АКАДЕМИЯ
ЦИФРОВЫХ ТЕХНОЛОГИЙ

Практические моменты обеспечения информационной безопасности образовательного учреждения

Докладчик: Артем Рачеев,
заместитель директора по ИКТ, методист, педагог ДО
ГБНОУ «Академия Цифровых Технологий»

Меры обеспечения ИБ в ОУ

- Технические
- Нормативные
- Административно-организационные

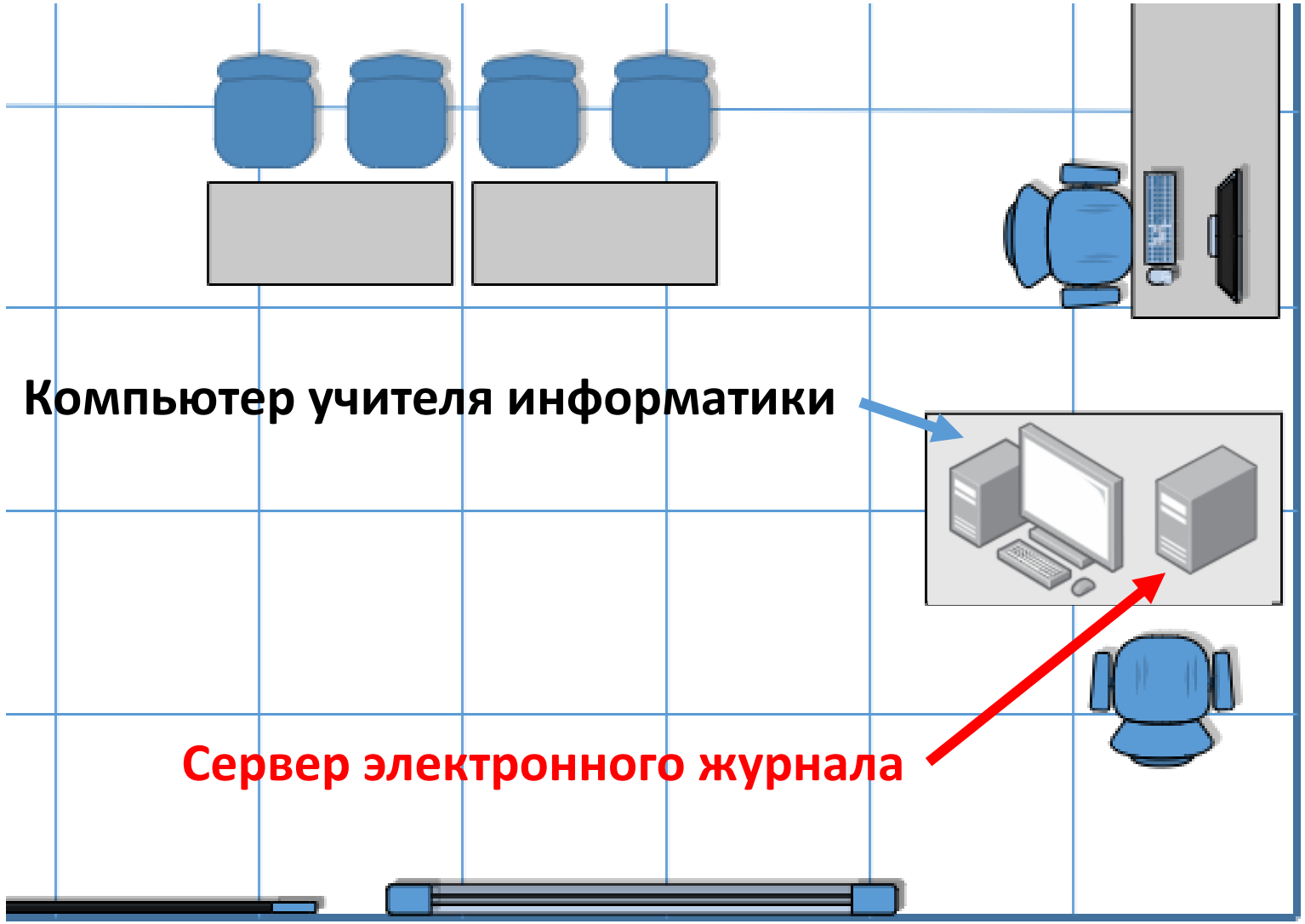
Физическая безопасность

- Не размещайте сервера и важное оборудование в помещениях с неограниченным или слабо ограниченным доступом
- Своевременно обслуживайте механические элементы оборудования
- Не располагайте компьютерную технику рядом с объектами, содержащими воду, пыль, грязь и т.п.

