная инженерия
- комбинированные техники
- инвентаризация сети

- закрепление
- распространение
- обновление
- поиск ключевой информации и методов достижения целей

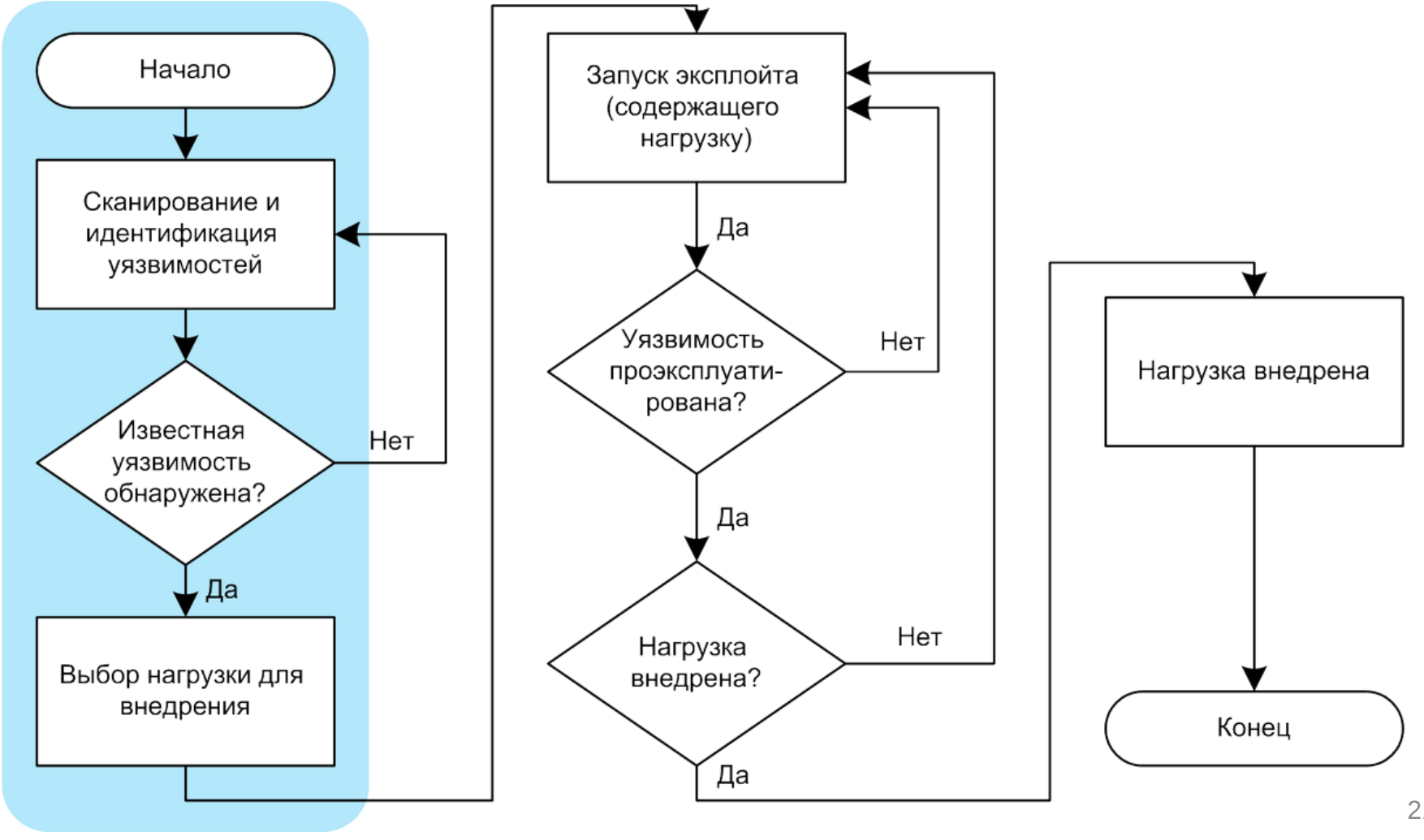
- изменение данных
- манипуляции с бизнес процессами
- хищение ключевой информации
- сокрытие следов
- точка возврата

Вениамин Левцов, "Анатомия таргетированной атаки", 16 декабря 2016
https://business.kaspersky.ru/targeted-attack-anatomy/4388/

