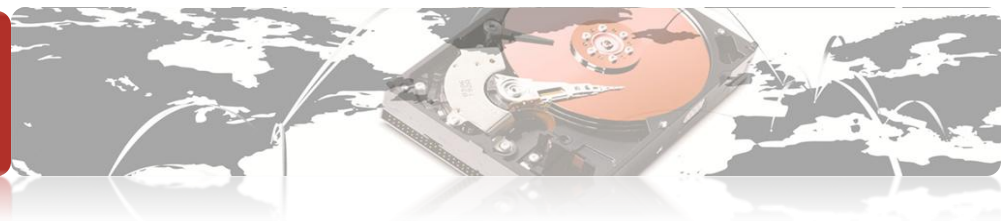


# Безопасность персональных данных. «Защитить нельзя игнорировать»



## О семинаре



- Цель: обсуждение вопросов организации обработки и обеспечения безопасности ПДн
- Формат: доклад + дискуссия (50/50 во время семинара)
- Основные вопросы:
  - Обзор ситуации в сфере обеспечения безопасности ПДн
  - Тенденции нормотворчества и правоприменения
  - Оптимизация ресурсов при создании СЗПДн
  - Отраслевые особенности обеспечения безопасности ПДн
  - Защита КИ + защита ПДн
  - Самостоятельная реализация СЗПДн
  - Особенности ведения проекта по обеспечению безопасности ПДн
  - Прогноз: что ожидает нас в части обработки ПДн
- Продолжение обсуждения возможно в кулуарах форума
- Материалы доступны на [inforion.ru](http://inforion.ru) после окончания выставки



## Обзор ситуации в сфере защиты ПДн (на март 2010 г.)

*«Хотели как лучше, а получилось как всегда»*

- Достойная цель, но проблемные пути ее достижения
- Отсутствие «баланса интересов» субъекта и оператора
- Жесткие требования (по организации обработки ПДн, по обеспечению безопасности ПДн)
- Недостатки нормативной базы сохраняются
- Высокая затратность при отсутствии видимой отдачи
- Выжидание как основная стратегия действий
- Группировка по отраслям и сферам деятельности (финансы и кредит, телеком, образование, здравоохранение)

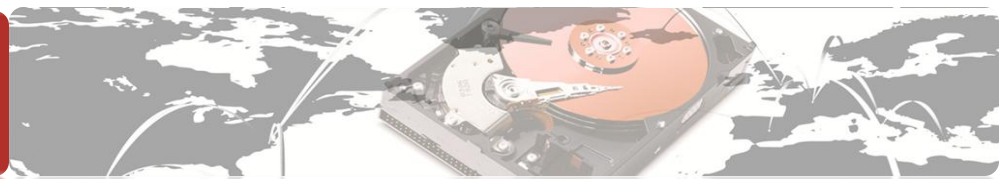
## Обзор ситуации в сфере защиты ПДн (продолжение)



- Активность «операторской» стороны (небывалое явление):
  - Инициативы по корректировке НПА
  - Обсуждения на форумах
  - Дискуссии в персональных блогах
  - Конференции, «круглые столы», семинары
- Появляется практика создания СЗПДн
- **Изменение отношения со стороны регуляторов**

Было	Стало
Стремление к изоляции специалистов	Участие в дискуссиях и обсуждениях
«Читайте документы, там все написано»	«Пожалуйста, обращайтесь, постараемся помочь»
«Документы проработаны, утверждены, потрудитесь исполнять»	Видна «работа над ошибками» (обсудим далее)

## Тенденции нормотворчества и правоприменения



*«Если долго мучиться - что-нибудь получится»*

### •Изменения в части нормативного обеспечения:

- «Четверокнижие» (уже «2+1-книжие») – не ДСП
- Новогодний подарок: поправки в 152-ФЗ
- Появление отраслевых требований, рекомендаций, методических указаний (Минобразования, Минздрав, АРБ, ...)
- Приказ ФСТЭК от 5 февраля 2010 г. № 58 (Положение о методах и способах защиты информации в ИСПДн)
- Решение от 5 марта 2010 г. об отмене «Основных мероприятий...» и «Рекомендаций...»