Физическая ~~без~~опасность

Рисунок 1:

Фрагмент схемы компьютерного класса в школе Н



Политика безопасных паролей

- Никогда не используйте пароли по умолчанию
- Не используйте один пароль для нескольких ресурсов
- Используйте двухфакторную аутентификацию
- ~~Менять пароли раз в X лет~~
- Не сохранять пароли в браузерах и т.п.
- Не использовать в качестве пароля общедоступные данные владельца
- Чем длиннее и сложнее пароль - тем лучше

Обновление ПО (с осторожностью)

Обновления функционала

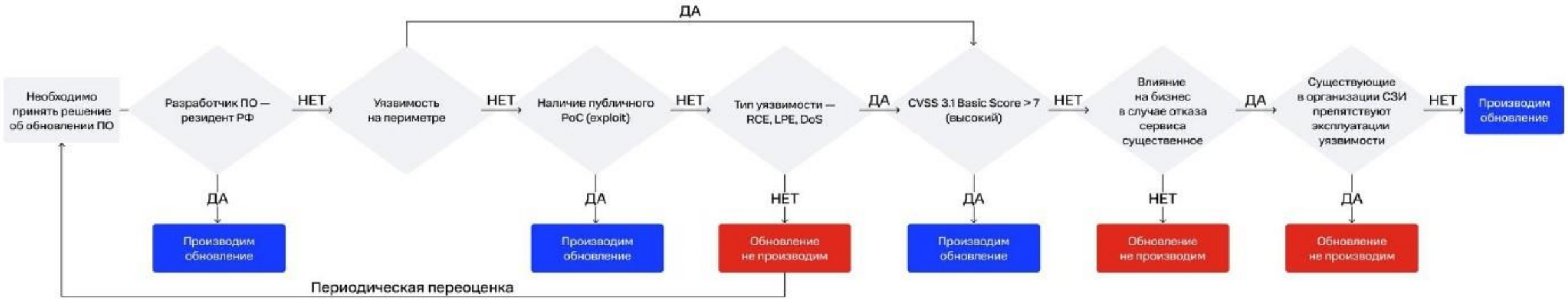
- Появляются новые функции
- Новые функции могут иметь недоработки
- Могут приводить к проблемам с безопасностью

Обновления безопасности

- Не содержат существенных изменений функционала
- Устраняют имеющиеся или потенциальные «уязвимости»

В текущих геополитических реалиях были неоднократно «Зафиксированы случаи внедрения разработчиками программного обеспечения (ПО) из недружественных Российской Федерации стран, недокументированных возможностей или добавления механизмов блокировки работы ПО.»

Алгоритм НКЦКИ*
для принятия решений необходимости обновления критичного ПО



* Национальный координационный центр по компьютерным инцидентам России (НКЦКИ, создан ФСБ)