АТАКА В КРАТКОСРОЧНОЙ ПЕРСПЕКТИВЕ

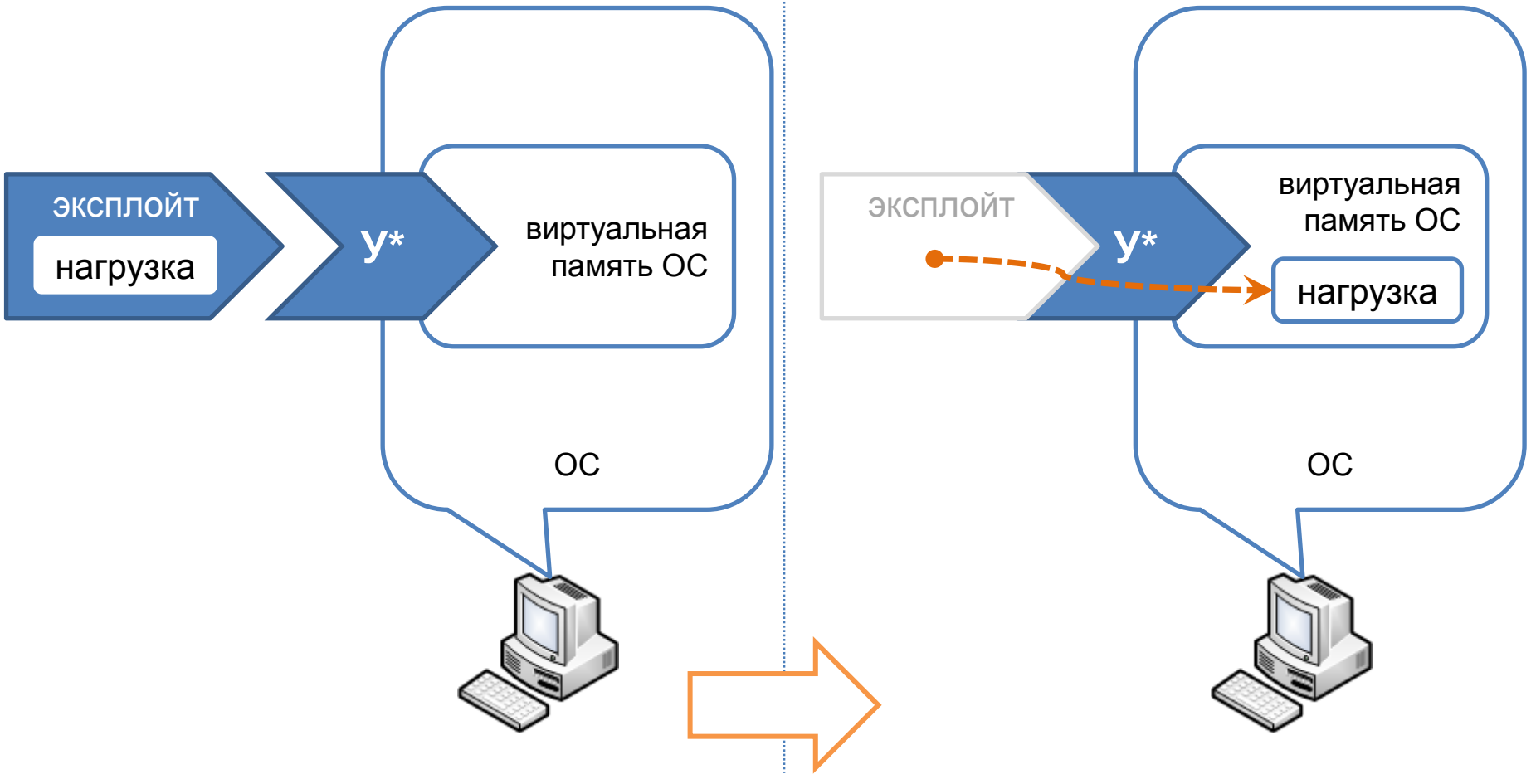
Пример алгоритма атаки

РОСЭНЕРГОАТОМ ВНИИАЭС



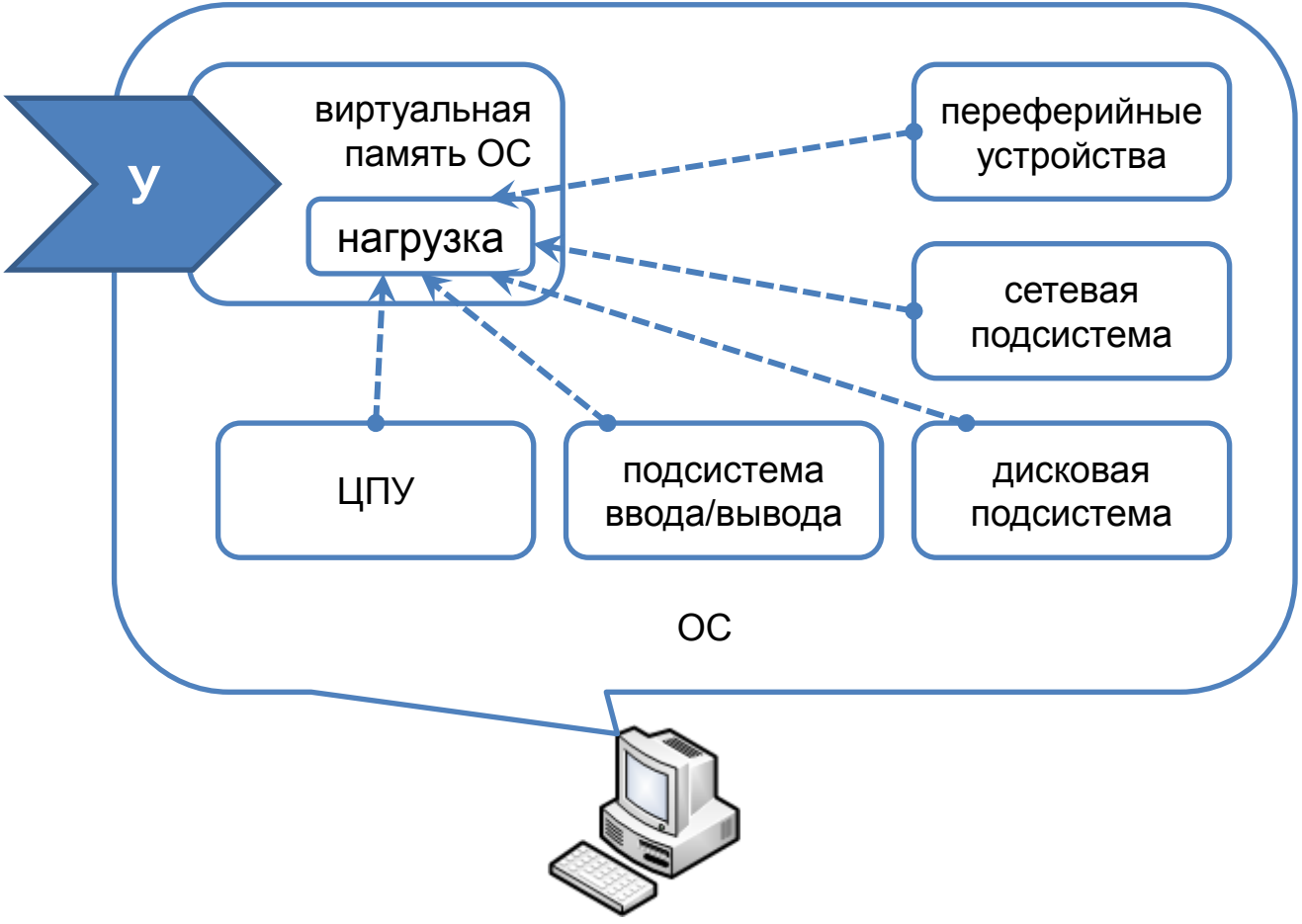
Пример атаки – Эксплуатация уязвимости

РОСЭНЕРГОАТОМ ВНИИАЭС

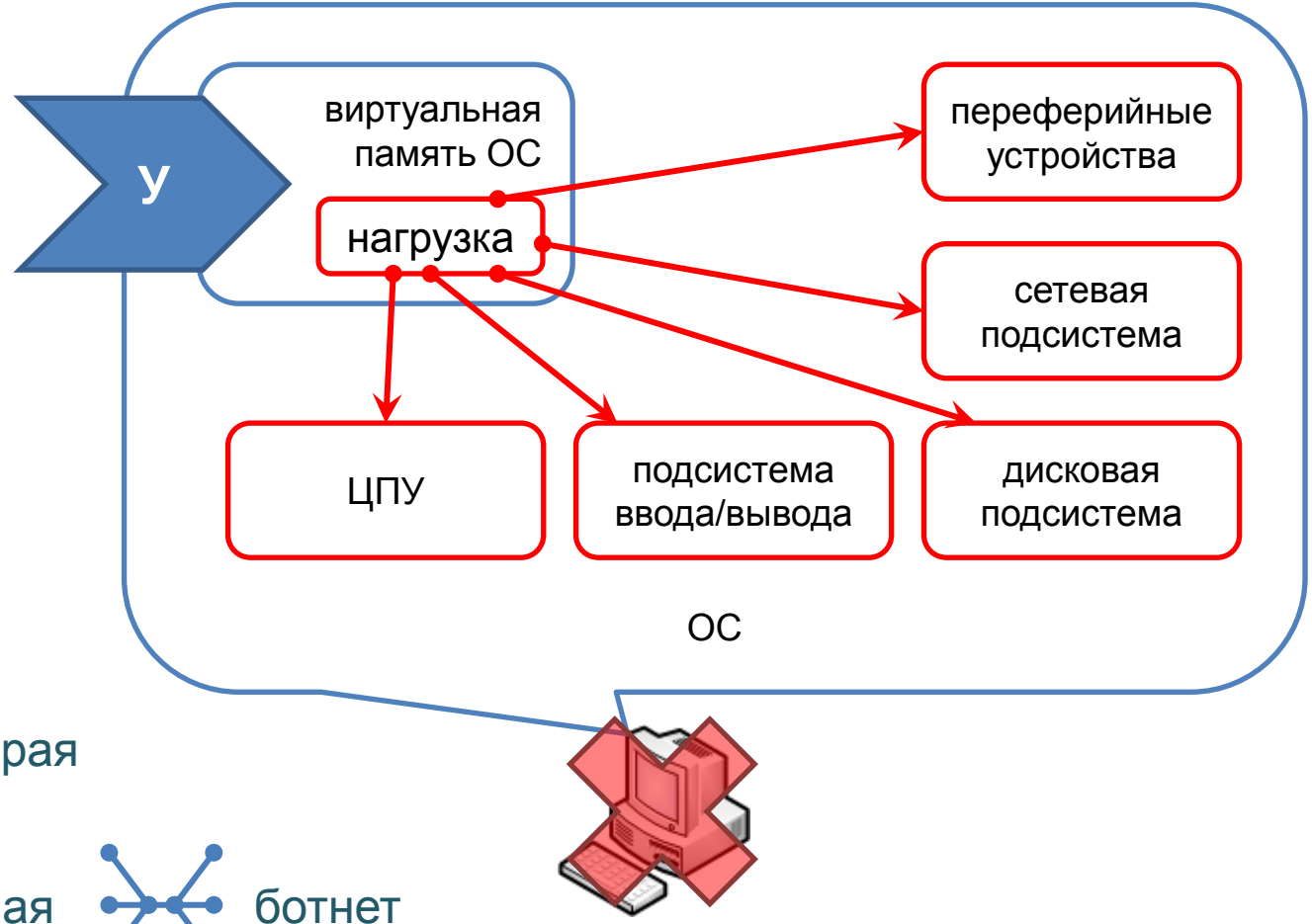


*У - уязвимость нулевого дня, forever-day уязвимость, forever-day bug

Пример атаки – Пассивная фаза



Пример атаки – Активная фаза



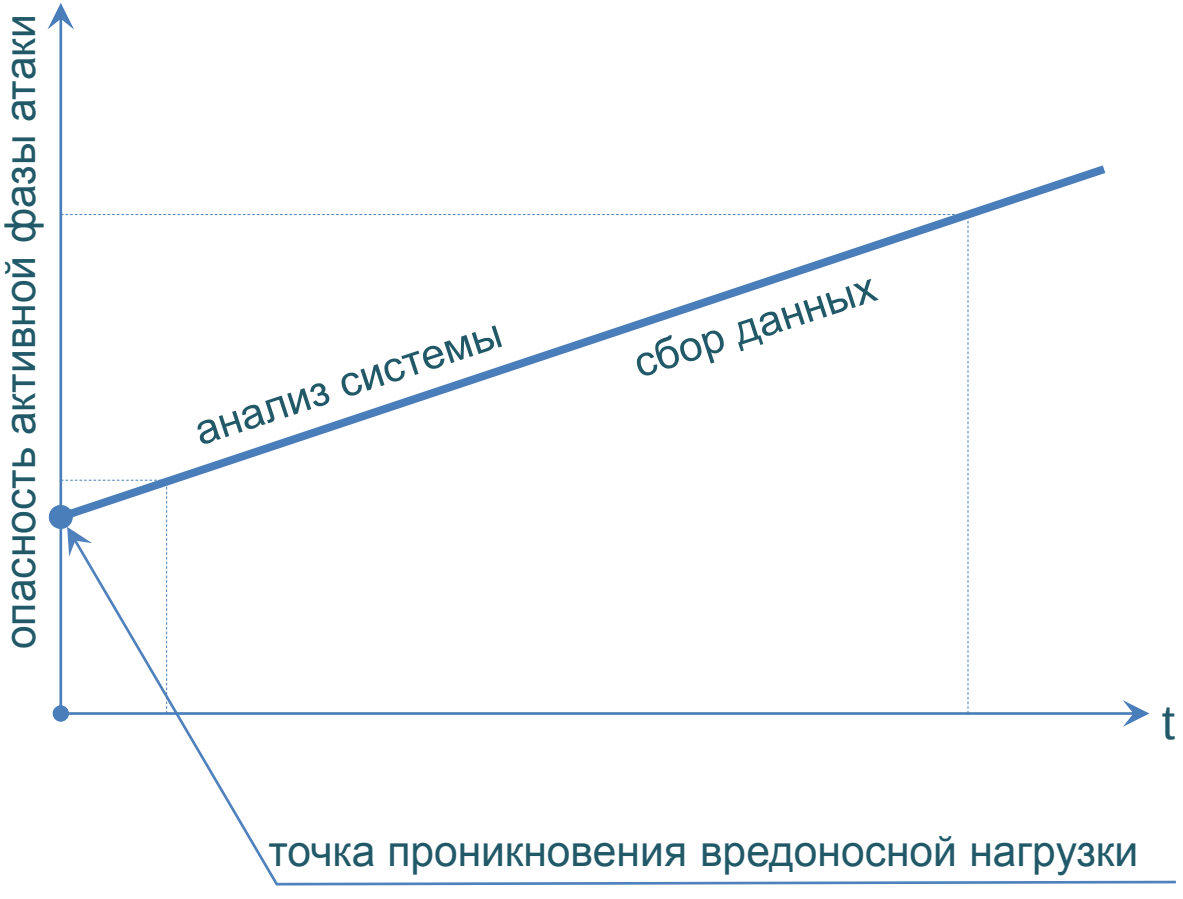
быстрая

точная

ботнет

Значимость периода атаки

РОСЭНЕРГОАТОМ ВНИИАЭС



Значимость периода атаки - Статистика

РОСЭНЕРГОАТОМ ВНИИАЭС

200 дней

По статистике «Лаборатории Касперского», в среднем **обнаружение целевой атаки** происходит спустя **200 дней** с момента ее активности…[1]

9 месяцев

Атака <Stuxnet> продолжалась **9 месяцев** [2]

60% не закрыто

Из 75 обнаруженных в 2016 году Kaspersky Lab уязвимостей к **середине марта 2017** года производителями промышленного ПО было **закрыто 30**. [3]

[1] Вениамин Левцов, "Анатомия таргетированной атаки", 16 декабря 2016 (https://business.kaspersky.ru/targeted-attack-anatomy/4388/)