### •Правоприменение:

- Проверки есть, суровых санкций [пока] нет
- Иски есть, «громких дел» нет
- В большей степени проверяется организация обработки ПДн
- «Сигналы» от регуляторов разнонаправленные

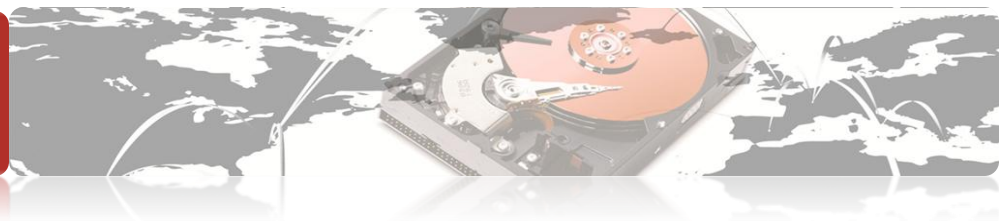
## Оптимизация ресурсов при создании СЗПДн (1)



*«Тот козел - особенный. У него на правой передней ноге серебряное копытце»*

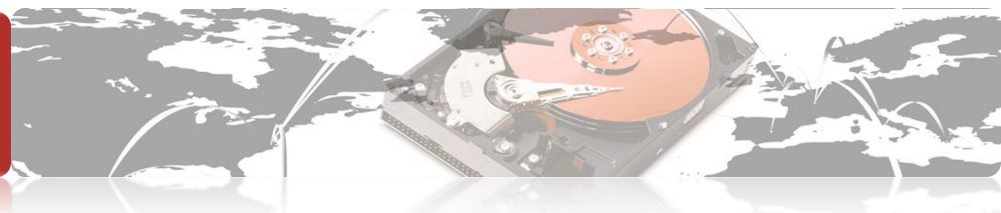
- В 99% случаев основным устремлением операторов является максимальное снижение расходов на создание СЗПДн
- Придумано множество способов «оптимизации расходов»:
  - Уменьшение количества АРМ, на которых ведется обработка ПДн
  - Исключение обработки ПДн из бизнес-процессов
  - Сегментация ИСПДн (в т.ч. «дробление» БД), изменение архитектуры
  - Отказ от обработки избыточной информации о субъектах ПДн
  - «Обезличивание» ПДн
  - Переход к обработке без использования средств автоматизации
  - ...и т.д.

## Оптимизация ресурсов при создании СЗПДн (2)



- Мы считаем, что понятию «оптимизация» более всего соответствует:
  - Построение реалистичной модели угроз и адекватная классификация ИСПДн (т.е. предъявление к СЗПДн только необходимых требований)
  - **Комплексная защита ПДн вместе с другой конфиденциальной информацией оператора**
- Не забываем про:
  - Альтернативные способы построения систем защиты (наложенные СрЗИ vs сертификация ПО, наложенные СрЗИ vs терминальные решения)
  - Использование имеющихся средств защиты и организационно-распорядительных документов
  - Возможность самостоятельно реализовать СЗПДн

ПДн + КИ = ?  
 ПДн + КИ = ☺!