Главная проблема информационной безопасности «среднестатистического» ОУ

Рисунок 2:
Схема ЛВС школы К

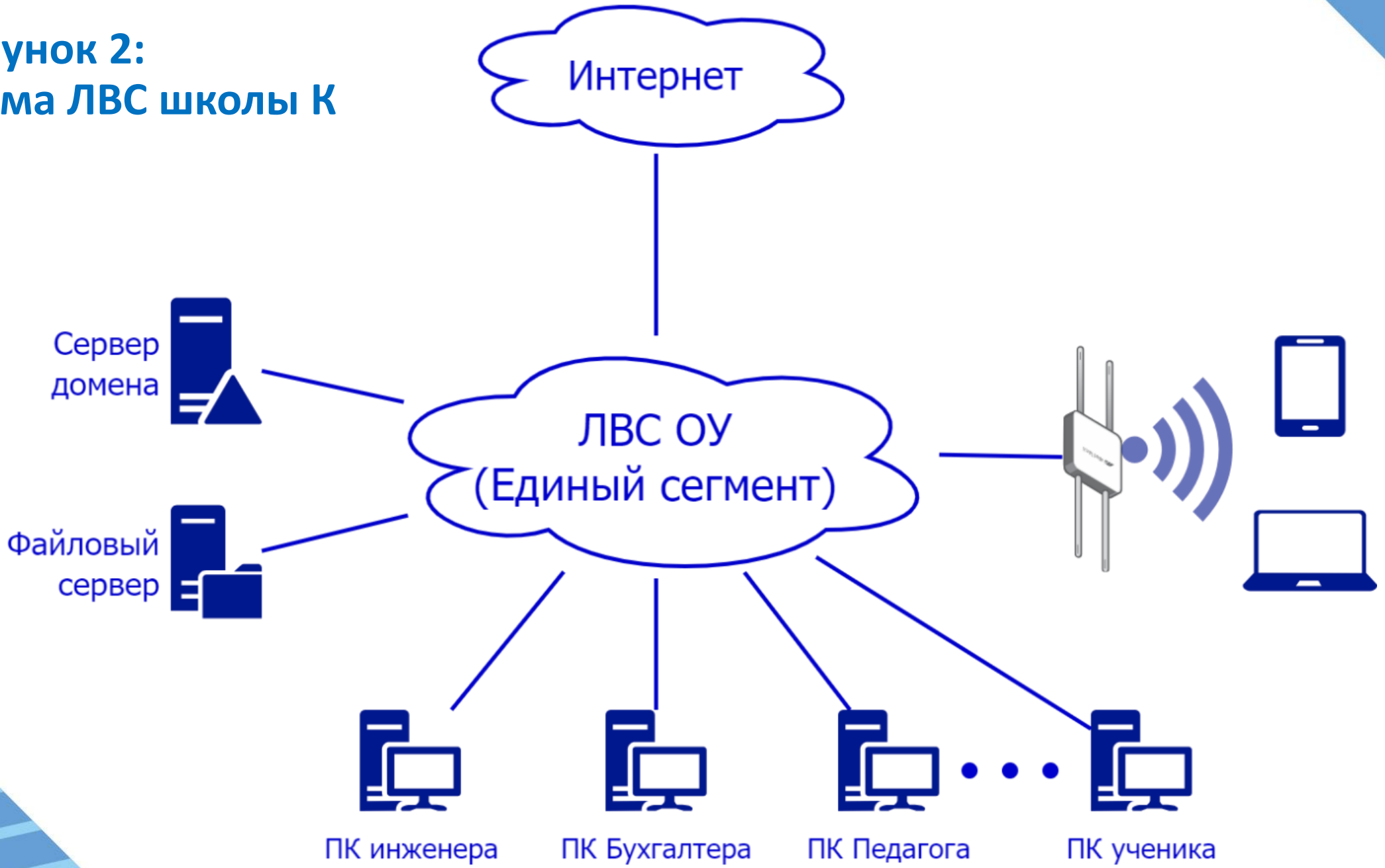


