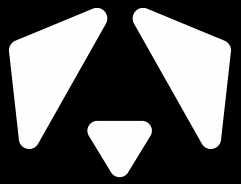


ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Игнорируем уязвимости сегодня? Расплачиваемся завтра!

Васин Вячеслав

Системный аналитик отдела исследований информационных технологий – ЗАО «Перспективный мониторинг», ГК «ИнфоТеКС»

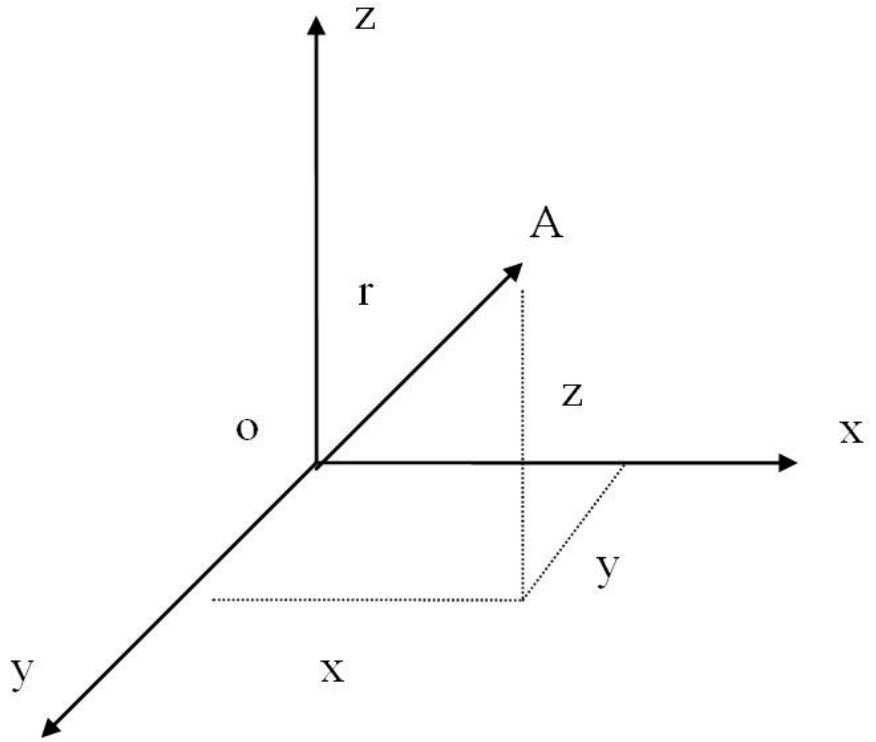
Agenda

- Разбираемся, почему об этом стоит поговорить
- Договариваемся о терминах
- Смотрим на современную уязвимость изнутри
- Делаем первые шаги к работе над уязвимостями

Положение дел на начало 2017

Цитата: Рене Декарт

Определив точно значения слов, вы избавите человечество от половины заблуждений. (Вариант 2: «Люди избавились бы от половины своих неприятностей, если бы смогли договориться о значении слов»)



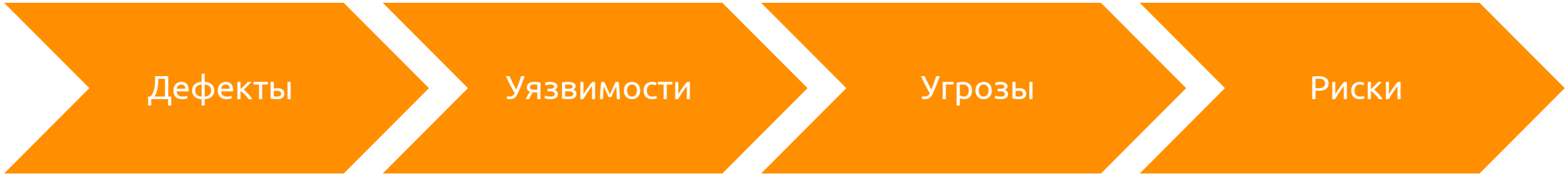
Договоримся о терминах

- под **информационной безопасностью** (ИБ) обычно понимают свойство (состояние) защищенности ее ресурсов в условиях наличия угроз в информационной сфере;
- определяющими факторами ИБ являют **угроза** (threat) и **риск** (risk);
- **угрозой** называют потенциальную причину (событие, нарушение, инцидент), снижающую уровень ИБ информационной системы, то есть потенциально способную привести к негативным последствиям и ущербу системы или организации;

