Министерство образования Кировской области

«Обеспечение безопасности персональных данных»

Докладчик:

Городилов Сергей Викторович

Руководитель направления ИБ, АСПЕКТ-СЕТИ

gors@aspectspb.ru

46-56-46, 30-13-23

Важные замечания!!!

- Ответственность за реализацию конкретных правовых и организационных мер на своей территории и в рамках своей организации несет её руководитель
- Представленные материалы являются результатом опыта работы докладчика в данной сфере, основанного на доступных на данный момент времени трактовках законодательства,
- Представленные формы, материалы и презентации не являются официальной позицией государства в сфере персональных данных
- Официальную трактовку тех или иных позиций законодательства и нормативных документов в области персональных данных осуществляют: Министерство связи и массовых коммуникаций РФ, Роскомнадзор РФ (только в рамках контроля и надзора), Суды РФ, а также ФСБ, ФСТЭК, Роструд и другие органы власти в рамках своей сферы компетенции.

ПЛАН СЕМИНАРОВ

Организационно-правовая часть

№	Дата проведения	Тема
1.	23.11.2017	Основы информационной безопасности. Персональные данные и другие категории конфиденциальной информации. Законодательство и нормативные документы в области защиты персональных данных
2.	14.12.2017	Правовые меры защиты персональных данных - КАДРЫ
3.	18.01.2018	Правовые меры защиты персональных данных – Образовательная деятельность

Организационно-техническая часть

4.	08.02.2018	Организационные меры защиты персональных данных
5.	27.02.2018	Информационные системы персональных данных (ИСПДн)
6.	05.04.2018	Порядок защиты ИСПДн Технологические процессы обработки ПДн Угрозы безопасности ПДн Методика определения угроз
7.	20.04.2018	Реализация мероприятий ИБ, Аттестация, сертификация и лицензирование в области защиты персональных данных. Контроль защищенности

Семинары №6-7

ПОРЯДОК ЗАЩИТЫ ИСПДН

Общие шаги

1. Собрать информацию
2. Понять угрозы и риски
3. Сформировать мероприятия
4. Внедрить мероприятия
5. Оценить их эффективность
6. Эксплуатировать безопасно
7. Выводить из эксплуатации безопасно

Общие шаги

1. Собрать информацию
2. Понять угрозы и риски
3. **Сформировать мероприятия**
4. Внедрить мероприятия
5. Оценить их эффективность
6. Эксплуатировать безопасно
7. Выводить из эксплуатации безопасно

Шаги выбора технических мер

1) Определить комплекс мер
2) Оценить соответствие требованиям (21, 17 приказ ФСТЭК, 378 приказ ФСБ)
3) Определить, закрывают ли меры угрозы ИБ

Выполнение выбора мер с трех точек зрения (шагов) позволяет оценить эффективность выбранных мер.

Принципы выбора технических мер

- Использование продуктов с высокой репутацией и зрелостью
- Использование последних версий
- Наличие поддержки производителем
- Оперативное закрытие уязвимостей
- Оптимальные затраты на сопровождение в самой организации (в т.ч. по компетентности)

- Наличие сертификатов ФСТЭК/ФСБ (если есть обязательное требование)

Комплексы мер

- До 5 компьютеров
- До 30 компьютеров
- Более 30 компьютеров
- Распределенные географически

До 5 ПК - особенности

- Нет серверов
- Обработка ПДн идет на ПК
- Имеются выходы к внешним системам
- Есть доступ пользователей в Интернет
- Наиболее простое оснащение (ПК, версии Windows Home)

До 5 ПК -Рекомендации

На все рабочие места:

- Windows 7/8/8.1/10 Home/Pro
- Kaspersky Endpoint Security 10/11* + KSN**
- Обновление и мониторинг:
  - Через Интернет из облака (MS, Kaspersky);

- Режим сети: рабочая группа
- **Резервные копии**

Периметр сети:

- Отдельный роутер
- Межсетевой экран начального уровня (рекомендуется)

*Требуется для АРМ подключаемым к защищенной сети ЕИОС КО

** Облачный сервис Kaspersky Security Network, детектирующий более 50% угроз

До 30 ПК - особенности

- Наличие одного сервера (ПК с таким статусом)
- Обработка ПДн идет в ИС
- Есть учебный класс
- Имеются выходы к внешним системам
- Есть доступ пользователей в Интернет
- Наиболее простое оснащение (ПК, версии Windows Home/Pro)

5-30 ПК - рекомендации

На все рабочие места и серверы:

- Windows Server 2012/2012 R2/2016
- Windows 7/8/8.1/10 Home/Профессиональная
- Kaspersky Endpoint Security 10/11* + KSN**
- Обновление и мониторинг безопасности:
  - Windows Server Update Services или через Интернет
  - Kaspersky Security Center или через интернет
  - Встроенные средства Windows (журналы)
- Режим сети: рабочая группа или домен AD
- **Резервные копии**