Рисунок 2.1:
Схема ЛВС школы К
С правами доступа

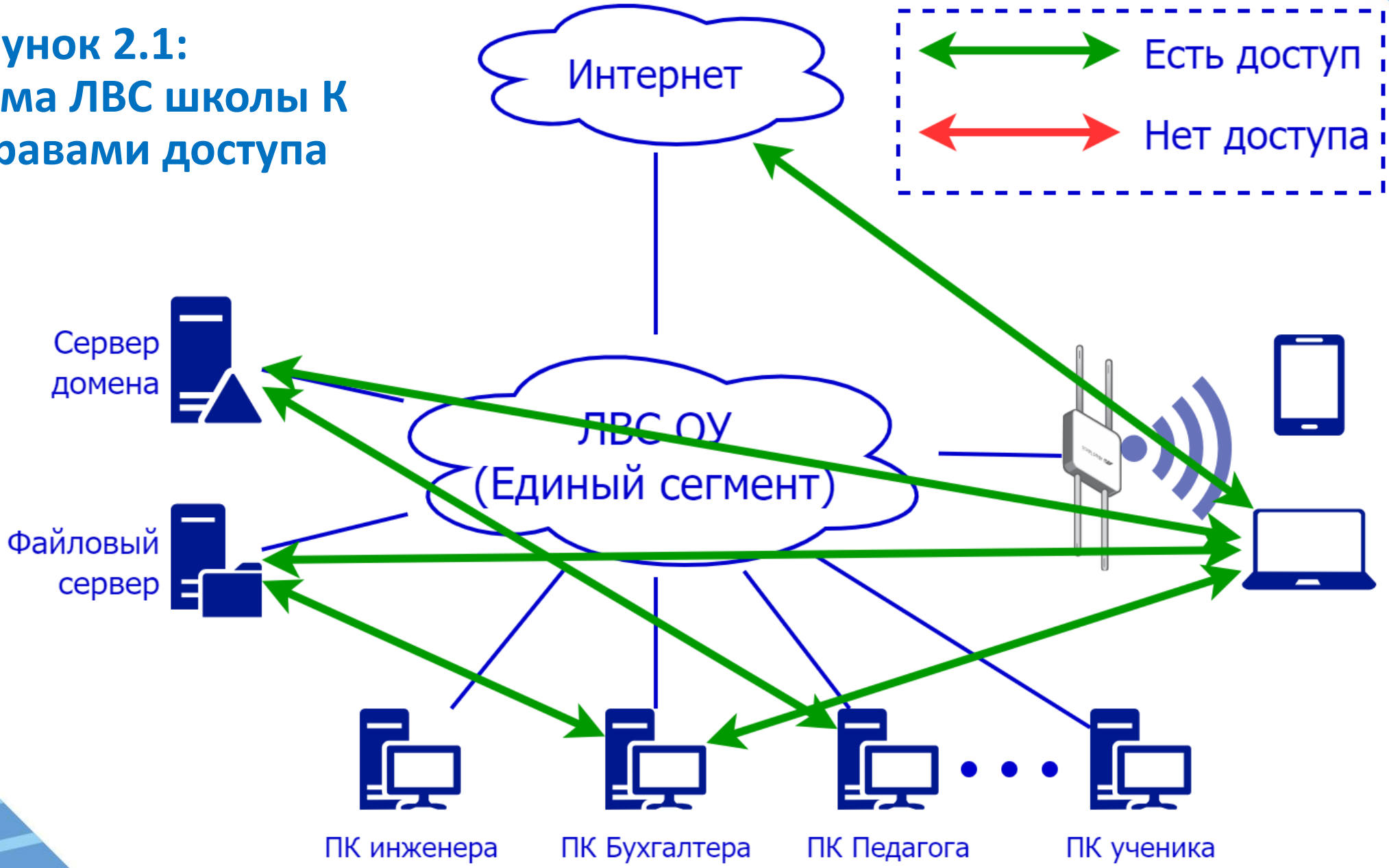


Рисунок 3:
Схема ЛВС школы К
С соблюдением мер ИБ

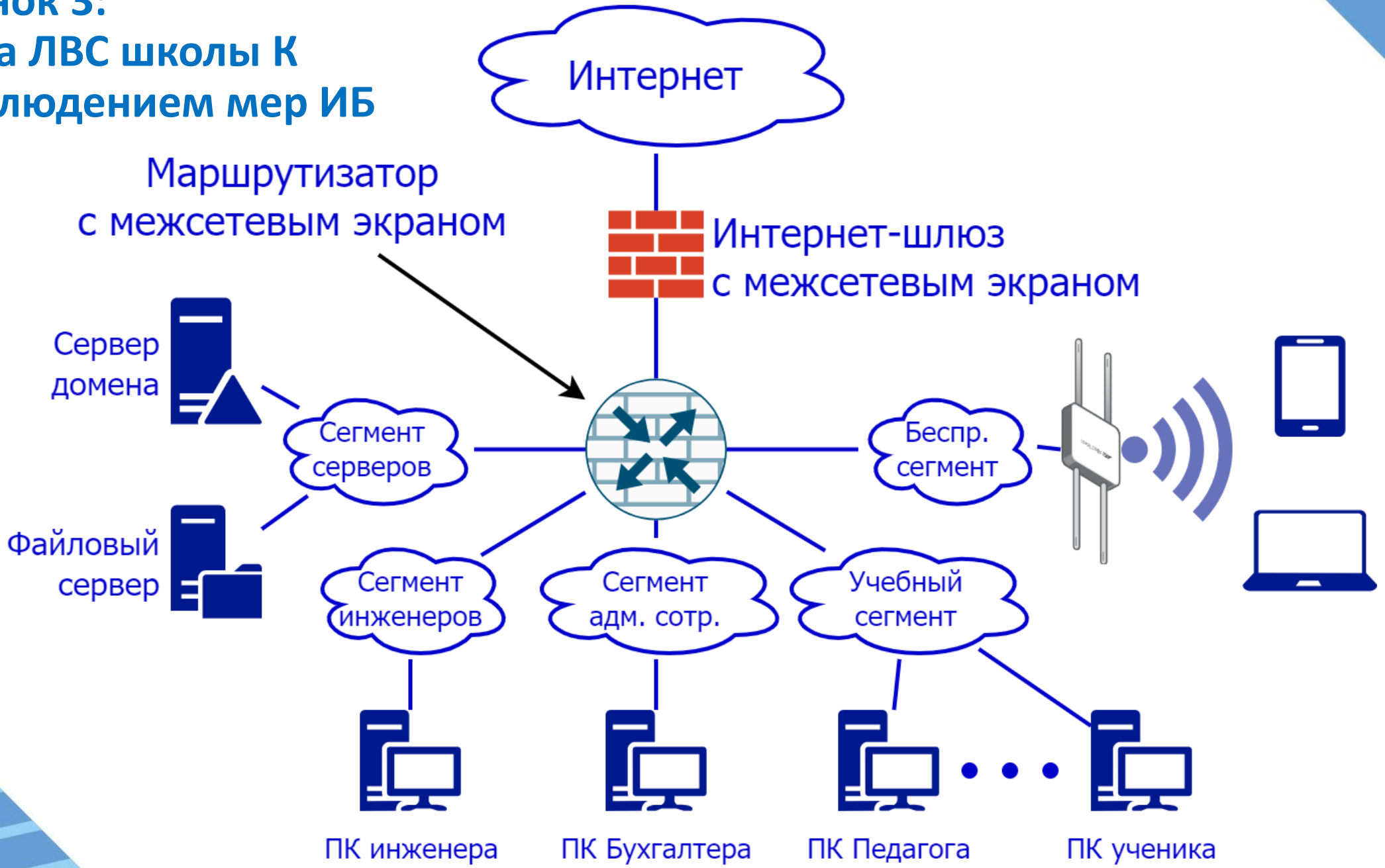
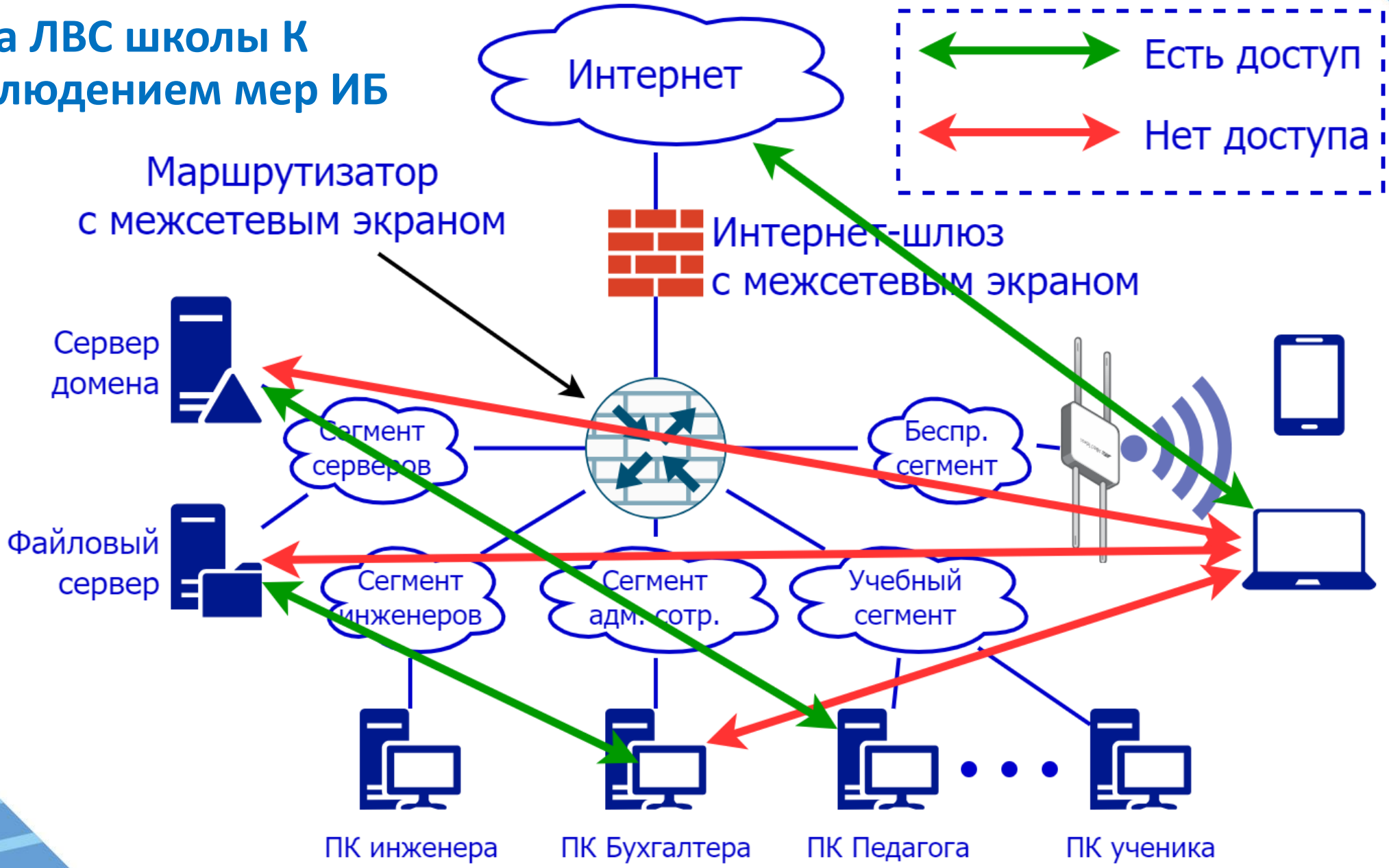


