

Руководителю  
образовательной организации  
об информационной  
безопасности

МАОУ ДПО ЦИТ,  
© Аникин Юрий, 2016

# Основные направления

- ◎ Защита детей от доступа к информации, несовместимой с целями образования
- ◎ Защита информационных систем общего назначения
- ◎ Защита информационных систем персональных данных

# Защита детей от нежелательной информации

- ◎ Нормативные документы
- ◎ Организационные меры
- ◎ Комплекс аппаратных средств и программных решений

# Безопасный Интернет. Нормативные документы

- ◎ Нормативные документы и шаблоны размещены на нашем сайте по адресу:  
<http://www.tgl.net.ru/ib/normativ/>
- ◎ Нельзя бездумно утверждать локальные акты; необходимо доработать размещенные шаблоны для своего учреждения

# Безопасный Интернет.

## Основные рекомендации

- ◎ Настоятельно рекомендуем ознакомиться с рекомендациями, размещенными по адресу:  
[http://wiki.tgl.net.ru/index.php/Категория:Безопасность в Интернет](http://wiki.tgl.net.ru/index.php/Категория:Безопасность_в_Интернет)
- ◎ Если осознание или выполнение каких-либо рекомендаций вызывает затруднения, обратитесь к специалистам

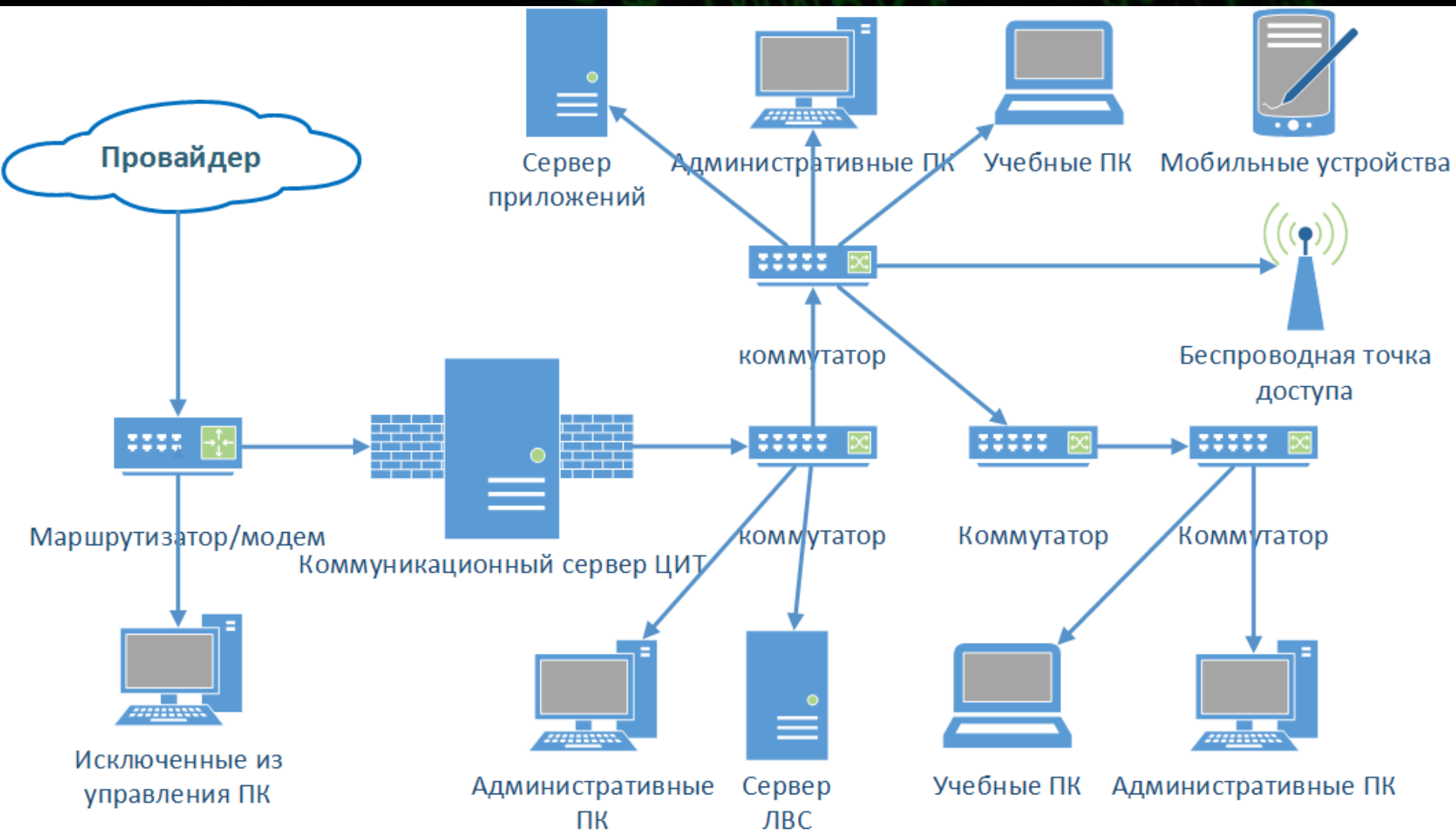
# Безопасный Интернет. Организационные меры