Договоримся о терминах

- **риск** представляет собой возможный ущерб, т.е. комбинацию, вероятности реализации угрозы и ущерба от нее;
- одной из наиболее актуальных угроз ИБ компьютерных систем является возможность реализации **уязвимости** (vulnerability) системы;
- под **уязвимостью** понимают реализуемый **дефект** (weakness) технического и программного обеспечения системы, снижающий уровень защищённости ресурсов от тех или иных угроз.

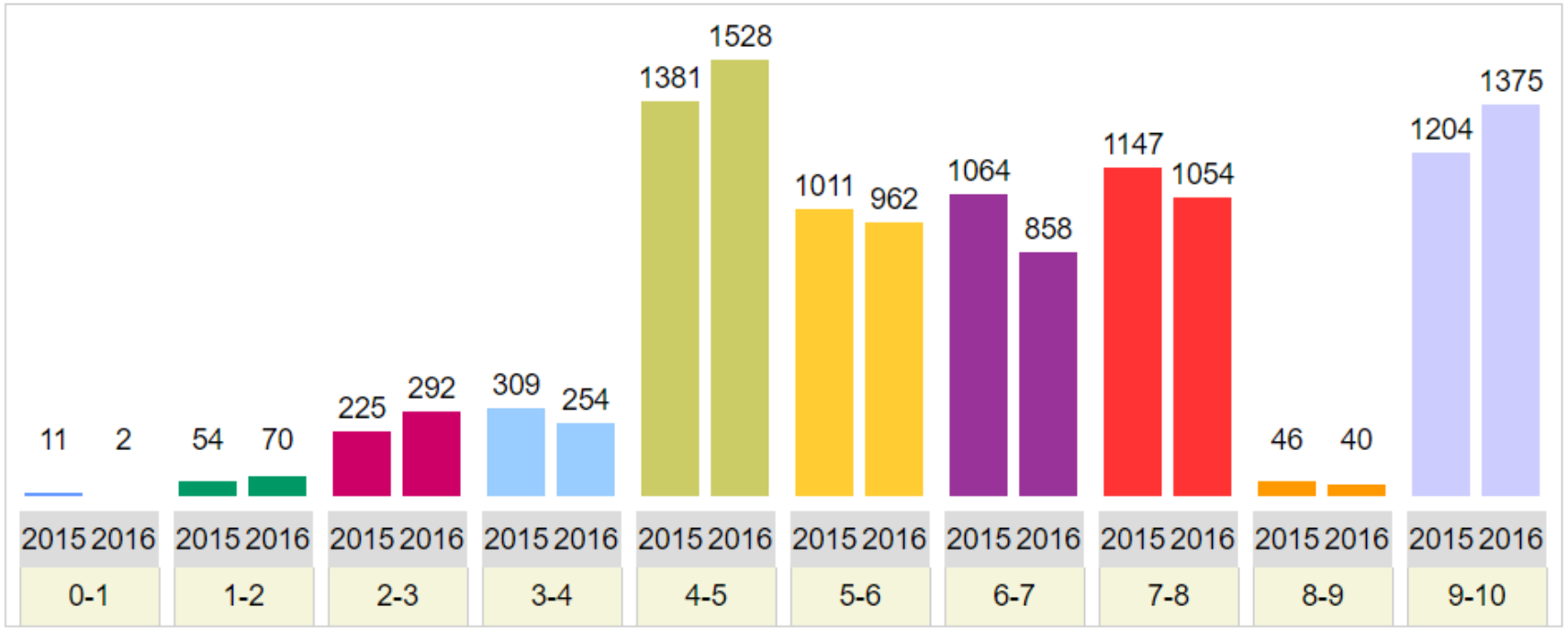
Меньше слов – больше смысла



Где и что искать?