Периметр сети и сегменты:

- Межсетевой экран начального уровня
- МЭ NGFW (рекомендуется)
- Отдельный сегмент учебных классов

*Требуется для АРМ подключаемым к защищенной сети ЕИОС КО

** Облачный сервис Kaspersky Security Network, детектирующий более 50% угроз

Более 30 ПК - особенности

- Наличие нескольких серверов (ПК с таким статусом)
- Наличие домена (редко его нет)
- Обработка ПДн идет в ИС
- Имеются выходы к внешним системам
- Есть доступ пользователей в Интернет
- Среднее оснащение (ПК, версии Windows Профессиональная, первая помощь)

Более 30 ПК - рекомендации

На все рабочие места и серверы:

- Windows Server 2012/2012 R2/2016
- Windows 7/8/8.1/10 Профессиональная
- Kaspersky Endpoint Security 10/11 + KSN
- Обновление и мониторинг безопасности:
  - Windows Server Update Services
  - Kaspersky Security Center
  - Встроенные средства Windows
- Режим сети: домен Active Directory
- **Резервные копии**

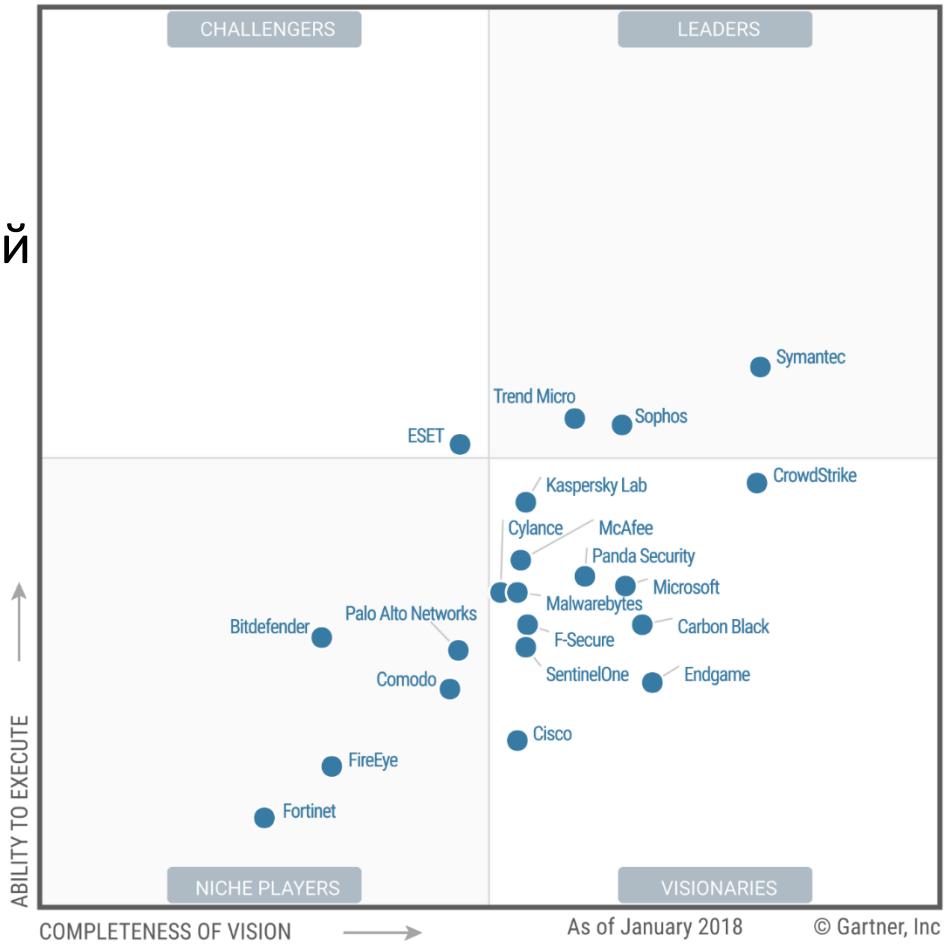
Периметр сети и сегменты:

- Межсетевой экран NGFW начального уровня
- Отдельный сегмент учебных классов (через межсетевой экран с запретом доступа в сегмент ИСПДн)

«Антивирусы»

Endpoint Protection, а не антивирус!