- ◎ Регламентация доступа в Интернет для различных групп пользователей и контроль соблюдения принятых регламентов
- ◎ Организация повышения квалификации для различных групп пользователей

# Безопасный Интернет. Технические решения

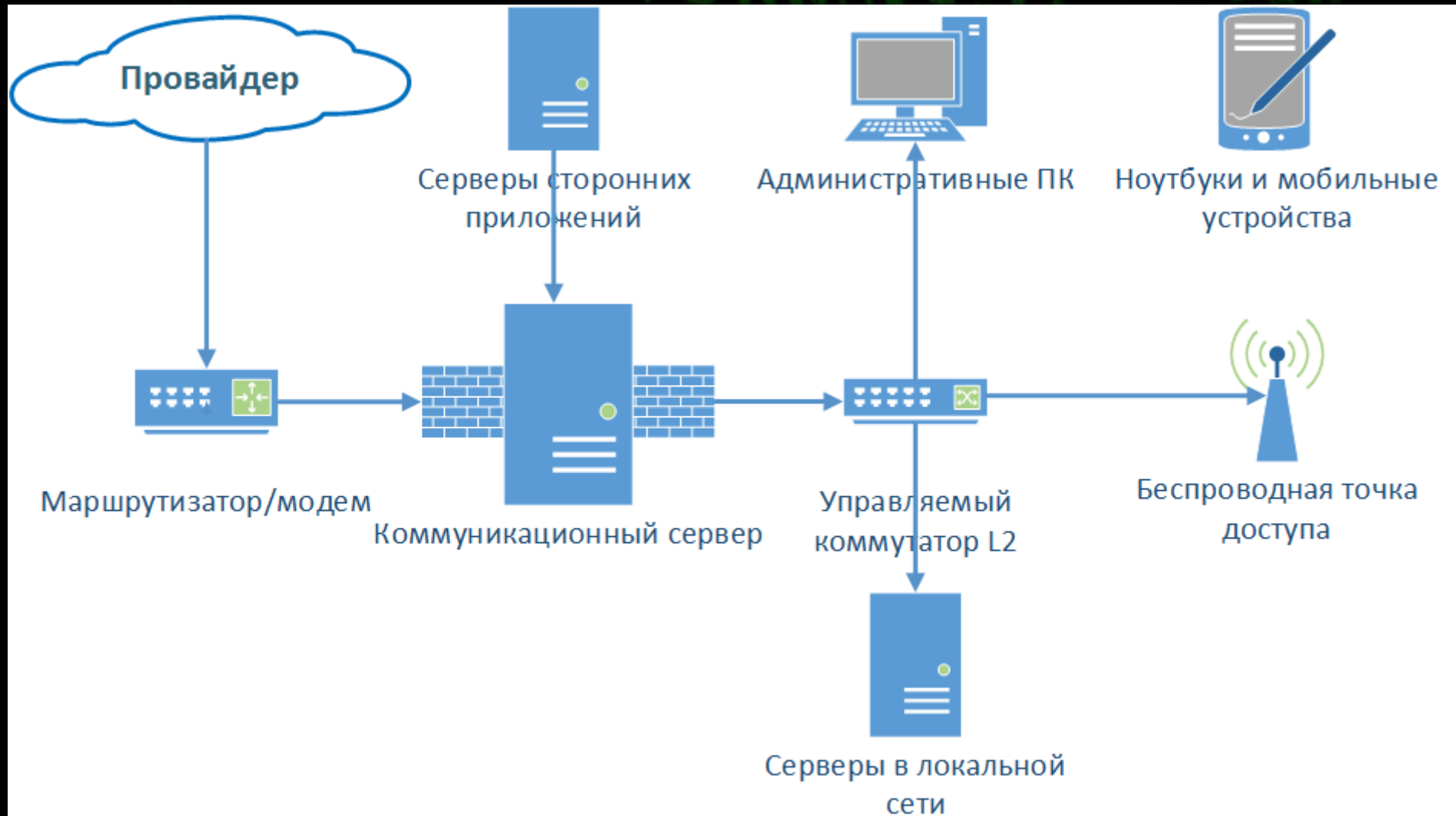
- ◎ Централизованное управление сетью
- ◎ «Поголовная» аутентификация пользователей и компьютеров
- ◎ Журналирование действий пользователей
- ◎ Системы фильтрации трафика и предотвращения вторжений
- ◎ Антивирусные средства
- ◎ Безопасность автоматизированного рабочего места