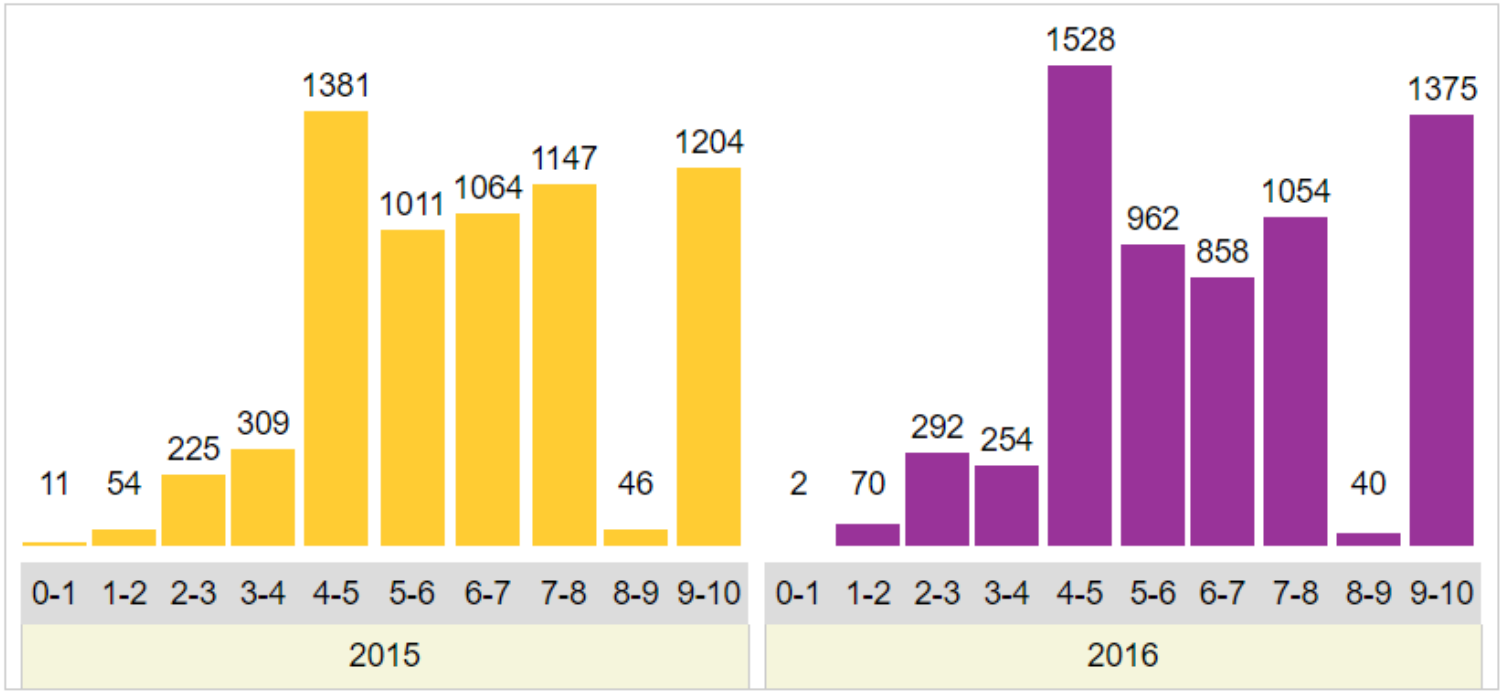
- **MITRE CVE https://cve.mitre.org/**
- **MITRE CWE https://cwe.mitre.org/**
- **Банк данных угроз ФСТЭК http://bdu.fstec.ru/**
- **База данных ИБ-контента Vulners https://vulners.com/**
- **Другие источники https://google.com/, https://yandex.ru/**

Распределение уязвимостей



http://www.cvedetails.com/cvss-score-charts.php?fromform=1&vendor_id=&product_id=&startdate=2015-01-01&enddate=2016-12-31&groupbyyear=1

Распределение уязвимостей



http://www.cvedetails.com/cvss-score-charts.php?fromform=1&vendor_id=&product_id=&startdate=2015-01-01&enddate=2016-12-31&groupbyyear=1

CVE-2016-4484

http://hmarco.org/bugs/CVE-2016-4484/CVE-2016-4484_cryptsetup_initrd_shell.html

Как так вышло?