- Контроль запуска приложений
- Контроль активности приложений
- **Контроль устройств (включить!)**
- **Веб-контроль (включить!)**
- Антивирус:
  - Файловый
  - Веб-антивирус
  - Почтовый антивирус
  - Instant Messaging-антивирус
- Межсетевой экран
- Защита от атак (хост)
- Мониторинг системы
- Облачный сервис



Рекомендуемые «Антивирусы»

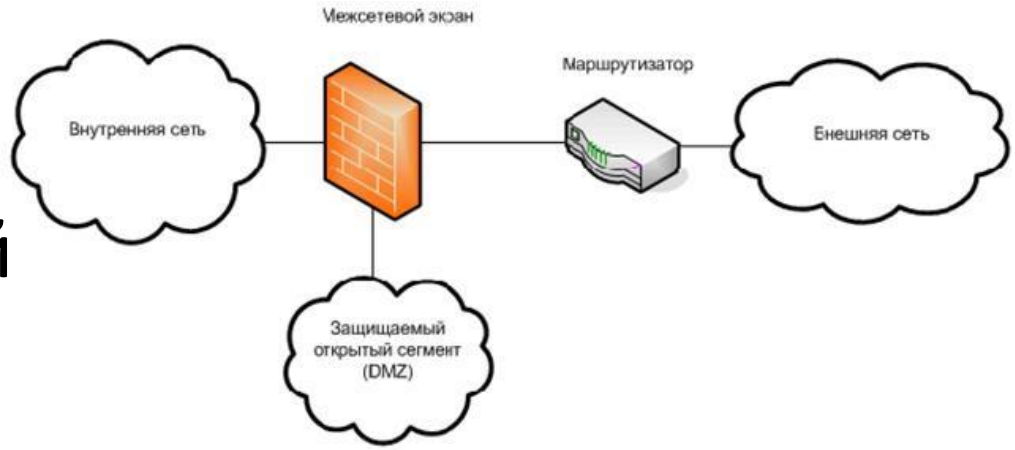
- Kaspersky Endpoint Security 10/11
- Symantec Endpoint Protection

EPP-продукты со средним уровнем защиты:

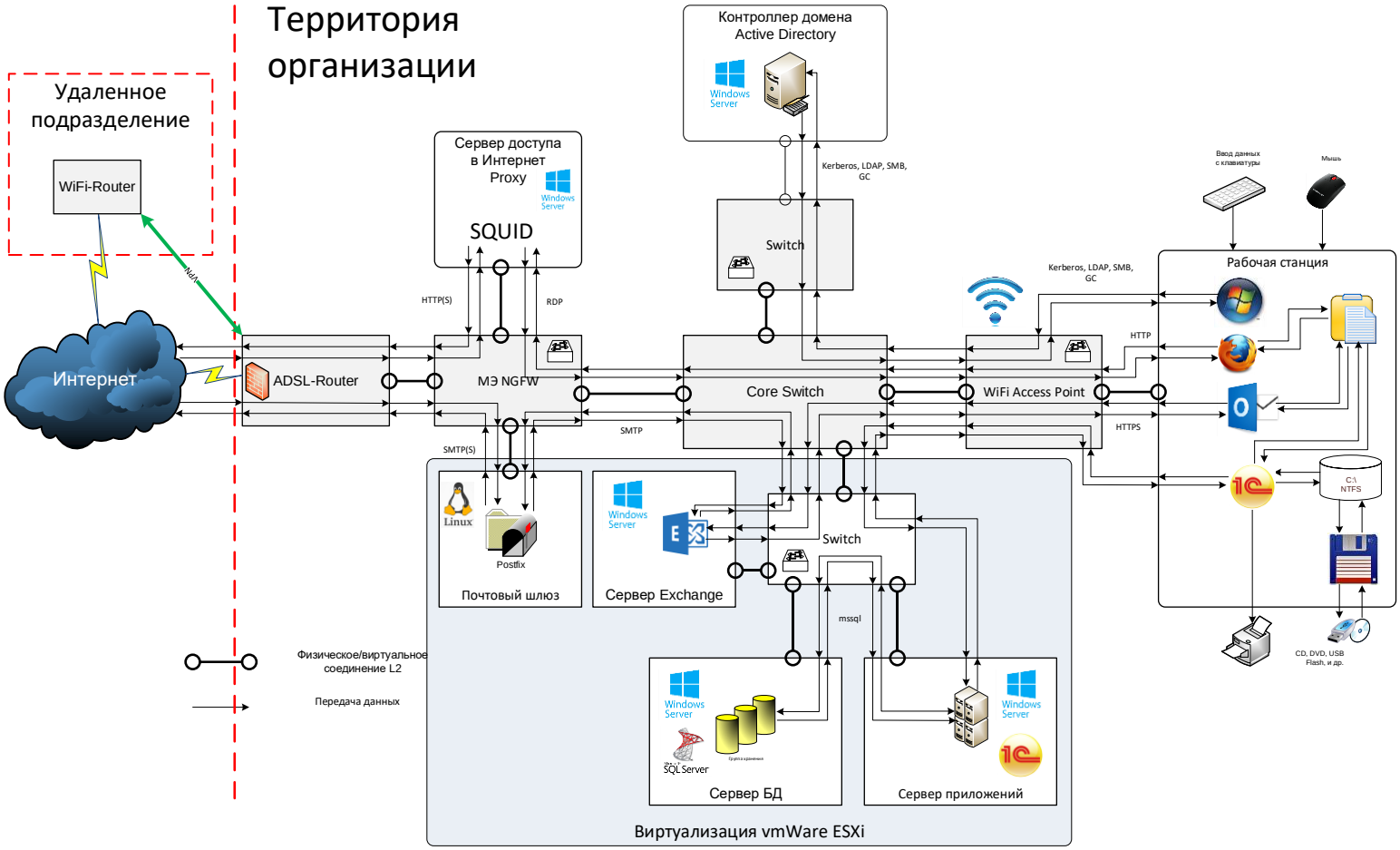
- 360 Total Security
- Avast
- Avira
- Windows Defender
- Др.