Рисунок 3:
Схема ЛВС школы К
С соблюдением мер ИБ



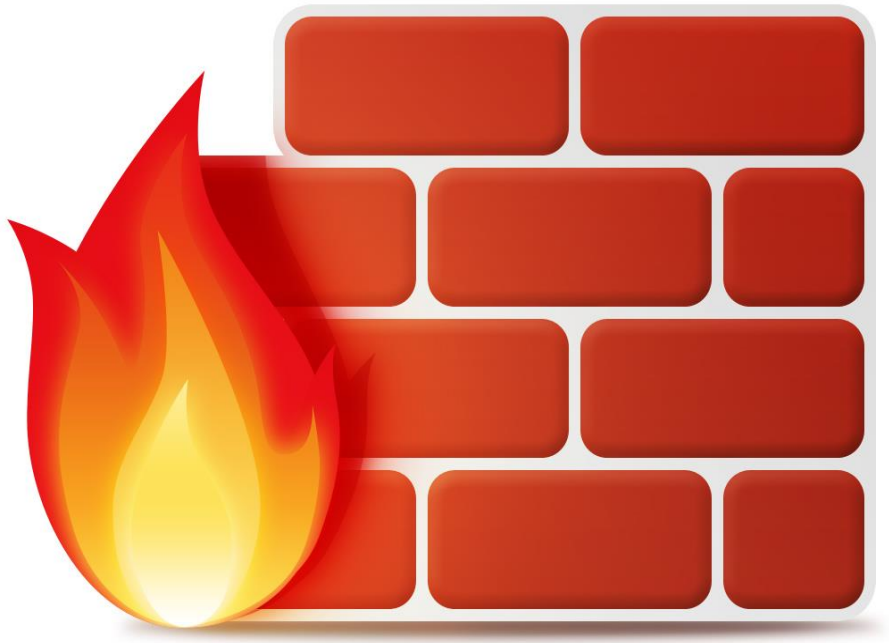
Ограничение доступа обучающихся к «нежелательной*» информации

- Крайне сложно выполнимо технически.
- Требует дополнительных административно организационных мер.
- Технические решения с актуальными списками доступа – все платные

*** видам информации, распространяемой посредством сети "Интернет", причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования**

Решение - NGFW

Брандмауэр «следующего» поколения (NGFW) является реализацией технологии межсетевого экранирования третьего поколения, сочетающей традиционный брандмауэр с другими функциями фильтрации сетевых устройств, такими как брандмауэр приложений, использующий встроенную глубокую проверку пакетов (DPI), систему предотвращения вторжений (IPS) и т.д.



Нормативные документы*

- Приказ об обеспечении ИБ в учреждении
- Пакет документов об ограничении доступа обучающихся к «нежелательной**» информации
- Пакет документов по работе с ПД
- Правила использования сети Интернет в образовательной организации (для сотрудников и для обучающихся)
- Сертификаты соответствия на имеющееся оборудование и ПО для ИБ
- И т.д.....

*** Список не является исчерпывающим и зависит от типа учреждения, региональной нормативной документации и множества других факторов**

**** видам информации, распространяемой посредством сети "Интернет", причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования**