

# СОВРЕМЕННЫЕ РОССИЙСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Корольков Сергей  
Технический директор  
АО «ДиалогНаука»

Целью презентации является обзор российских средств защиты информации с учетом текущей ситуации с импортозамещением.

План презентации:

- Вопросы импортозамещения
- Обзор современных российских СЗИ
  - Мониторинг событий ИБ
  - Средства анализа защищенности
  - Сканнер защищенности исходных кодов
  - Противодействие сетевым атакам
  - Контроль утечек конфиденциальной информации
  - Защита от целенаправленных атак
  - Контроль привилегированных пользователей
  - и др.

## Вопросы импортозамещения

Ключевые требования  
Постановления Правительства от  
16/11/2015 г. № 1236:

- ПО (СЗИ) для обеспечения государственных и муниципальных нужд должно быть российским.
- Исключение – если российского ПО такого же класса нет в «едином реестре российских программ для электронных вычислительных машин и баз данных».
- Минсвязи должно сформировать классификатор ПО и создать «единый реестр...»



**ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ПОСТАНОВЛЕНИЕ**

от 16 ноября 2015 г. № 1236

МОСКВА

**Об установлении запрета на допуск программного обеспечения,  
происходящего из иностранных государств, для целей  
осуществления закупок для обеспечения государственных  
и муниципальных нужд**

Важное исключение:

можно не покупать российское ПО  
если:

«...программное обеспечение, сведения о котором включены в реестр и которое соответствует тому же классу программного обеспечения, что и программное обеспечение, планируемое к закупке, по своим функциональным, техническим и (или) эксплуатационным характеристикам не соответствует установленным заказчиком требованиям к планируемому к закупке программному обеспечению.»



**ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ**

ПОСТАНОВЛЕНИЕ

от 16 ноября 2015 г. № 1236

МОСКВА

**Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд**

- В каких случаях нужен сертификат ФСТЭК?
- Какой производитель ПО (СЗИ) является российским?
- Какие классы средств защиты информации предусмотрены?
- Другие требования ПП:
  - Свободное распространение на всей территории РФ
  - Если ПО реализует функции защиты конфиденциальной информации, то у него должен быть сертификат соответствия

# В каких случаях нужен сертификат ФСТЭК?

В соответствии с правилами формирования реестра, если ПО является СЗИ, то ему нужен сертификат ФСТЭК.

Разъяснение Минкомсвязи от  
15/03/2016:

Заказчики самостоятельно  
формируют требования по защите  
информации к ПО.



МИНИСТЕРСТВО СВЯЗИ  
И МАССОВЫХ КОММУНИКАЦИЙ  
РОССИЙСКОЙ ФЕДЕРАЦИИ

МИНИСТР

Тверская ул., 7, Москва, 125375  
Справочная: +7 (495) 771-8000

*15.03.2016* № *НН-П11-4736*

на № \_\_\_\_\_ от \_\_\_\_\_

О необходимости соблюдения  
государственными заказчиками  
требований по защите информации

Какой производитель ПО является российским?

В соответствии с ПП 1236:

- организация зарегистрирована на территории РФ
- исключительное право на программное обеспечение на территории всего мира и на весь срок действия исключительного права принадлежит одному либо нескольким из следующих лиц:
  - Субъект РФ или муниципальное образование
  - Российская некоммерческая организация без преобладающего иностранного участия
  - Российская коммерческая организация без преобладающего иностранного участия
  - Гражданин РФ
- Годовые выплаты не российским организациям должны составлять менее 30% от выручки правообладателя.



Какие классы средств защиты информации предусмотрены?

Приказ Минкомсвязи от 31/12/2015 г. № 622 «Об утверждении правил применения классификатора программ для электронных вычислительных машин и баз данных». Вступил в силу 06.03.2016.