[2] По материалам статьи "Целенаправленные атаки - обнаружение и защита", Николай Петров, издание "Information Security“, №2, 2014 (http://www.itsec.ru/imag/insec-2-2014/)
[3] https://ics-cert.kaspersky.ru/reports/2017/03/28/threat-landscape-for-industrial-automation-systems-in-the-second-half-of-2016/

Значимость периода атаки - Статистика

РОСЭНЕРГОАТОМ ВНИИАЭС

2008 июль

The Fanny worm presumably **compiled** in July 2008

2008 декабрь

It was **first observed** and blocked by our systems in December 2008

2009 июнь

For escalation of privilege, Fanny used a vulnerability **patched** by the Microsoft bulletin MS09-025...*

По материалам: https://securelist.com/blog/research/68750/equation-the-death-star-of-malware-galaxy/
* https://technet.microsoft.com/ru-ru/library/security/ms09-025.aspx

Вредоносная нагрузка - Примеры

РОСЭНЕРГОАТОМ ВНИИАЭС

Примеры вредоносной нагрузки (payload):

- удаленный доступ;
- модуль распространения внутри инфраструктуры;
- очистка следов активности, самоуничтожение;
- взаимодействие с C&C* и обновление;
- поиск информации на диске;
- шифрование;
- клавиатурный шпион;
- запись экрана;
- чтение локальной почты.

Вениамин Левцов, "Анатомия таргетированной атаки", 16 декабря 2016, https://business.kaspersky.ru/targeted-attack-anatomy/4388/
* C&C – command and control server (командный сервер)

ПРИМЕРЫ АТАК

Пример атаки - Duqu

In one case, Duqu arrived at the target using a specially crafted, Microsoft Word document. The Word document contained a currently undisclosed **0-day kernel exploit** that allows the attackers to install Duqu onto the computer **unbeknownst to the user**.

One of the variant's driver files was signed with a **valid digital code signing certificate** that expires on August 2, 2012. We believe the private keys used to generate the certificate were stolen from the company. Having a legitimate certificate allows Duqu to **bypass default restrictions on unknown drivers and common security policies**.

Symantec, "W32.Duqu. The precursor to the next Stuxnet", Version 1.4 (November 23, 2011)

Пример атаки - Duqu

In addition, **the DLL can scan for and attempt to bypass components** of a variety **of security products**.

Resource 302 is a loader program. **It can load the payload into memory and execute it in several different ways.**

The **peer-to-peer protocol** is not configured by default for use, but **has been seen configured** for use in cases **where a computer cannot reach the external C&C server**.

Symantec, "W32.Duqu. The precursor to the next Stuxnet", Version 1.4 (November 23, 2011)

Пример атаки - Duqu 2.0

In general, once the attackers gain access into a network, two phases follow:

- reconnaissance and identification of network topology;
- lateral movement.

In the case of Duqu 2.0, the **lateral movement** technique appears to have taken advantage of another **zero-day** (CVE-2014-6324), which was patched in November 2014 with MS14-068.

This **exploit allows** an unprivileged domain user **to elevate credentials** to a domain administrator account.

The attackers can deploy two types of packages to their victims:

- **"basic"**, **in-memory** remote backdoor **(~500K)**;
- **fully featured**, C&C-capable, **in-memory** espionage platform **(18MB)**.