# Технические решения. Построение сети «как проще»





# Технические решения. Построение сети «как лучше»



# Технические решения. Аутентификация

- ◎ Определение полномочий пользователя
- ◎ Предоставление доступа к ресурсам в зависимости от полномочий
- ◎ Возможность протоколирования действий пользователя

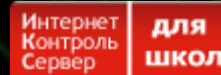
# Индивидуальные системы контентной фильтрации

- NetPolice Child -- 300 руб на 1ПК/год
- KinderGate -- 490 руб на 1 ПК/год
- Kaspersky SafeKids -- 900 руб на 1 ПК/год
- Hidetools Parental Control -- \$40 на 1ПК/год
- Child Control 2015 -- \$30 на 1 ПК/2 года
- Детский браузер Гугуль -- бесплатно
- Фильтрация по доменным именам:  
YandexDNS, SkyDNS

# Серверные системы контентной фильтрации

- ◎ Интернет Контроль Сервер *бесплатно для дома*, цена для ОУ зависит от кол-ва пользователей

Специальная поставка для учебных учреждений



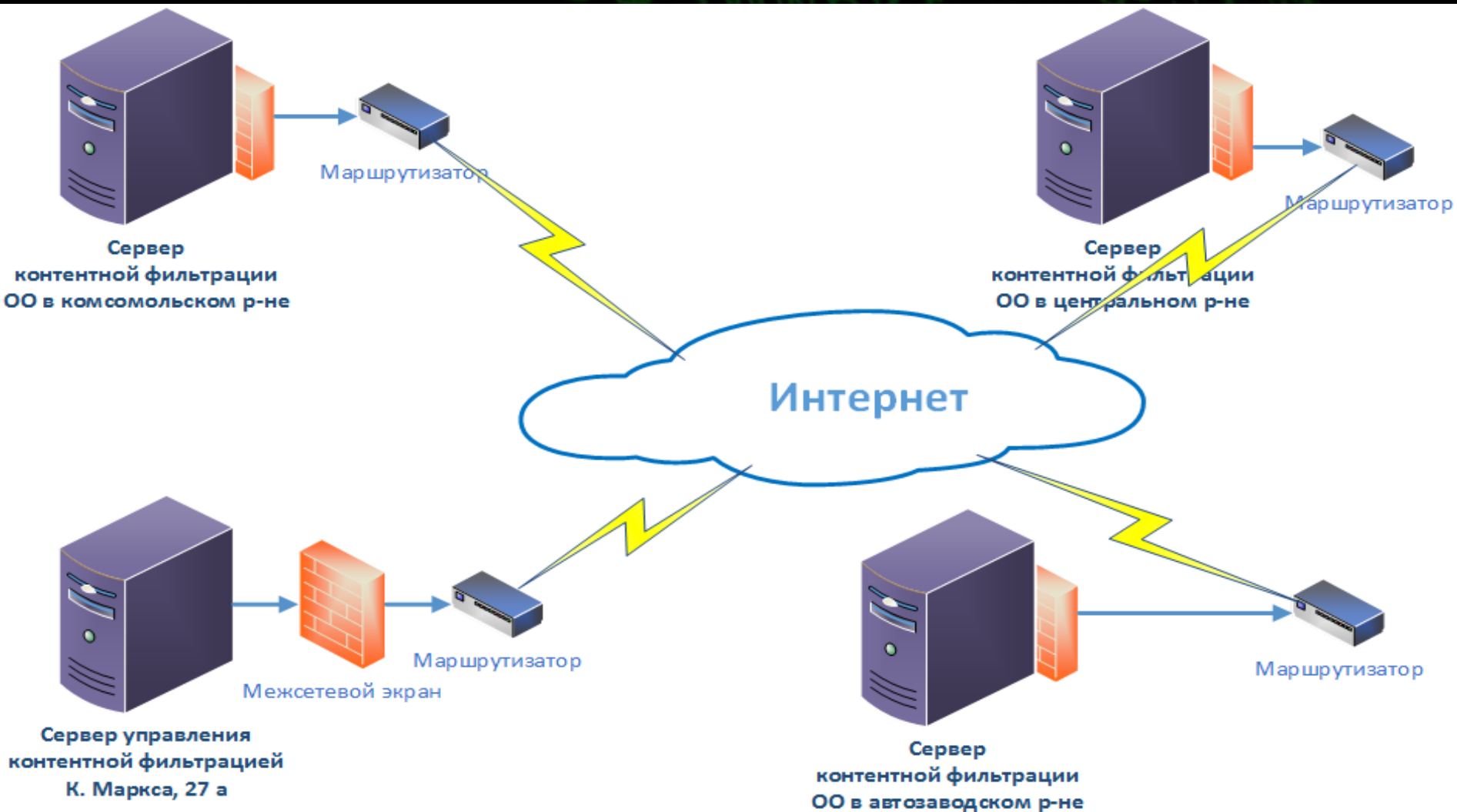
Пользователи	Программа	Аппаратное решение (сервер+программа)	Переход на версию ФСТЭК	Пакет "Обновления"	Пакет "Обновления+Поддержка"
100	6 600	48 600	10 200	2 000	4 000
200	13 200	55 200	18 000	3 000	6 000
свыше 200	26 400	214 400	24 000	4 500	9 000