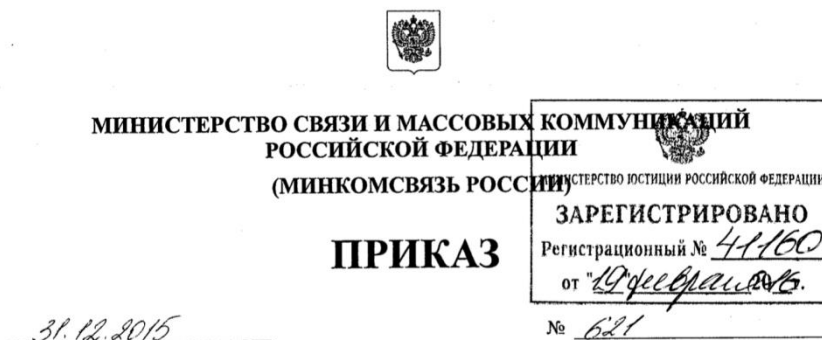
Вводит 2-х уровневую классификацию ПО

- раздел
- класс

24/02/2016 опубликован Приказ №621 от 19/02/2016 Министерства связи и массовых коммуникаций РФ «Об утверждении классификатора программ для электронных вычислительных машин и баз данных»

Раздел - Системное ПО - 02

Класс - Средства обеспечения информационной безопасности - 07



Об утверждении классификатора программ для электронных вычислительных машин и баз данных

В соответствии с абзацем вторым подпункта «а» пункта 7 постановления Правительства Российской Федерации от 16 ноября 2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» (Собрание законодательства Российской Федерации, 2015, № 47, ст. 6600)

Программы, а так же программно-технические средства (Системы), обеспечивающие поддержание конфиденциальности, целостности, доступности, отказоустойчивости, подотчётности, аутентичности и достоверности информации или средств её обработки. Включают в себя:

- Средства защиты от НСД.
- Системы управления событиями информационной безопасности.
- Межсетевые экраны.
- Средства фильтрации негативного контента.
- Системы защиты сервисов онлайн-платежей и дистанционного банковского обслуживания.
- Средства антивирусной защиты.
- Средства выявления целевых атак.
- Средства гарантированного уничтожения данных.
- Системы предотвращения утечек информации.
- Средства криптографической защиты информации и электронной подписи.
- Системы управления доступом к информационным ресурсам.
- Системы резервного копирования.

Классы СЗИ не учтенные в реестре:

- Средства защиты от спам рассылок.
- Средства противодействия сетевым вторжениям.
- Средства управлениями мобильными устройствами.
- Анализаторы исходного кода.
- Средства многофакторной и централизованной аутентификации.
- Средства защиты сред виртуализации.
- Средства анализа уровня защищенности.
- Средства и сервисы защиты от DDoS.
- Контроль привилегированных пользователей.
- СЗИ для мобильных платформ.
- Безопасность АСУ ТП.

## Обзор современных российских СЗИ

# Динамика появления российских СЗИ

Классы СЗИ	2010	2015	в реестре
Средства защиты от НСД	>5	>5	>5
Системы управления событиями информационной безопасности	-	4	1
Межсетевые экраны	>5	>5	>5
Средства фильтрации негативного контента	-	2	-
Системы защиты сервисов онлайн-платежей и ДБО	-	4	1
Средства антивирусной защиты	4	4	2
Средства выявления целевых атак	-	2	1
Средства гарантированного уничтожения данных	>5	>5	-
Системы предотвращения утечек информации	3	>5	1
Средства криптографической защиты информации и электронной подписи	>5	>5	>5
Системы управления доступом к информационным ресурсам	-	3	2
Средства защиты от спам рассылок	3	2	2
Средства противодействия сетевым вторжениям	3	>5	1
Средства управлениями мобильными устройствами	-	2	1
Анализаторы исходного кода	2	>3	3
Средства многофакторной и централизованной аутентификации	3	4	1
Средства защиты сред виртуализации	-	1	1
Средства анализа уровня защищенности	1	5	4
Средства и сервисы защиты от DDoS	2	3	-
Контроль привилегированных пользователей	-	1	-
СЗИ для мобильных платформ	-	4	1
Безопасность АСУ ТП	-	2	1

# Мониторинг событий ИБ

---

SIEM - Security information and event management. Средства сбора и анализа событий информационной безопасности.

Назначение SIEM:

- выявление инцидентов ИБ в режиме максимально приближенном к реальному, на основании информации от одного или нескольких источников ИТ инфраструктуры и СЗИ;
- обеспечение сохранности данных о событиях ИБ для дальнейшего расследования и пр.