Межсетевые экраны - рекомендации

- Аппаратное исполнение
- Эшелонированный подход
- Next Generation Firewall



Эшелонирование

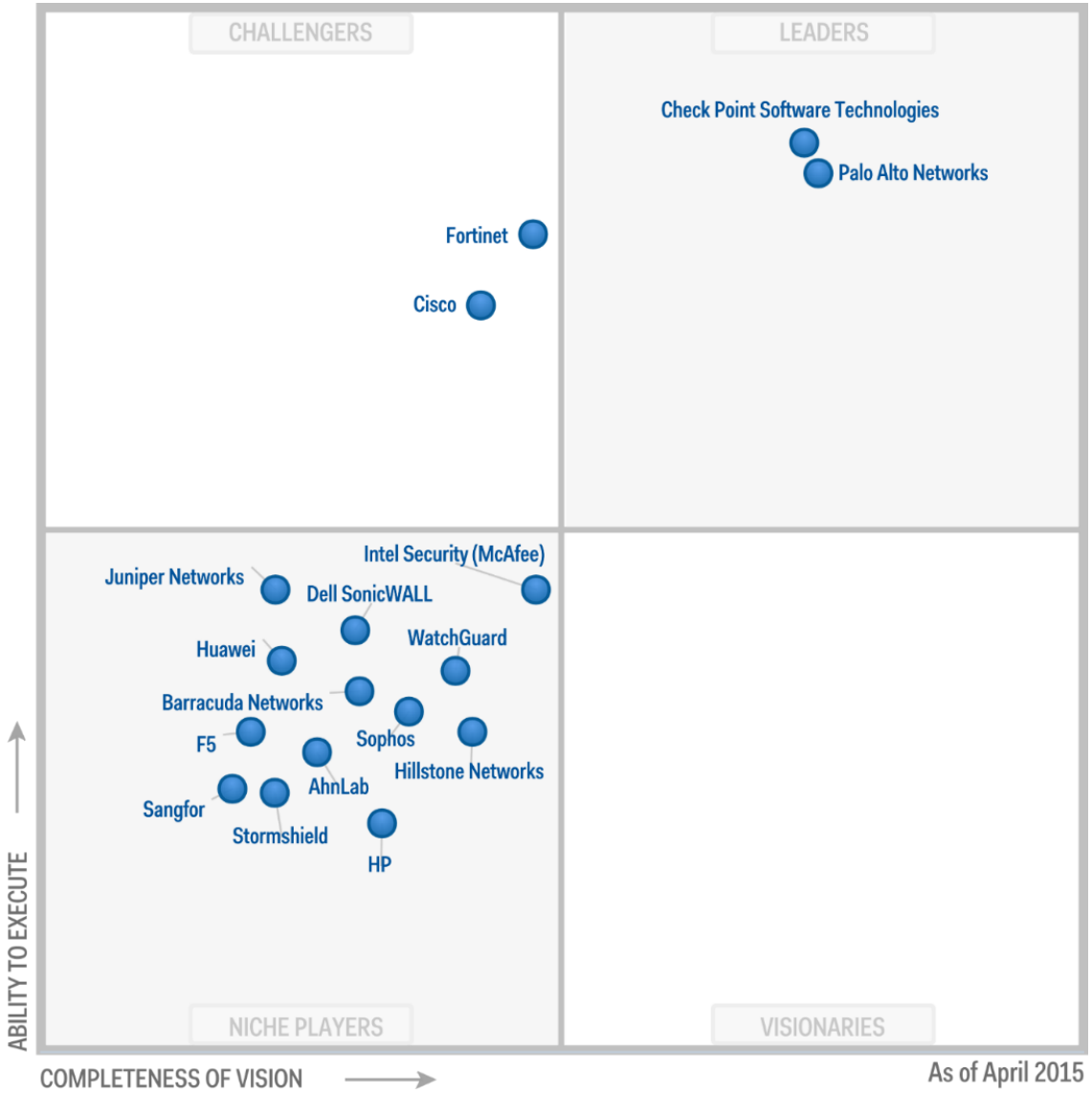


«Межсетевые экраны» NGFW

Next generation Firewall (NGFW) помимо фильтра пакетов и Stateful Inspection имеют:

- Intrusion prevention (предотвращение вторжений)
- Антивирус
- Антиспам
- Веб-прокси (прокси и прозрачный)
- Публикация приложений (реверс-прокси)
- Контроль приложений (десятки тысяч)
- Анти-бот
- Белые и черные списки IP
- Облачные сервисы ИБ

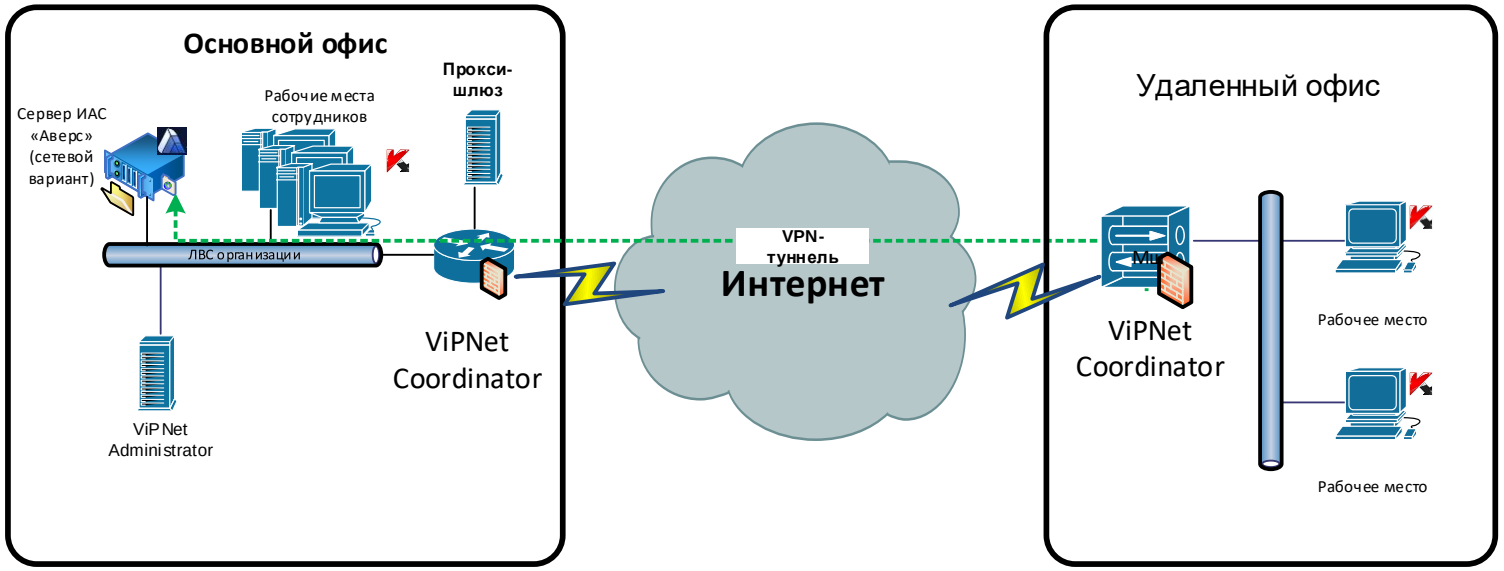
«Межсетевые экраны» NGFW



МЭ для малых организаций

- Zyxel Zywall USG 40/60/100
- Huawei USG 6320
- Fortinet 30E (имеет сертификат ФСТЭК)

VPN для защиты ПДн



Только сертифицированные ФСБ решения:

- ViPNet VPN 4 (Coordinator, Client, Administrator)
- АПКШ «Континент» 3.7
- S-Terra CSP VPN Gate 4

Беспроводной доступ WiFi

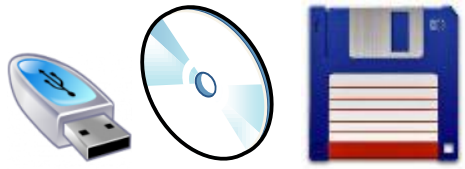
- Доступен снаружи зданий
- Злоумышленник может копировать незаметно
- Записанный трафик взламывается – вычислительные мощности есть

Рекомендации, если без WiFi нельзя:

- Использовать WPA2
- Скрытый SSID
- Регулярно менять пароль, и на устройствах ☹
- Ждать устройства с WPA3

Съемные носители информации

USB-flash, USB-HDD, CD, FDD и т.п.