# Серверные системы контентной фильтрации

## ◎ UserGate UTM

Продукт	Кол-во лицензий	Сумма, руб
Приобретение права на использование UserGate UTM	200	142100
Подписка Security Updates (1 год) для UserGate UTM	200	42630
Модуль Advanced Threat Protection (1 год) для UserGate UTM	200	42630
Антивирусный модуль Касперского (1 год) для UserGate UTM	200	42630
Модуль Mail Security для UserGate UTM	25	9420
ИТОГО:		279410

# Коммуникационный сервер с фильтрацией контента



# Политика фильтрации

- ⦿ Запрещено всё сетевое взаимодействие, кроме явно разрешенного
- ⦿ Фильтрация по «белым спискам»
- ⦿ Фильтрация по «черным спискам»
- ⦿ Фильтрация по регулярным выражениям (шаблонам) типа «sex», «порно»
- ⦿ Фильтрация по лексемам (от др. –греч. λέξις — слово, выражение, оборот речи) и устойчивым словоформам (группам ассоциированных слов) в полной мере не реализована

# Защита ИС общего назначения

- ◎ Каждый пользователь должен пройти аутентификацию для доступа к ресурсам
- ◎ Подключение каждого устройства к сети должно быть санкционировано
- ◎ Электронные журналы избавляют от необходимости вести бумажные «для проверяющих»



# Защита ИС общего назначения. Разграничения полномочий

- ◎ Каждому пользователю предоставляются полномочия не более необходимых
- ◎ Создание или изменение каждого ресурса санкционируется и документируется
- ◎ Доступ к каждому ресурсу предоставляется только необходимым группам пользователей
- ◎ Каждый ресурс сопровождается только ответственными лицами

# Защита ИС общего назначения.

## Обеспечение надежности

- ⦿ Для каждого ресурса и компонента анализируются риски отказа функционирования
- ⦿ Для наиболее критических ресурсов и компонентов применяется дублирование и резервирование
- ⦿ Для каждого критического ресурса
  - выбираются компоненты повышенной надежности
  - обеспечивается качественное и бесперебойное электропитание

# Защита ИС общего назначения.

## Антивирусные средства

### ◎ На каждом АРМ

- должен быть установлен антивирус
- должны быть настроены задачи обновления баз и проверки жесткого диска

### ◎ Каждый пользователь должен уметь работать с антивирусом и соблюдать правила обработки входных и выходных данных

# Защита ИС общего назначения. Резервное копирование

- ◎ Для каждого ресурса
  - документируются на бумаге его параметры и процесс восстановления
  - регламентируется резервное копирование и тестируется восстановление
- ◎ Выполнение данных процедур регулярно контролируется ответственными лицами

# Защита ИС общего назначения. Ответственность пользователя

- ◎ Регламентируются права и обязанности пользователей при использовании ресурсов ЛВС и Интернет
- ◎ Постоянно осуществляется контроль действий пользователей, сотрудников обслуживающих организаций
- ◎ Регулярно осуществляется повышение квалификации пользователей

# Защита ИС общего назначения.

## Работа с почтой

- ◎ Не будьте чрезмерно доверчивы при разборе почты
- ◎ Не открывайте вложения непосредственно из писем
- ◎ Настройте и используйте спам-фильтры
- ◎ Настройте обязательную антивирусную проверку входящих и исходящих писем

# Спасибо за внимание!

◎ Вопросы?

◎ Контакты для связи: Аникин Юрий

◎ Тел. (8482)-329-727