Основные задачи SIEM:

- Сбор событий:
  - фильтрация, агрегация, нормализация;
- Мониторинг и анализ:
  - корреляция событий, уведомление администраторов;
- Хранение и поиск.

Российские средства мониторинга событий:

- Positive Technologies Security Monitor (Positive Technologies)
- RuSIEM (IT TASK)
- Комрад (НПО «Эшелон»)
- Security Vision (компания АйТи)

Особенности средств:

- MaxPatrol SIEM:
  - автоматическая инвентаризация и построение моделей ИС;
  - наличие среды для организации расследования инцидентов;
  - интеграция с MaxPatrol.
- RuSIEM и Комрад:
  - обладает достаточным для большинства случаев функционалом в части сбора и отображения событий.



# Средства анализа защищенности

---

Назначение средств анализа защищенности - автоматизация процесса управления уязвимостями:

- выявление уязвимостей;
- устранение уязвимостей;
- контроль устранения.

Современные средства анализа защищенности обеспечивают:

- автоматическое сканирование в сетевом режиме;
- автоматическое сканирование в «агентском» режиме;
- выявление изменений конфигурации;
- оценка соответствия техническим стандартам;
- проверку простых паролей, типичных недостатков конфигурирования.

# Средства анализа защищенности

---

Особенности российских сканнеров:

- MaxPatrol 8 (Positive Technologies)
  - наиболее развитое средство. Обладает всем необходимым набором механизмов выявления уязвимостей.
- REDCHECK (Алтекс Софт):
  - обладает необходимым набором механизмов выявления уязвимостей;
  - работает с использованием агентов, устанавливаемых на сканируемые хосты;
  - имеет гибкую систему отчетности.
- Сканер ВС (НПО Эшелон):
  - имеет возможности оценки защищенности российской ОС МСВС, оценки защищенности WiFi сетей и пр.

# Сканнер защищенности исходных кодов

---

Назначение сканнеров исходных кодов – выявление уязвимостей и закладок в приложениях на этапе их разработки и приемки.

Важное преимущество перед сетевыми сканерами защищенности – возможность быстрого анализа исходного кода с целью выявления ошибок.

Проблема сканнеров исходного кода – огромное количество ложных срабатываний и низкая квалификация (с точки зрения программирования) пользователей таких средств.

Цель всех производителей сканнеров – минимизировать количество ложны срабатываний с сохранением качества анализа.

# Сканнер защищенности исходных кодов

---

Особенности российских сканнеров:

- PT Application Inspector (Positive Technologies):
  - максимально упрощен процесс анализа;
  - наличие кнопки «демонстрировать уязвимость»;
  - интеграция с WAF.
- Solar inCode (Solar Security):
  - анализ защищенности без исходного кода;
  - анализ мобильных приложений;
  - рекомендации для настройки WAF;
  - возможность использования в качестве облачного сервиса.
- InfoWatch APPERCUT (InfoWatch):
  - возможность использования в качестве облачного сервиса;
  - оценка соответствия требованиям заказчика анализируемого ПО.

WAF – Web Application Firewall, межсетевые экраны уровня web приложений.

Назначение межсетевых экранов уровня приложений – выявление и блокирование атак непосредственно на уязвимости веб протоколов и веб приложений.

Российские межсетевые экраны уровня веб приложений:

- PT Application Firewall:
  - возможность защиты от уязвимостей Web сервиса выявленного анализатором защищенности кода (Virtual Patching);
  - наличие успешных внедрений.
- SolidWall (SolidSoft)

# Противодействие сетевым атакам

---

Средства выявления/предотвращения сетевых атак:

- средства обнаружения вторжений (COB);
- средства обнаружения атак (COA);
- intrusion detection system (IDS);
- Intrusion prevention system (IPS).

Задача IPS – «очистка» траффика.

Задача IDS – выявление и уведомление об атаках.

Функции средств выявления/предотвращения сетевых:

- сигнатурный анализ;
- поведенческий анализ;
- выявление аномалий;
- антивирусная защита;
- защита от DDoS.