- Ограничить в Kaspersky Endpoint Security
- Зарегистрировать в журнале
- Выдать под роспись ответственному лицу
- Записывать ПДн только на них

Оценка соответствия

- Определение уровня защищенности ПДн
- Определение перечня мер-требований
- Оценка комплекса мер по перечню мер-требований

ПП 1119 - Уровни защищенности ПДн

Тип ИСПДн	Категории субъектов	Количество субъектов	Тип актуальных угроз		
			1 тип	2 тип	3 тип
ИСПДн-С	Не сотрудников	Более 100 000	УЗ 1	УЗ 1	УЗ 2
		Менее чем 100 000	УЗ 1	УЗ 2	УЗ 3
	Сотрудников	Более 100 000	УЗ 1	УЗ 2	УЗ 3
		Менее чем 100 000	УЗ 1	УЗ 2	УЗ 3
ИСПДн-Б	Не сотрудников	Более 100 000	УЗ 1	УЗ 2	УЗ 3
		Менее чем 100 000	УЗ 1	УЗ 2	УЗ 3
	Сотрудников	Более 100 000	УЗ 1	УЗ 2	УЗ 3
		Менее чем 100 000	УЗ 1	УЗ 2	УЗ 3
ИСПДн-И	Не сотрудников	Более 100 000	УЗ 1	УЗ 2	УЗ 3
		Менее чем 100 000	УЗ 1	УЗ 3	УЗ 4
	Сотрудников	Более 100 000	УЗ 1	УЗ 3	УЗ 4
		Менее чем 100 000	УЗ 1	УЗ 3	УЗ 4
ИСПДн-О	Не сотрудников	Более 100 000	УЗ 2	УЗ 2	УЗ 4
		Менее чем 100 000	УЗ 2	УЗ 3	УЗ 4
	Сотрудников	Более 100 000	УЗ 2	УЗ 3	УЗ 4
		Менее чем 100 000	УЗ 2	УЗ 3	УЗ 4

99%

Приказ 21/17 ФСТЭК

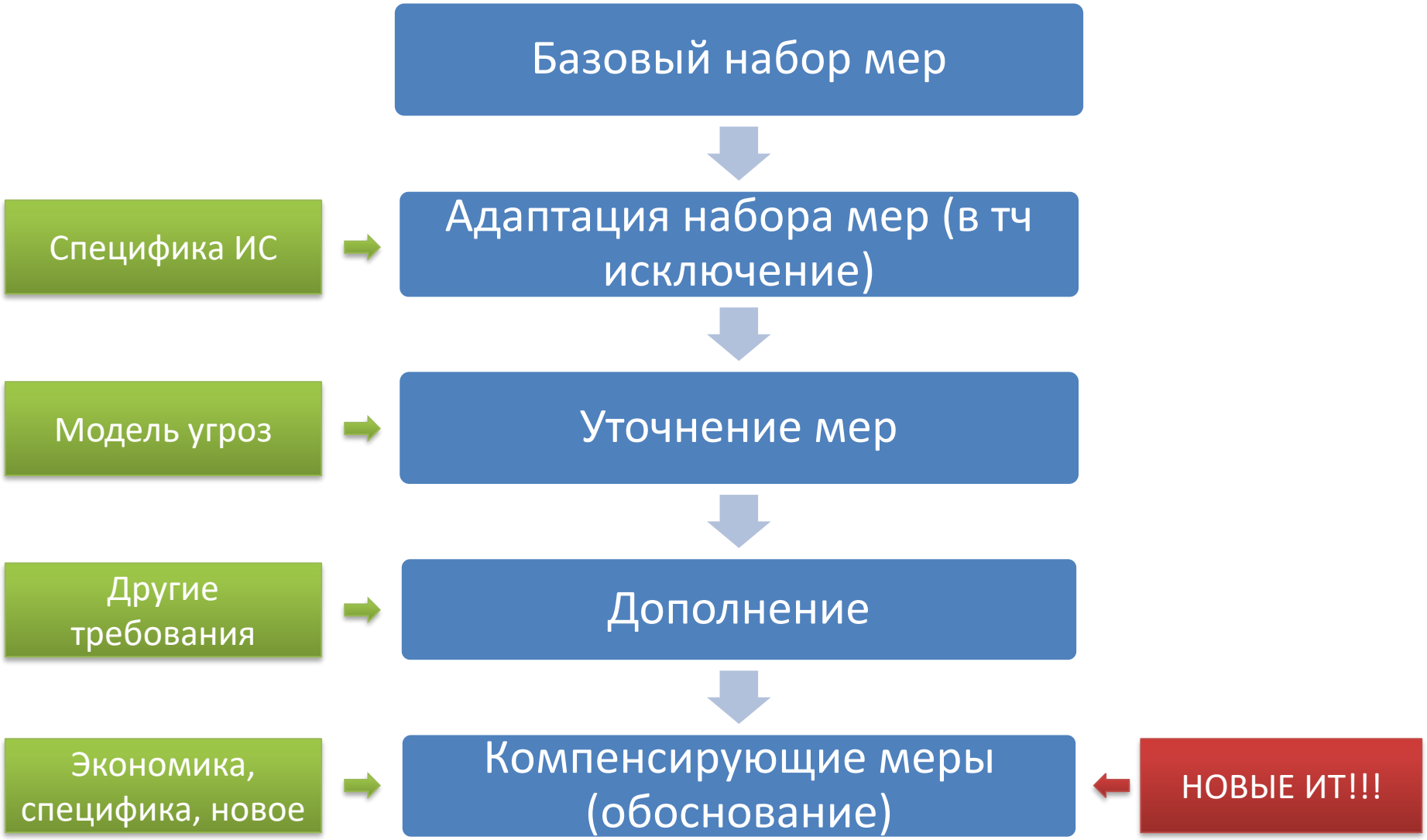
- идентификация и аутентификация (6);
- управление доступом (17);
- ограничение программной среды (4);
- защита машинных носителей информации (8);
- регистрация событий безопасности (8);
- антивирусная защита (2);
- обнаружение (предотвращение) вторжений (2);
- контроль (анализ) защищенности (5);
- обеспечение целостности (8);
- обеспечение доступности (7);
- защита среды виртуализации (10);
- защита технических средств (5);
- защита информационной системы, ее средств, систем связи и передачи данных (30);
- выявление инцидентов (6) – только в приказе № 21;
- управление конфигурацией ИС (4) – только в приказе № 21.