Kaspersky Lab, "The DUQU 2.0. Technical Details", Version: 2.1 (11 June 2015)

Пример атаки - Stuxnet

РОСЭНЕРГОАТОМ ВНИИАЭС

9 атака продолжалась **9 месяцев**

3 за это время были отмечены **3 модификации червя** <прим.: три «волны» атаки>

0-day червь использовал **уязвимости нулевого дня**

По материалам статьи "Целенаправленные атаки - обнаружение и защита", Николай Петров, издание "Information Security“, №2, 2014
http://www.itsec.ru/imag/insec-2-2014/

Пример атаки - Stuxnet

РОСЭНЕРГОАТОМ ВНИИАЭС

3

после инсталляции с USB-флеш три раза,
червь себя удалял <прим.: самоуничтожался>

0

ни одна из иранских систем
не имела прямого соединения с Интернет

12 тыс.

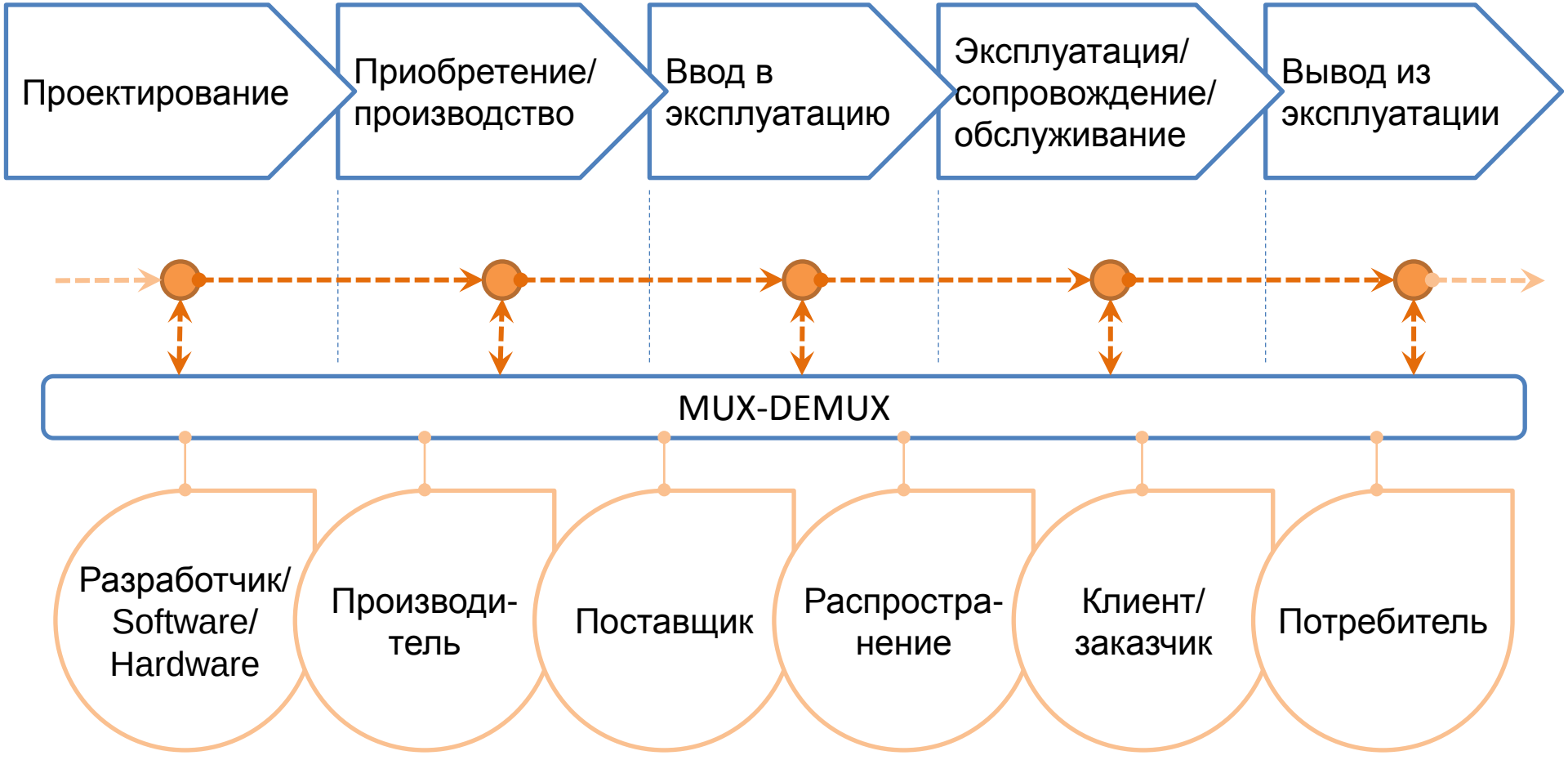
атака инфицировала **12 тыс. компьютеров**
в **пяти иранских организациях**