# Противодействие сетевым атакам

---

Российские системы обнаружения сетевых атак:

- Континент IDS (Код Безопасности).
- Рубикон (НПО Эшелон).
- Форпост (РНТ).
- ViPNet IDS (Инфотекс)
- Altell NEO (АльтЭль)

Общие особенности продуктов:

- почти все имеют схожие источники сигнатур;
- почти все имеют функции только сигнатурного анализа.

Анонсировано появление IPS:

- Континент IPS



# Противодействие сетевым атакам

---

## Особенности продуктов

- Континент IPS:
  - наличие средств централизованного управления;
  - обнаружение DDoS атак;
  - анализ IPv6 трафика;
  - поддержка VLAN;
  - возможность интеграции с SIEM системами.
- COB Форпост:
  - наиболее производительное решение (более 1Г трафика).
- ViPNet IDS:
  - наличие средств централизованного управления и мониторинга.

Data Leak Prevention (DLP) – средства предотвращения утечек конфиденциальной информации.

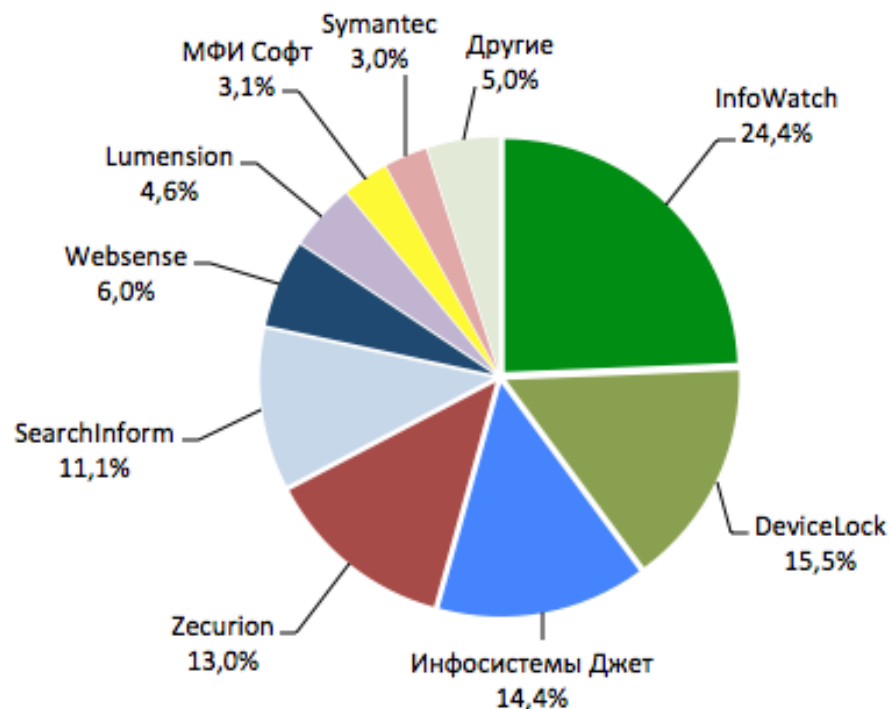
Назначение средств – контроль информационных потоков внутри ИС и на ее периметре с целью выявления отклонений от заданной политики безопасности.

Функции средств DLP:

- Категорирование информации методом «цифровых отпечатков» и ключевых слов.
- Контроль сетевого трафика на предмет передачи категорируемой информации.
- Контроль ОС и приложений на APM на предмет «перемещения» категорируемой информации.

# Контроль утечек конфиденциальной информации

- Solar Dozor 6.0 (Solar Security).
- Infowatch traffic monitor enterprise (ИнфоВотч).
- Zecurion (СекьюрИТ).
- DeviceLock (SmartLine Inc.).
- SearchInform.
- Iteranet (Итера ИТ).



Особенности российских средств - это «сплав» 5-х типов продуктов:

- средство контроля портов;
- средства контроля действий пользователя;
- средства анализа и проведения расследований;
- средства полного архивирования;
- DLP – средства категорирования информации и контроля ее перемещения.

Особенности российских средств:

- Solar Dozor 6.0
  - ближе всего к DLP и Forensic (средству проведения расследований).
- SearchInform
  - наиболее продвинутый функционал для контроля пользователя.
- Infowatch Traffic Monitor Enterprise
  - максимальное количество функциональных возможностей;
  - проблемы при переконфигурировании;
  - самый развитый Forensic.
- DeviceLock и Zecurion
  - распространённое средство контроля портов, развивающееся в сторону DLP.