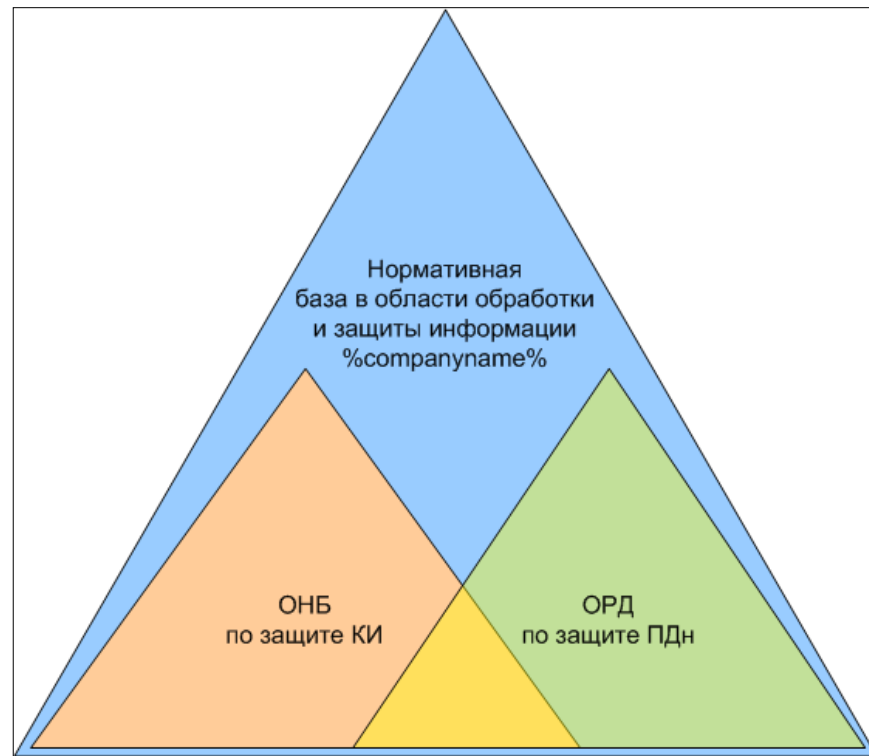
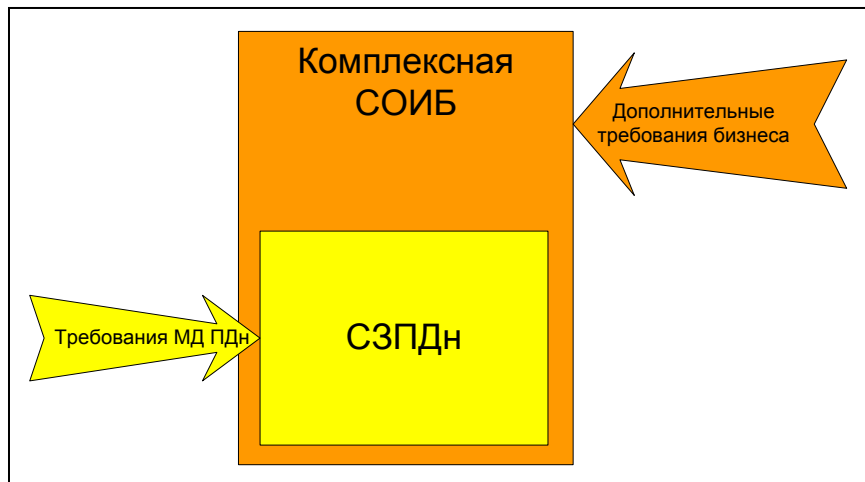
- Кто в теремочке живет?  
 - Я, мышка-норушка!  
 - Я, лягушка-квакушка!  
 - Я, петушок-золотой гребешок!

- Что в ИС обрабатывается?  
 - Я, служебная тайна!  
 - Я, коммерческая тайна!  
 - Мы, персональные данные!

Вопрос: почему охраняем только петушка?

- Безопасность КИ за шумихой вокруг ПДн незаслуженно забыта
- Между тем, логичным решением является интегрированная защита:
  - Дешевле реализация
  - Лучше управляемость
  - Синергетический эффект

ПДн + КИ = ?  
 ПДн + КИ = ☺!



- Единая техническая система
- Интегрированный пакет ОРД
- Централизация управления
- Расширенное поле требований и механизмов безопасности

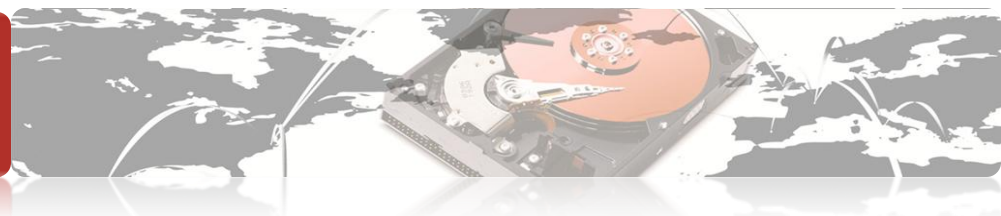
## Отраслевые особенности обработки и защиты ПДн



*«И швец, и жнец, и на дуде игрец?»*

- Дифференциация по отраслям касается в первую очередь вопросов организации обработки ПДн
- Вспомним слайд № 3: в чем причины группировки по отраслям и сферам деятельности? Ответ: разные законы регулируют разные сферы деятельности
- От этого зависят организационные аспекты обработки ПДн:
  - Установление правового основания обработки
  - Необходимость подачи уведомления об обработке ПДн
  - Организация процесса сбора ПДн
  - Организация процесса обработки ПДн
  - Организация процесса получения согласий субъектов на обработку их ПДн
  - Определение сроков хранения ПДн
  - Определение условий прекращения обработки ПДн