По материалам статьи "Целенаправленные атаки - обнаружение и защита", Николай Петров, издание "Information Security“, №2, 2014
http://www.itsec.ru/imag/insec-2-2014/

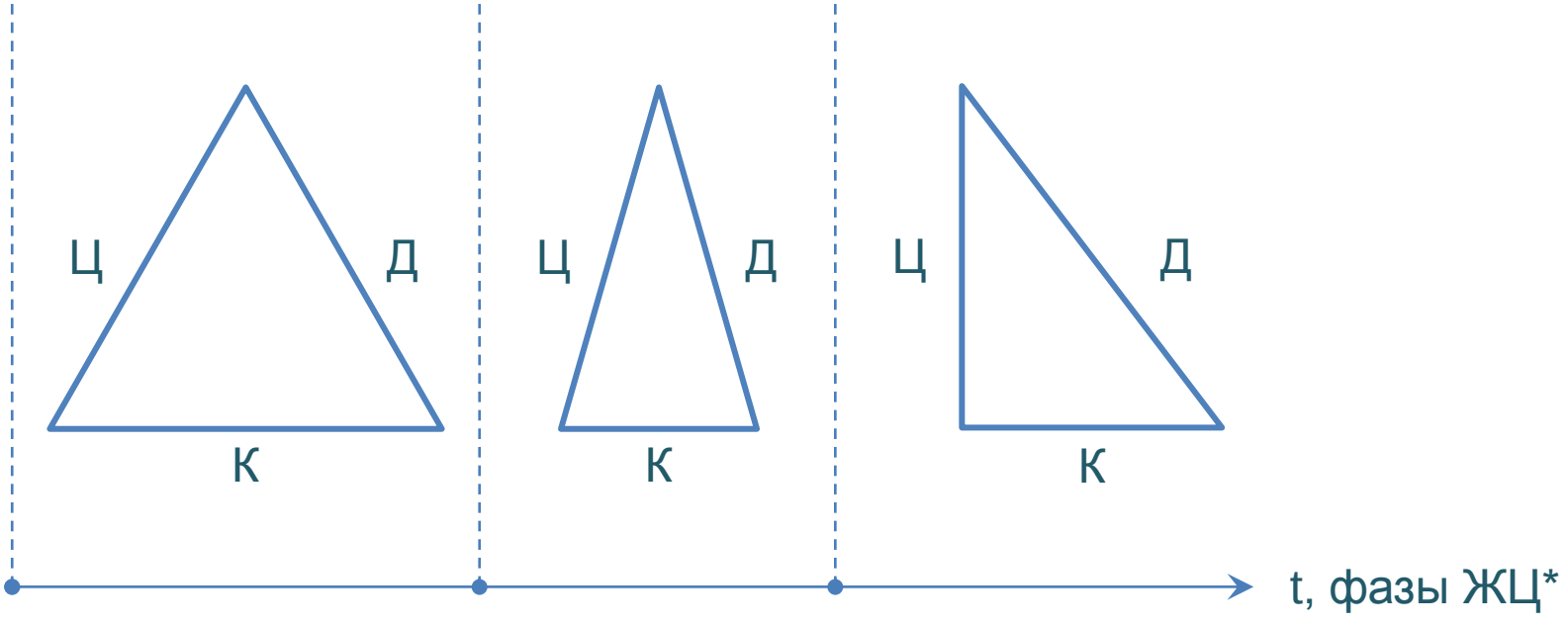
АТАКА НА УРОВНЕ ЖИЗНЕННОГО ЦИКЛА

Атака на уровне жизненного цикла

РОСЭНЕРГОАТОМ ВНИИАЭС



Значимость на различных фазах ЖЦ



* ЖЦ – жизненный цикл

Пример атаки в перспективе ЖЦ - Duqu

The attackers are looking for information such as **design documents** that could help them **mount a future attack** on various industries, including industrial control system facilities.

Duqu's purpose is **to gather intelligence data and assets from** entities such as **industrial infrastructure and system manufacturers**, amongst others not in the industrial sector, in order to more easily **conduct a future attack against another third party**.

Symantec, "W32.Duqu. The precursor to the next Stuxnet", Version 1.4 (November 23, 2011)

ВЫВОДЫ

Выводы

РОСЭНЕРГОАТОМ ВНИИАЭС

1. Конфиденциальность в АСУ ТП **≠ 0**.