АТР, Advanced Threat Protection – средства защиты от целенаправленных атак.

Комплексы, позволяющие выявлять в короткие сроки новые и неизвестный вредоносный код в различных каналах распространения.

Функции АТР:

- Контроль каналов распространения целенаправленных атак – электронная почта, веб, файлы.
- Запуск подозрительного содержимого и анализ происходящего на АРМ.
- Анализ трафика с центрами управления.

АТР от Лаборатории Касперского обеспечивает выполнение основных функций:

- контроль почтового трафика и веб трафика;
- выявление осуществляется за счет запуска в виртуальных машинах;
- контроль трафика на предмет выявления взаимодействия с центрами управления.

Планируется сбор расширенной информации с антивирусных агентов на рабочих станциях.

АТР от Positive Technologies является составным продуктом:

- Positive Technologies HoneyPot
  - основан на свободно распространяемой «песочнице».
- Positive Technologies Multiscanner
  - утилита для анализа содержимого файлов несколькими антивирусными ядрами (аналогично сервису [virustotal.com](http://virustotal.com)).



Задача средств контроля привилегированных пользователей – контроль (запись) действий администраторов ИС в защищаемых системах.

Российский продукты

- SafeInspect:
  - наличие необходимого функционала для контроля администраторов развитой инфраструктуры;
  - возможность внедрения системы без внесения изменений в конфигурацию сети.

Под продуктами данного класса имеет смысл рассматривать СЗИ, применение которых в сегментах АСУ ТП технологически возможно и принесет явную пользу.

В настоящее время на рынке известно о следующих СЗИ:

- Kaspersky Industrial CyberSecurity (в реестре)
- ViPNet SIES Core & Pack
- Контроллеры с функциями безопасности

Под продуктами данного класса имеет смысл рассматривать СЗИ для мобильных платформ.

В настоящее время на рынке известно о следующих СЗИ:

- iVlob - защищенный почтовый клиент для iOS с применением КриптоПро CSP 3.6.1.
- Мобильное рабочее место руководителя (iOS, Android) (в реестре)
- Tizen 2.4 + Infotecs VPN Client + SafePhone
- В разработке российские версии Tizen и SailFish

Задача – построить ИС на основе импортозамещённого ПО и СЗИ для рабочих станций. Из чего выбирать:

- СЗИ для РС в реестре:
  - Антивирус Касперского
  - Антивирус Dr.Web
  - SecretNet LSP
  - Континент АП
  - Infowatch
  - СЗКИ Крипто Про
- Операционные системы в реестре :
  - ОС Alt Linux
  - Astra Linux

# Складывается ли головоломка?

Задача – построить ИС на основе импортозамещённого ПО и СЗИ для рабочих станций.

СЗИ	Alt Linux	Astra Linux
Антивирус Касперского	-	+
Антивирус Dr.Web	+	+
SecretNet LSP	+	-
Континент АП	+	-
Инфотекс vpn client	-	-
Infowatch	-	-
Solar Dozor	-	+
СЗКИ Крипто Про	+	+

Серверные компоненты. Из чего выбирать:

- Операционные системы :
  - ОС Alt Linux, Astra Linux
- СУБД
  - Ред База Данных, Postgres Pro, СУБД «ARL», Линтер

СЗИ	Alt Linux	Astra Linux	Postgres	Линтер	СУБД «ARL»
Антивирус Касперского	-	-	-	-	-
Антивирус Dr.Web	+	+	+	-	-
SecretNet LSP	-	-	-	-	-
Infowatch	-	-	+	-	-
Solar Dozor	-	+	+	-	-

### Выводы:

- Изменения происходят очень быстро.
- В большинстве областей ИБ российские СЗИ доступны и есть из чего выбирать.
- По ряде случаев СЗИ сравнимы по функциональным возможностям с зарубежными аналогами.
- Не всегда можно обеспечить выполнение базовых требований ИБ только импортозамещенными средствами.

Спасибо за внимание

Вопросы?