## Самостоятельная реализация СЗПДн



*«Я знаю точно - невозможное возможно»*

- Факторы, свидетельствующие в пользу возможности самостоятельной работы по защите ПДн
  - Готовность тратить на проработку мероприятий в области защиты ПДн ресурсы своего персонала
  - До 20% операторов имеют необходимые квалифицированные кадры для разработки и реализации СЗПДн
  - Методические документы регуляторов доступны
  - В конце концов, это обязанность оператора (ст. 19 Федерального закона №152-ФЗ)
  - Несложно обратиться за методической поддержкой лицензиата. Это стоит в разы меньше полного комплекса услуг

*Вечный спор на тему: «что лучше – аутсорсинг или свои ресурсы?» выносим за скобки (не предмет семинара)  
Ответ на вопрос «Нужна ли лицензия?» будет дан тремя слайдами ниже*

## На что обратить внимание при строительстве СЗПДн



*«Корабли лавировали-лавировали, да не вылавировали»*

### •Здесь только общие рекомендации:

- Желательно не пренебрегать предпроектным аудитом
- Целесообразно воспользоваться некоторыми положениями отмененных МД (в части организации работ)
- При классификации ИСПДн есть возможность идти «от ущерба» (обсудим особенности)
- Особое внимание – составлению модели угроз
- Глубокое документирование как для организационного, так и для технического уровня
- СЗПДн не должна ухудшать производительность и надежность защищаемой ИСПДн
- Запуск СЗПДн не только «на бумаге», но и на практике

## Краткий обзор новых требований (1)

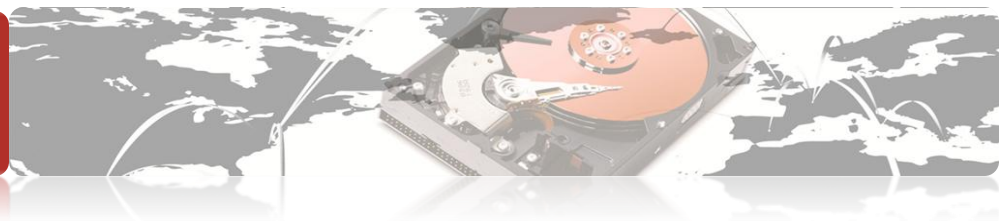


*«За одного битого двух небитых дают»*

*Дополнительно к заявленной программе семинара рассматриваются аспекты применения «Положения о методах и способах...», введенного в действие приказом ФСТЭК № 58 от 5 февраля 2010 г.*

- «Положение ...» утверждено руководителем службы, зарегистрировано в Минюсте
- С принятием «Положения...» принципиальных изменений в подходах к обеспечению безопасности ПДн не произошло
- Выполненные оператором наработки по «4-книжке» не выбрасываются на свалку
- ПДн-гостайна и СКЗИ по-прежнему за рамками «Положения...»
- Установлено два направления защиты: от угроз НСД и от угроз утечки по ТК

## Краткий обзор новых требований (2)



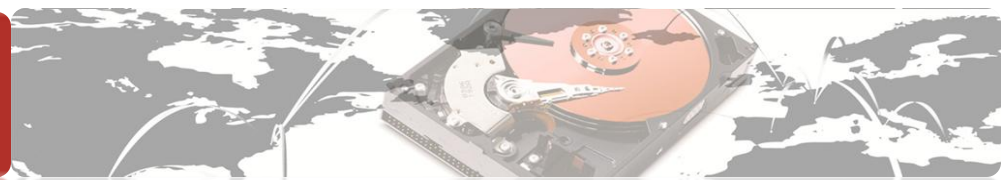
### • Кто защищает?

- может назначаться структурное подразделение или должностное лицо
- может привлекаться организация, имеющая лицензию на ТЗКИ (ранее это было только в МД ФСБ)

### • «Основные мероприятия...» отменены, необходимость получения лицензии сохраняется:

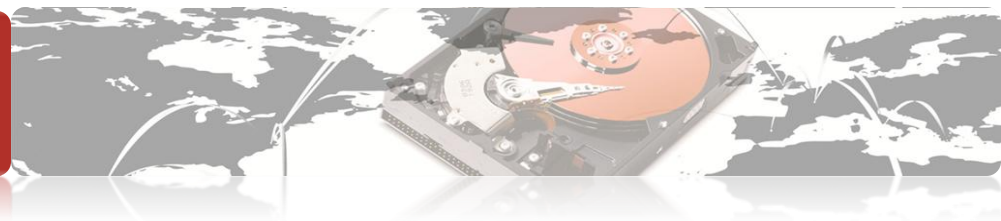
- См. ФЗ «О лицензировании отдельных видов деятельности»
- См. Положение о лицензировании деятельности по ТЗКИ
- Известно о попытках инициировать изменения ФЗ «О лицензировании...» - добавить формулировку «за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд»
- Выбор методов и средств – на основе МУ и в зависимости от класса

## Краткий обзор новых требований (3)



- Определен перечень методов и способов:
  - реализация разрешительной системы допуска пользователей
  - ограничение доступа в помещения, где размещены ТС и носители
  - разграничение доступа к информационным ресурсам, СОИ, СрЗИ
  - регистрация действий, контроль НСД и действий
  - учет и хранение съемных носителей информации
  - резервирование технических средств
  - использование СрЗИ, прошедших процедуру оценки соответствия
  - использование защищенных каналов связи
  - размещение ТС в пределах охраняемой территории
  - организация физической защиты помещений и ТС
  - предотвращение внедрения в ИС вредоносных программ и программных закладок
- Подсистемы (РД) → Мероприятия (МД «4-кн.») → Функции (МД «2+1-кн.»)

## Краткий обзор новых требований (4)



• Более детально проработаны вопросы межсетевого взаимодействия:

- «ИСПДн + сеть общего пользования»
- «ИСПДн + сеть общего пользования с целью получения общедоступной информации»
- «При удаленном доступе к ИСПДн через сеть общего пользования»
- «При межсетевом взаимодействии отдельных ИСПДн через сеть общего пользования»
- «При межсетевом взаимодействии отдельных ИСПДн разных операторов через сеть общего пользования»

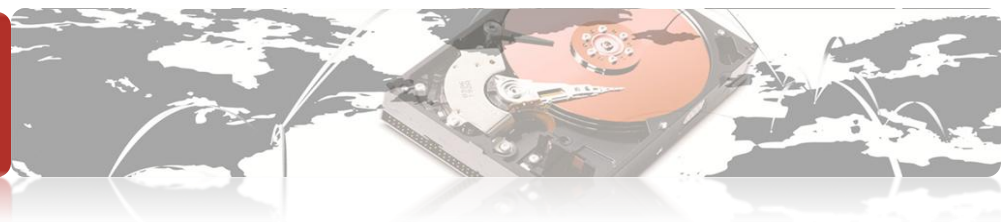
## Краткий обзор новых требований (5)



• Для заданных типов таких взаимодействий добавляются еще т.н. «основные методы и способы»

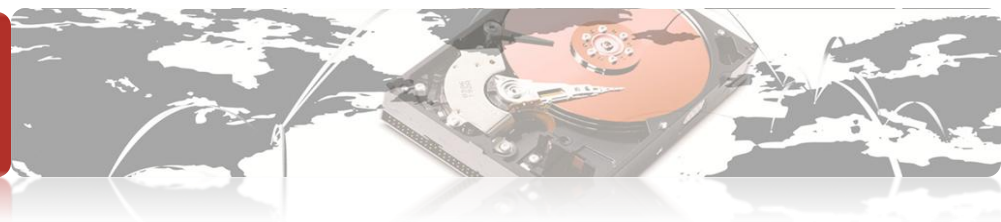
- межсетевое экранирование
- обнаружение вторжений
- анализ защищенности (сканеры безопасности)
- защита информации при ее передаче по каналам связи
- использование надежной идентификации и аутентификации пользователей
- использование средств антивирусной защиты
- централизованное управление СЗПДн
- фильтрация входящих (исходящих) сетевых пакетов по правилам
- периодический анализ (имитация внешних атак)
- активный аудит безопасности
- анализ принимаемой информации
- проверка подлинности отправителя и целостности данных
- управление доступом
- использование атрибутов безопасности
- создание канала связи, обеспечивающего защиту передаваемой информации
- осуществление аутентификации взаимодействующих информационных систем
- обеспечение предотвращения возможности отрицания факта отправки/получения ПДн