initrd.img:/script/local-top/cryptroot

```
0   #!/bin/sh
    . . .

171 setup_mapping()
172 {
    . . .
273         # Try to get a satisfactory password $crypttries times
274         count=0
275         while [ $crypttries -le 0 ] || [ $count -lt $crypttries ]; do
276                 export CRYPTTAB_TRIED="$count"
277                 count=$(( $count + 1 ))
    . . .
298                 if [ ! -e "$NEWROOT" ]; then
                                # cryptkeyscript = /lib/cryptsetup/askpass
                                # cryptopen = /sbin/cryptsetup -T 1
                                # The user is asked the password and then passed to $cryptopen
299                             if ! crypttarget="$crypttarget" cryptsource="$cryptsource" \
300                               $cryptkeyscript "$cryptkey" | $cryptopen; then
301                                  message "cryptsetup: cryptsetup failed, bad password or options?"
302                                  continue
303                             fi
304                 fi
305

    . . .
```

Как так вышло?

initrd.img:/script/local-top/cryptroot

```
    . . .
342                 #if [ -z "$FSTYPE" ] || [ "$FSTYPE" = "unknown" ]; then
343                 if [ -z "$FSTYPE" ]; then
344                         message "cryptsetup: unknown fstype, bad password or options?"
345                         udev_settle
346                         $cryptremove
347                         continue
348                 fi
349
350                 message "cryptsetup: $crypttarget set up successfully"
351                 break
352         done
353         # Always false -> never taken the if
354         if [ $crypttries -gt 0 ] && [ $count -gt $crypttries ]; then
355                 message "cryptsetup: maximum number of tries exceeded for $crypttarget"
356                 return 1
357         fi
358
359         udev_settle
360         return 0
361 }
    . . .
402 # Do we have any settings from the /conf/conf.d/cryptroot file?
403 if [ -r /conf/conf.d/cryptroot ]; then
404         while read mapping <&3; do
405                 setup_mapping "$mapping" 3<&-   # Try to unlock each encrypted partition.
406         done 3< /conf/conf.d/cryptroot
407 fi
408
409 exit 0
```

Как так вышло?

initrd.img:/script/local

```
. . .
local_device_setup()
{
    . . .
        # If the root device hasn't shown up yet, give it a little while
        # to allow for asynchronous device discovery (e.g. USB).  We
        # also need to keep invoking the local-block scripts in case
        # there are devices stacked on top of those.
        if ! real_dev=$(resolve_device "${dev_id}") ||
           ! get_fstype "${real_dev}" >/dev/null; then
                log_begin_msg "Waiting for ${name} file system"

                # Timeout is max(30, rootdelay) seconds (approximately)
                case $DPKG_ARCH in
                        powerpc|ppc64|ppc64el)
                                slumber=180
                                ;;
                        *)
                                slumber=30
                                ;;
                esac
                if [ ${ROOTDELAY:-0} -gt $slumber ]; then
                        slumber=$ROOTDELAY
                fi

                while true; do
                        sleep 1
                # local_block() calls to setup_mapping() 30 times,
                # trying to unlock LUKS root filesystem.
```