Итого: 109 мер.

Расширенный набор мер: итого

- Всего мер - 112
- Базовых мер для УЗ 4 - 27
- Базовых мер для УЗ 3 - 41
- Базовых мер для УЗ 2 - 63
- Базовых мер для УЗ 1 - 69
- Всего дополнительных (компенсирующих) мер - 40

Приказ ФСТЭК 21, 17
Процедура выбора мер



Пример протокола выбора мер и закрытия угроз ИБ

Общие шаги

1. Собрать информацию
2. Понять угрозы и риски
3. Сформировать мероприятия
4. **Внедрить мероприятия**
5. Оценить их эффективность
6. Эксплуатировать безопасно
7. Выводить из эксплуатации безопасно

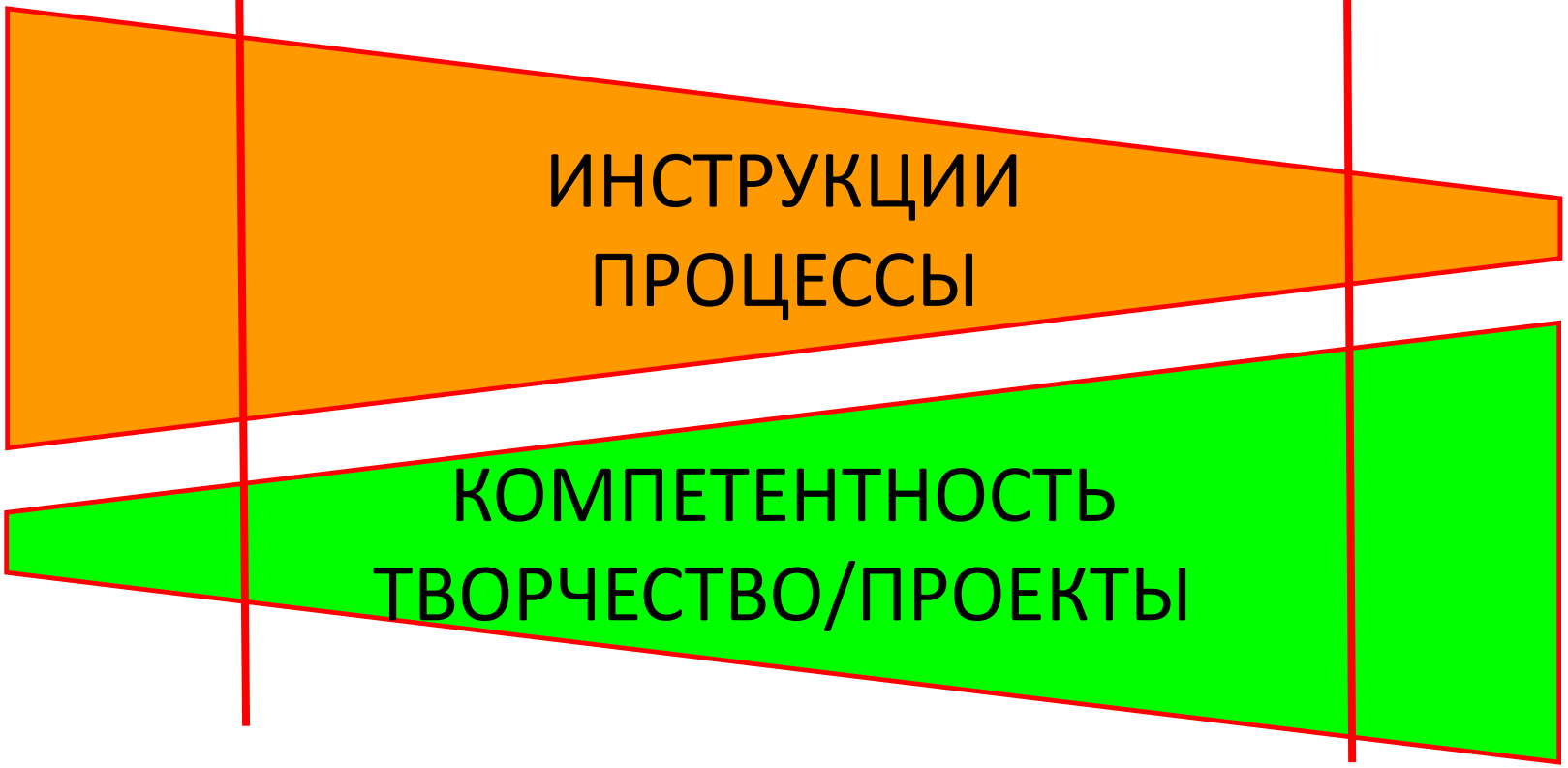
Внедрение мероприятий

- Назначение и доведение полномочий
- Установка и настройка технических средств
- Документирование

Уровень документирования

Система основана на детализации процедур и выстраивании процессов

Система основана на компетентности и квалификации персонала



Определение обязанностей

- Инструкция администратору безопасности
- Инструкция по безопасной обработке ПДн
- Инструкция по работе с носителями информации
- Инструкция по порядку резервирования и восстановления

Все инструкции в примерах.

Требуется адаптация!!!

Доведение обязанностей

- ТК РФ, ст.86 п.8) работники и их представители должны быть ознакомлены под роспись с документами работодателя, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области;

Компетентность

Ознакомление – доведение ответственности.

Компетентность – профессиональные качества, достигаемые через:

- Образование
- Обучение
- Тренинги
- Наставничество
- Информирование
- Опыт

При внедрении мер

Меры должны закрывать риски, связанные с уязвимостями в:

- технологиях (30%*);
- ПО и оборудовании (50%*);
- конфигурации (70%*);
- процессах (15%*);
- персонале (10%*);
- правовых мерах (облачные, аутсорсинг*).

*% от угроз в банке данных угроз ФСТЭК, содержит 207 угроз и 18317 уязвимостей в ПО и оборудовании