## Краткий обзор новых требований (6)



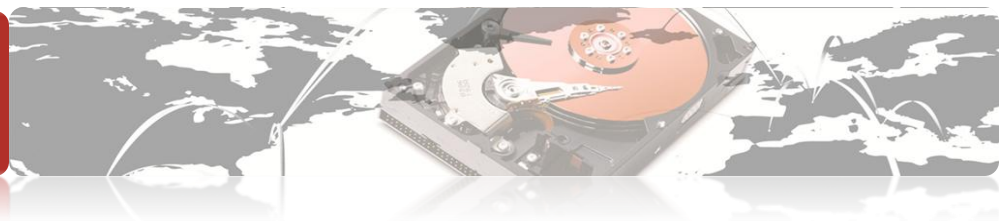
- Контроль отсутствия НДС:
  - Для ИСПДн 1 класса – по 4 уровню контроля отсутствия НДС
  - Для ИСПДн 2 и 3 класса – на усмотрение оператора
- По методам и способам защиты ИСПДн 2 и 3 класса уравниены, практически соответствуют 1Д по РД АС
- По методам и способам защиты ИСПДн 1 класса практически соответствуют 1Г по РД АС

## Краткий обзор новых требований (7)



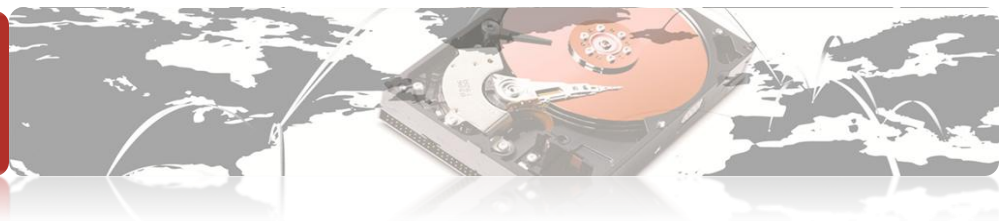
- Требования к применяемым МЭ:
  - ИСПДн 3 класса – 5 класс защищенности по РД МЭ (+ одно требование для 4 класса)
  - ИСПДн 2 класса – 4 класс защищенности по РД МЭ
  - ИСПДн 1 класса – 3 класс защищенности по РД МЭ
- Анализ защищенности - для распределенных ИС и для ИС, подключенных к сетям международного информационного обмена
- Обнаружение вторжений - для информационных систем, подключенных к сетям международного информационного обмена

## Наш прогноз развития ситуации



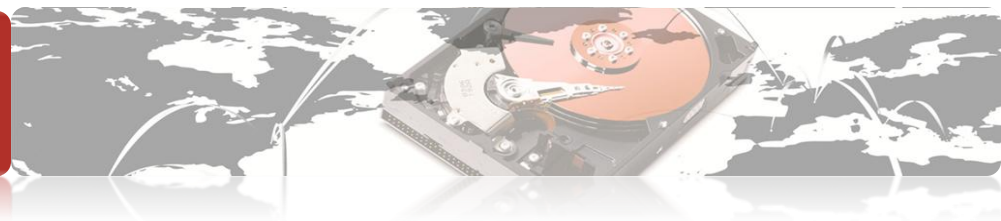
- Рынок ожидает принятия второго пакета поправок к 152-ФЗ, их появление станет существенным стимулом к выходу из «подвешенного» состояния большей части операторов
- При отсутствии громких скандалов из-за утечек ПДн активность регуляторов и жесткость санкций будет нарастать постепенно
- Ожидается появления отраслевых норм, учитывающих специфику конкретных видов деятельности
- Следует ожидать роста числа сертифицированных ФСТЭК программных продуктов и средств защиты информации
- В целом - умеренный оптимизм: «верхи могут, низы хотят» (появляется обратная связь, происходят изменения в законодательстве, нарабатывается опыт)

Поставим точку над *i*



**Персональные данные: защитить нельзя игнорировать**

## Контактная информация



**Россия, Москва**

**107023, ул. Большая Семеновская 45**

**Тел/факс: +7 (495) 730-74-88**

**Электронная почта: [info@inforion.ru](mailto:info@inforion.ru)**

**Адрес в сети Интернет: <http://www.inforion.ru/>**