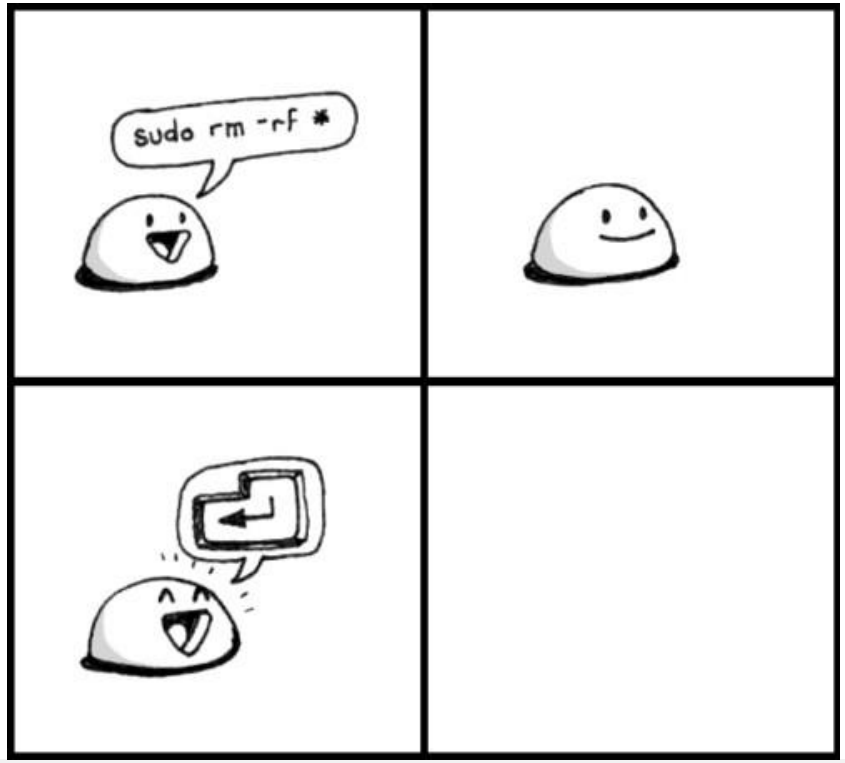
Как так вышло?

initrd.img:/script/local

```
99                      local_block "${dev_id}"
100                     if real_dev=$(resolve_device "${dev_id}") &&
101                        get_fstype "${real_dev}" >/dev/null; then
102                             wait_for_udev 10
103                             log_end_msg 0
104                             break
105                     fi
106                     slumber=$(( ${slumber} - 1 ))
107                     if [ ${slumber} -eq 0 ]; then
108                             log_end_msg 1 || true
109                             break
110                     fi
111             done
112     fi
113
114     # We've given up, but we'll let the user fix matters if they can
115     while ! real_dev=$(resolve_device "${dev_id}") ||
116           ! get_fstype "${real_dev}" >/dev/null; do
117             echo "Gave up waiting for ${name} device.  Common problems:"
118             echo " - Boot args (cat /proc/cmdline)"
119             echo "   - Check rootdelay= (did the system wait long enough?)"
120             if [ "${name}" = root ]; then
121                     echo "   - Check root= (did the system wait for the right device?)"
122             fi
123             echo " - Missing modules (cat /proc/modules; ls /dev)"
124             panic "ALERT!  ${dev_id} does not exist.  Dropping to a shell!"
125     done
126
127     DEV="${real_dev}"
128 }
. . .
```

Последствия?

- **Повышение привилегий:**
  - **Setuid**
  - **Ядро и (или) INITRD**
- **Раскрытие информации:**
  - **Доступ к незашифрованной информации**
- **Отказ в обслуживании:**
  - **«rm –Rf»**



First Step

Как сделать жизнь лучше?

- ## Аудит информационной безопасности

Аудит информационной безопасности — независимая оценка текущего состояния системы информационной безопасности, устанавливающая уровень ее соответствия определенным критериям, и предоставление результатов в виде рекомендаций.

- ## Управление и мониторинг ИБ (управлять уязвимостями)

Управление уязвимостями — это идентификация, оценка, классификация и выбор решения для устранения уязвимостей.

- ## Тестирование на проникновение

Тестирование на проникновение (пентест) популярная услуга в области информационной безопасности, суть которой заключается в санкционированной попытке обойти существующий комплекс средств защиты информационной системы.

- ## Практики безопасной разработки программного обеспечения

Практики безопасной разработки сокращают совокупную стоимость разработки за счёт более раннего обнаружения и устранения уязвимостей.

Как сделать жизнь лучше?

- Аудит информационной безопасности

http://amonitoring.ru/service/security-analysis/audit/

- Управление и мониторинг ИБ (управлять уязвимостями)

http://amonitoring.ru/service/vulnerability-management/

- Тестирование на проникновение

http://amonitoring.ru/service/pentest/complex/

- Практики безопасной разработки программного обеспечения

http://amonitoring.ru/service/secure-development/

Спасибо за внимание!

Васин Вячеслав

Системный аналитик

Компании «Перспективный мониторинг»

Vyacheslav.Vasin@amonitoring.ru