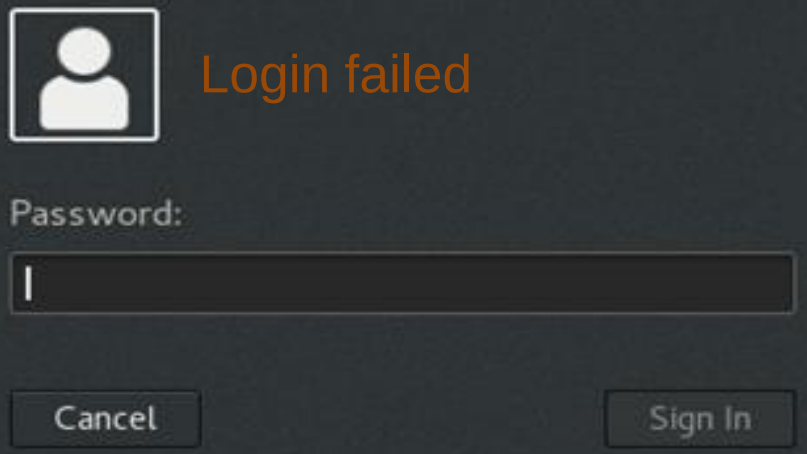
2. Конфиденциальность ВАЖНА.
   Нельзя пренебрегать и не учитывать.

3. В подавляющем большинстве случаев для АСУ ТП целостность или доступность имеют приоритет выше, чем конфиденциальность, то есть в общем случае:

Ц, Д > К > 0

РОСЭНЕРГОАТОМ
ВНИИАЭС

Благодарю за внимание.
Вопросы?



ПРИЛОЖЕНИЯ

Недекларированные возможности

РОСЭНЕРГОАТОМ ВНИИАЭС

Недекларированные возможности:

Функциональные возможности средств вычислительной техники и программного обеспечения, не описанные или не соответствующие описанным в документации, которые могут привести к снижению или нарушению свойств безопасности информации.

ГОСТ Р 53114-2008, 2008, «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения».

Нагрузка (payload) - Определение

РОСЭНЕРГОАТОМ ВНИИАЭС

Payload (нагрузка, вредоносная нагрузка):

The "cargo" code in a virus rather than the portions used to avoid detection or replicate. The payload code can display text or graphics on the screen, or it may corrupt or erase data. Not all viruses contain a deliberate payload. However, these codes affect CPU usage, hard disk space, and the time it takes to clean viruses. Payload can also refer to the data or packets sent during an attack.

[McAfee] http://home.mcafee.com/virusinfo/glossary?ctst=1

Payload (нагрузка):

Payload is the actual application data a packet contains.

[SANS Institute] https://www.sans.org/security-resources/glossary-of-terms/

Ландшафт угроз

РОСЭНЕРГОАТОМ ВНИИАЭС

- Изоляция промышленных сетей больше не может рассматриваться как мера их защиты. Доля попыток заражений вредоносным ПО с участием переносных носителей, заражений резервных копий, использование в сложных атаках изощренных способов переноса данных из изолированных сетей свидетельствуют о том, что **невозможно избежать рисков путем простого отключения системы от интернета**.

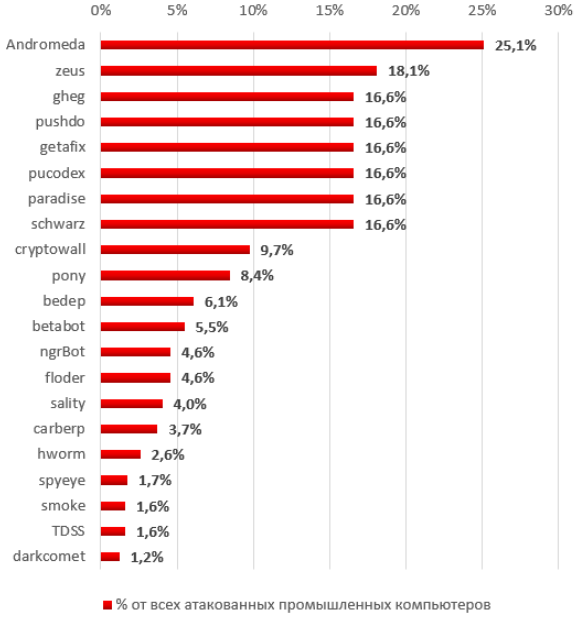
- Относительно независимое (от «традиционного» IT) развитие систем промышленной автоматизации привело к тому, что производители индустриальных решений годами разрабатывали программное и аппаратное обеспечение АСУ ТП практически без учета требований информационной безопасности.

https://ics-cert.kaspersky.ru/reports/2017/03/28/threat-landscape-for-industrial-automation-systems-in-the-second-half-of-2016/

Ландшафт угроз - Статистика

РОСЭНЕРГОАТОМ ВНИИАЭС

Большинство ботнет-агентов являются **модульным** вредоносным **ПО**, **функциональность** которого **может изменяться динамически**, в том числе **на основе данных о системе**, переданных на командные серверы злоумышленников.



Распределение промышленных компьютеров, атакованных ботнет-агентами, по семействам ботов

https://ics-cert.kaspersky.ru/reports/2017/03/28/threat-landscape-for-industrial-automation-systems-in-the-second-half-of-2016/

Примеры воздействий (типы атак)

РОСЭНЕРГОАТОМ ВНИИАЭС