Документирование мер

Установить и контролировать:

- Схемы топологии сети
- Перечни защищаемых ресурсов
- Матрица доступа
- Конфигурация средств безопасности (архивы, текстовые файлы, xml, скриншоты)
- Журнал изменений

Общие шаги

1. Собрать информацию
2. Понять угрозы и риски
3. Сформировать мероприятия
4. Внедрить мероприятия
5. **Оценить их эффективность**
6. Эксплуатировать безопасно
7. Выводить из эксплуатации безопасно

Оценка эффективности мер

- Ввод в эксплуатацию коммиссионно
- Аттестация

Ввод в эксплуатацию

ИСПДн – по акту о вводе в ксплуатацию или приказу:

- Оценка эффективности
- Оценка соответствия

Государственные ИС:

- Аттестация
- П.17.3 – разрешена аттестация типовых сегментов

Аттестация

17 приказ ФСТЭК, ГОСТ РО 0043-003-2012 (ДСП):

- Разработка программы и методики испытаний
- Проведение испытаний
  - экспертно-документальный метод (по всем документам);
  - анализ уязвимостей информационной системы, в том числе вызванных неправильной настройкой (конфигурированием);
  - испытания системы защиты информации путем осуществления попыток несанкционированного доступа
  - тесты на проникновение (в будущем)
- Составление заключения
- Выдача аттестата соответствия (срок до 5 лет).

Лицензируемые виды деятельности

ФЗ-99 «О лицензировании отдельных видов деятельности»

ФСТЭК:

- Деятельность по технической защите конфиденциальной информации (ПП-79)

Лицензируемые виды деятельности

ФСБ (ПП-313):

- деятельность **по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств** (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя), осуществляемой юридическими лицами и индивидуальными предпринимателями

Исключения:

- техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя

Ваши вопросы?

Спасибо за внимание!

Городилов Сергей

Руководитель направления ИБ, АСПЕКТ СПб

gors@aspectspb.ru

www.aspectspb.ru