группа компаний «Стинс Коман»

Академия Информационных Систем

Электронная почта – схемы надежной защиты сервера и трафика

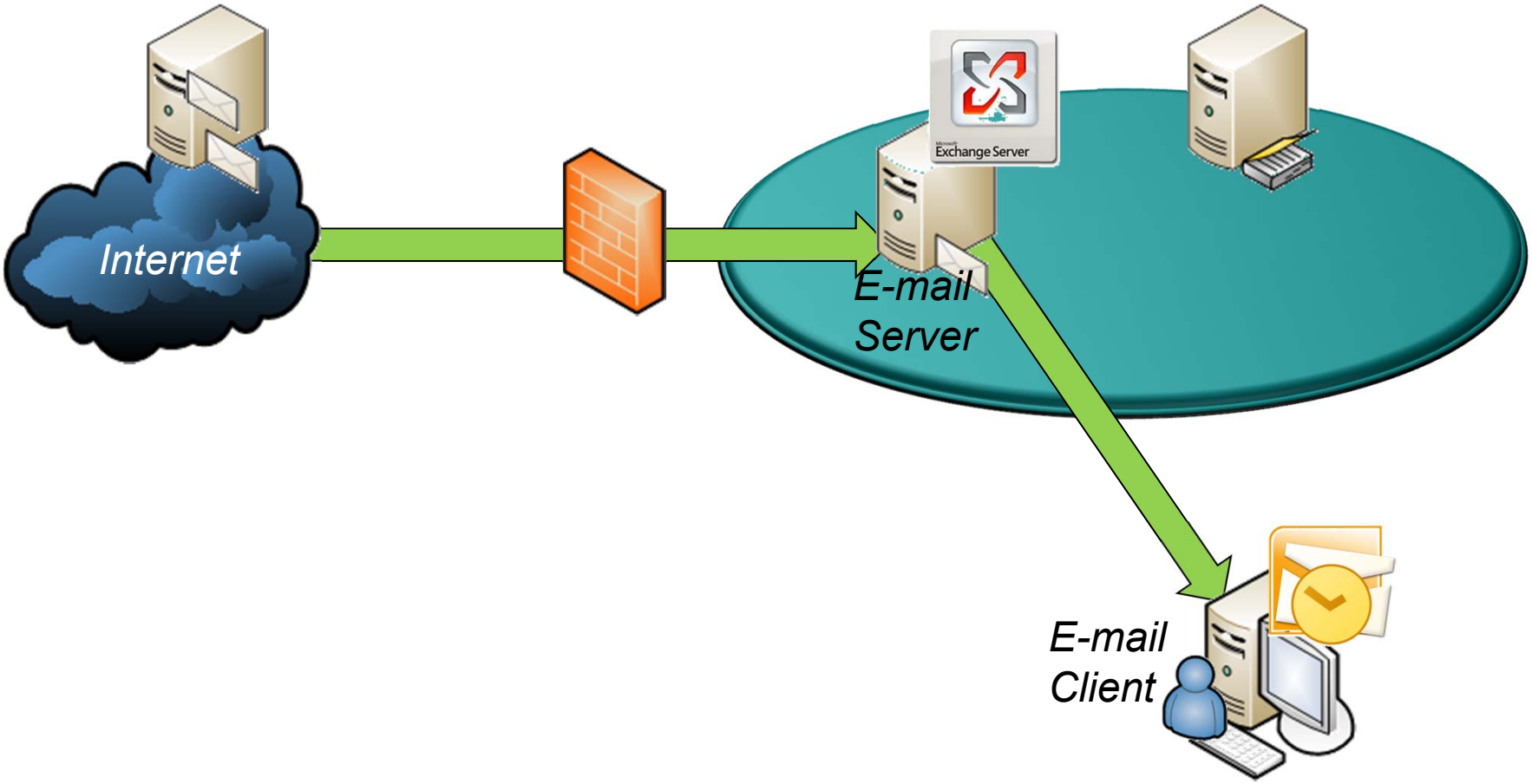
Абрамянц Карен Олегович

Преподаватель в области ИБ, MCNPS, MCSA
НОУ «Академия Информационных Систем»

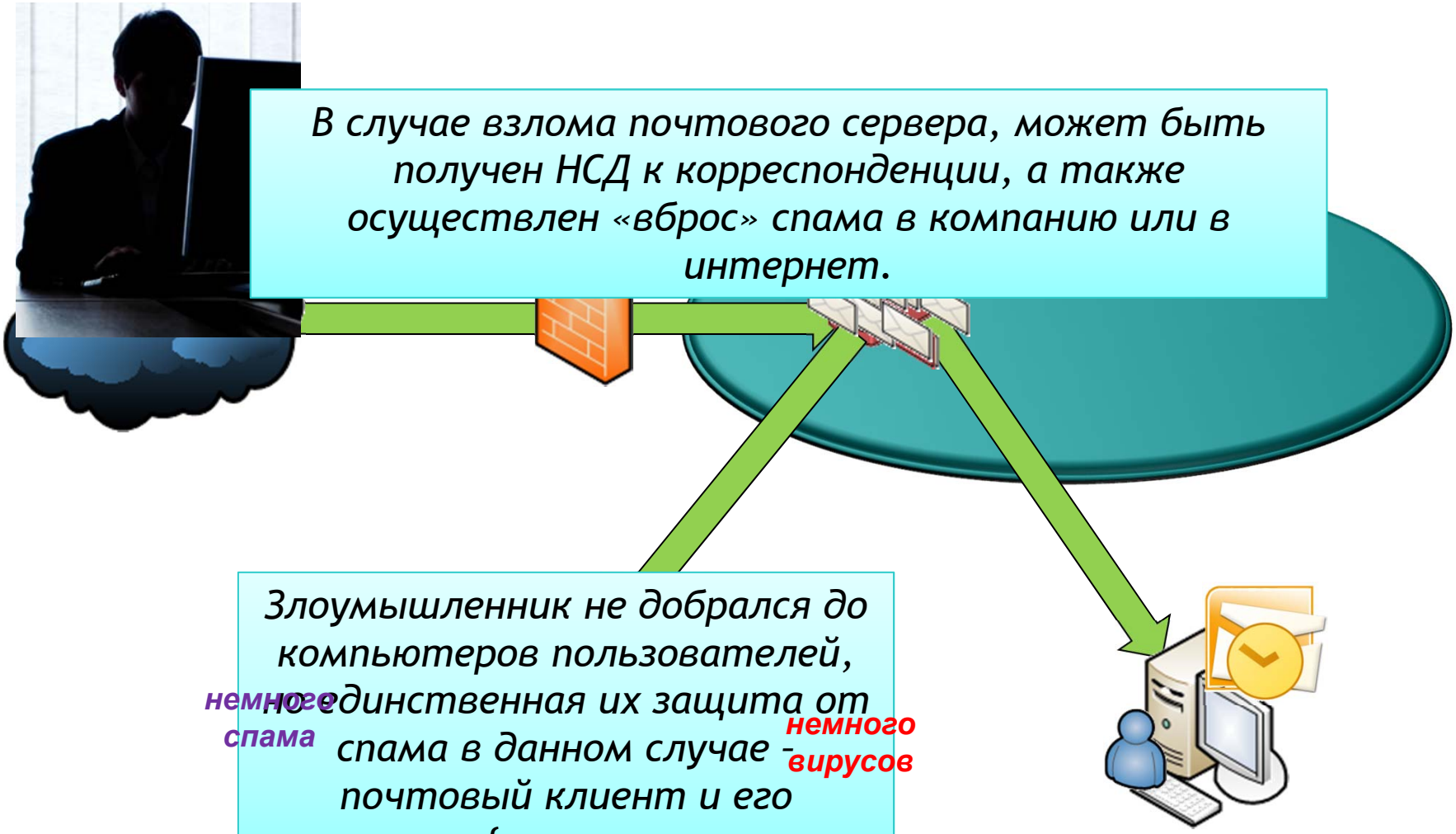
Основные вопросы по защите электронной почты

1. В чем опасность?
2. Как обеспечить защиту почтового сервера?
3. Как обеспечить защиту корреспонденции?
4. Пользовательский, серверный и более высокий уровень
5. Выделенный сервис – преимущества и недостатки
6. Выбор оптимальной схемы защиты
7. Спектр существующих решений на рынке

Стандартная схема размещения почтового сервера



В чем опасность?



Типовое решение – Edge или Relay

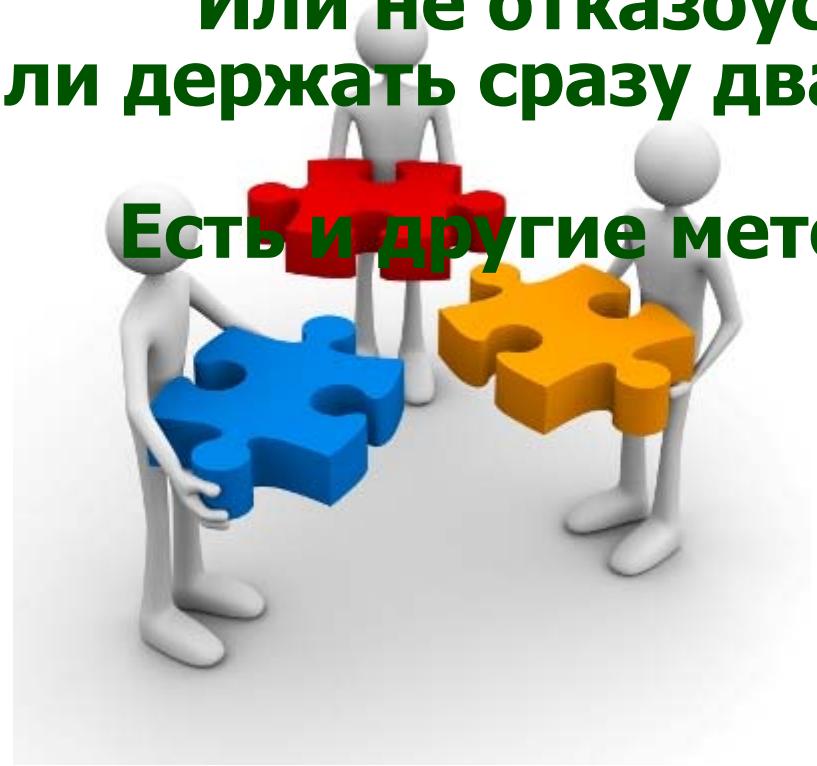
В схеме Edge предусмотрен
ступенчатый отсев данных.
схема не отказоустойчива.

Ваш администратор не имеет прямого доступа к Front-End серверу и не может его обслуживать в полную силу.

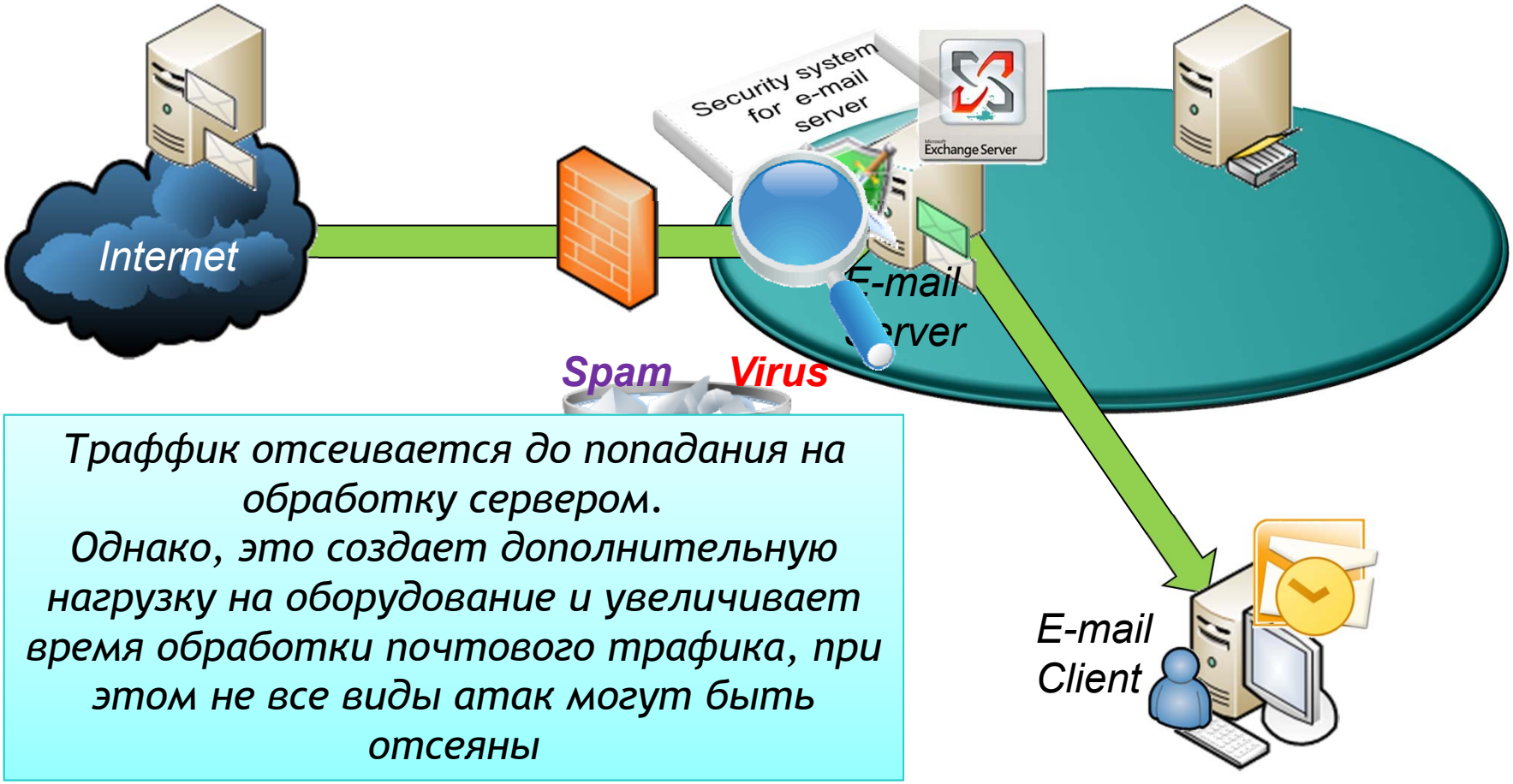
Что делать?

Оставлять систему незащищенной?
Или не отказоустойчивой?
Или держать сразу два E-mail сервера?

Есть и другие методы защиты!

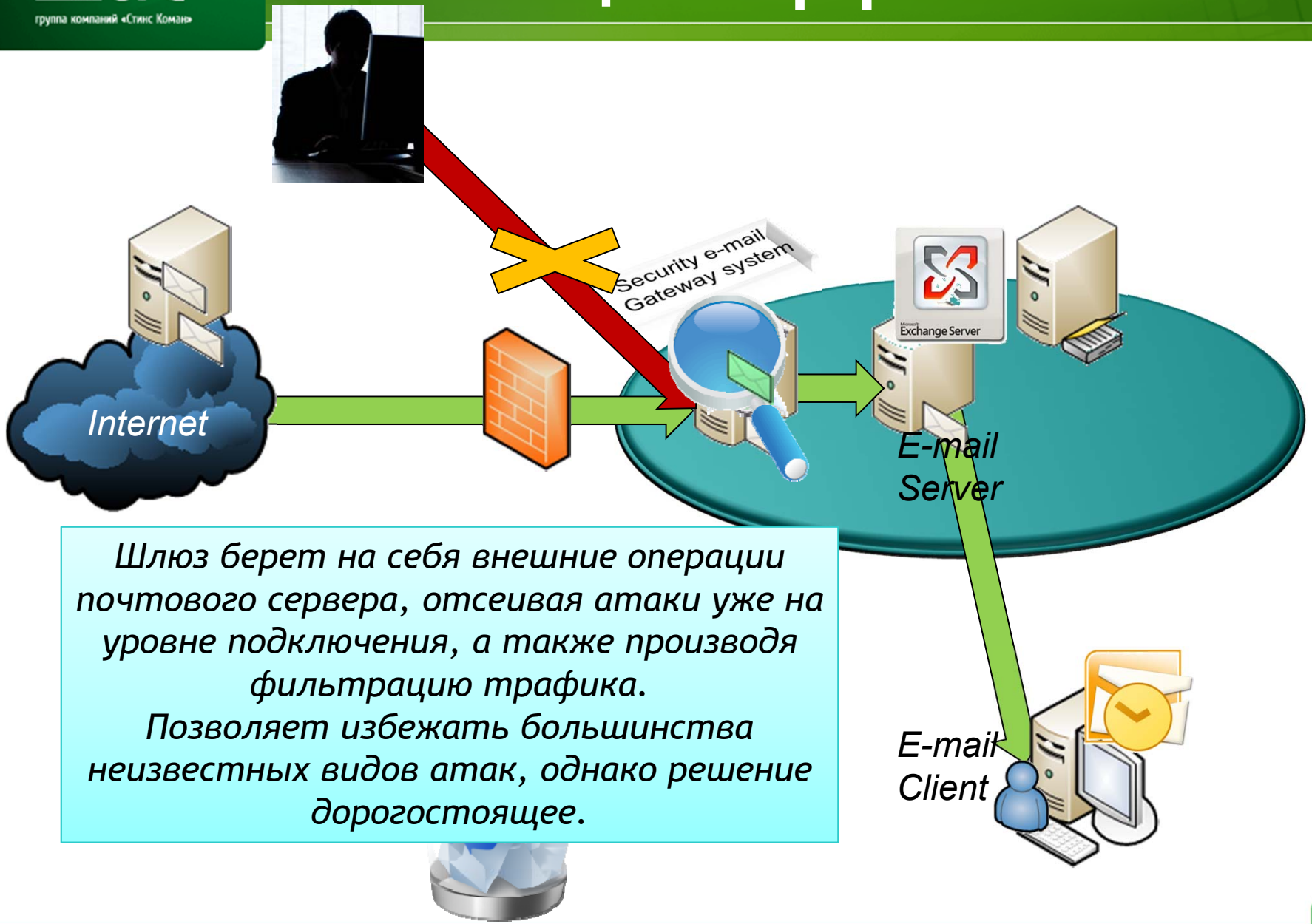


Добавка или дополнительный щит



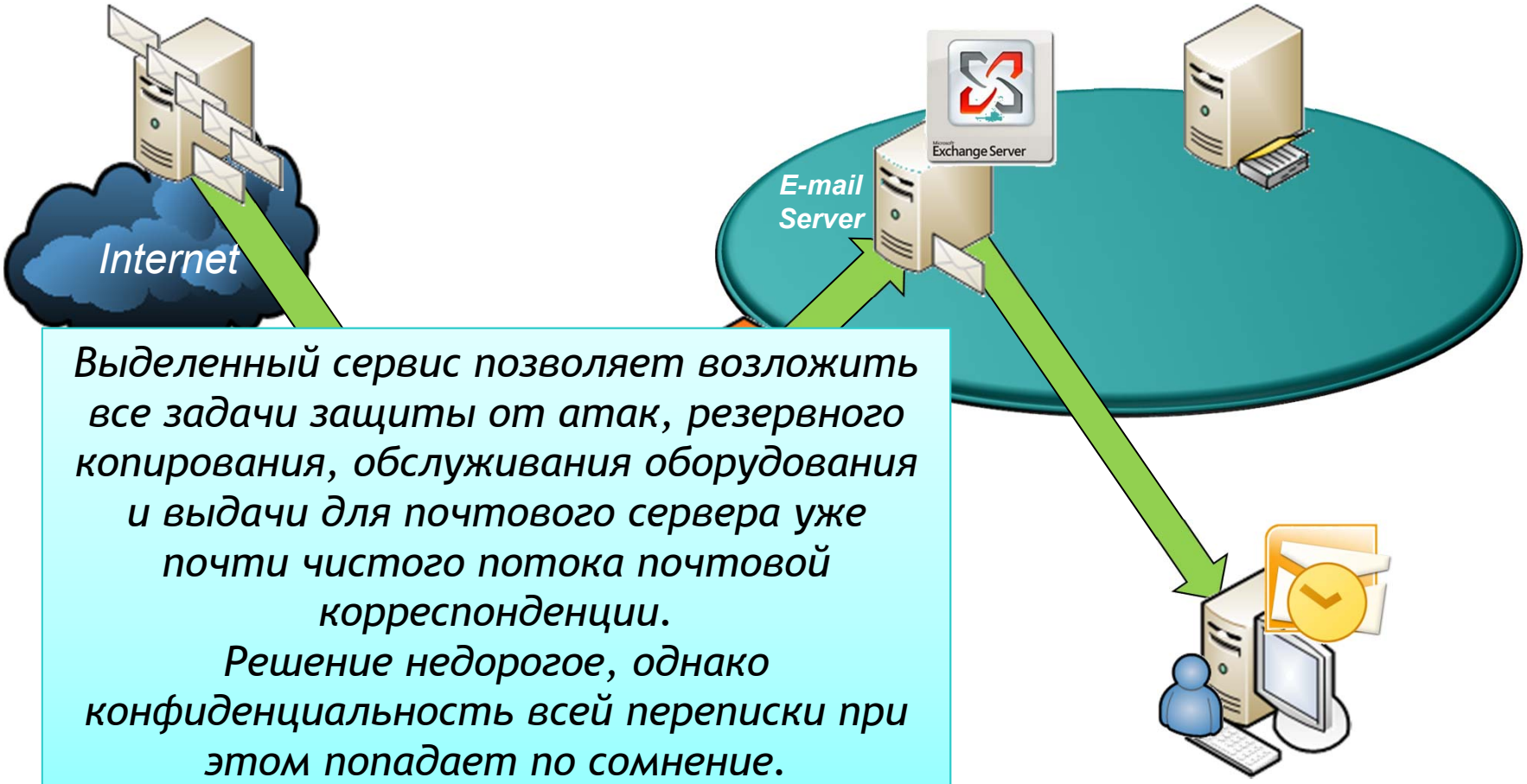
Траффик отсеивается до попадания на обработку сервером.
Однако, это создает дополнительную нагрузку на оборудование и увеличивает время обработки почтового трафика, при этом не все виды атак могут быть отсеяны

Защита в форме шлюза



Шлюз берет на себя внешние операции почтового сервера, отсеивая атаки уже на уровне подключения, а также производя фильтрацию трафика.
Позволяет избежать большинства неизвестных видов атак, однако решение дорогостоящее.

Выделенный сервис



Выделенный сервис позволяет возложить все задачи защиты от атак, резервного копирования, обслуживания оборудования и выдачи для почтового сервера уже почти чистого потока почтовой корреспонденции.
Решение недорогое, однако конфиденциальность всей переписки при этом попадает по сомнение.

Фазы работы защитника почты

Белый и черный список

Проверка параметров соединения

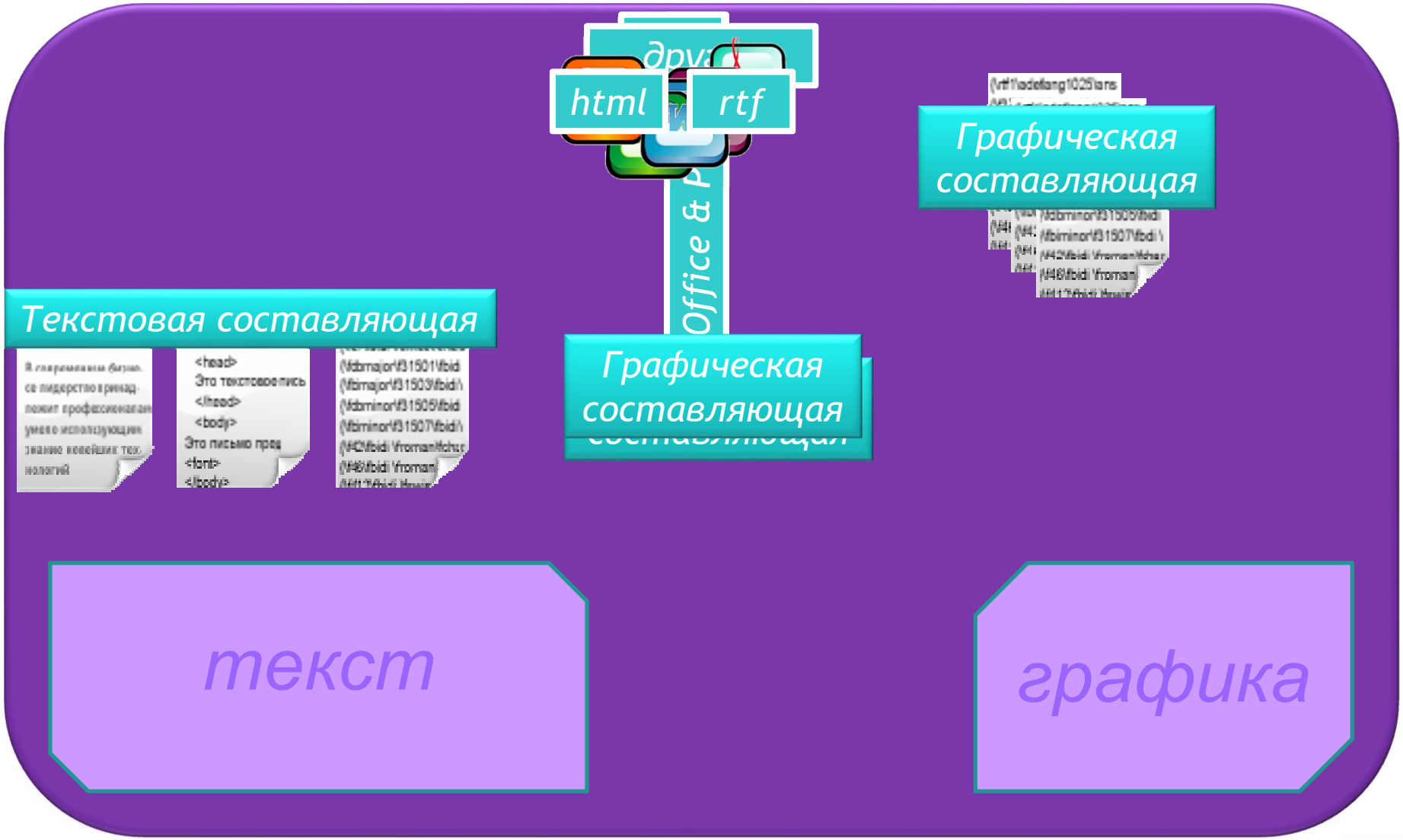
Антиспам проверка

Антивирусная проверка

Передача на маршрутизацию

После всех проверок, если сообщение не было окончательно передано в антивирус- или антиспам-карантин, в его конец добавляются соответствующие служебные заголовки и оно передается на маршрутизацию для пользователей

Разделение корреспонденции на составляющие



Разделение корреспонденции на составляющие

html

rtf

Исполняемые

Скрипты

Макро

Макро

скрипты

исполняемые

Использование нескольких движков

McAfee | Kaspersky

Microsoft AV | Kaspersky

AVG | BitDefender | Norman

Norman | VirusBuster | Authentium

Примеры предлагаемых решений

Производитель	Добавка к почтовому серверу	Шлюзовое Решение	Выделенный сервис
Microsoft	Microsoft Forefront Protection 2010 for Exchange Server	Microsoft Forefront Threat Management Gateway 2010	Microsoft Forefront Online Protection for Exchange
symantec.	Symantec Mail Security for Microsoft® Exchange	Symantec Brightmail™ Gateway	SYMANTEC HOSTED SERVICES MessageLabs Hosted Email Security
лаборатория Касперского	Kaspersky Security для почтовых серверов	Mail gateway v5.6	Касперского Kaspersky® Hosted Email Security
TREND MICRO	TREND MICRO ScanMail™ Suite for Microsoft® Exchange	TREND MICRO InterScan™ Messaging Security Suite	Trend Micro™ Hosted Email Security
McAfee	McAfee GroupShield for Microsoft Exchange	McAfee Email Gateway	McAfee SaaS Email Protection
Dr.WEB® Антивирус	Dr.WEB® for Microsoft Exchange Server	Dr.WEB® Mail Gateway	Dr.Web Avdesk
GFI	GFi MailSecurity for Exchange/SMTP/Lotus	GFi MailEssentials for Exchange/SMTP/Lotus	

http://www.infosystems.ru

Вопросы?

Абрамянц Карен Олегович

MCNPS, MCSA, Eset TSE, IBM Tivoli SM TP, Kaspersky DST, TrendMicro TSMP, CryptoPro Trainer, ViPNet Admin & Trainer

Преподаватель в области ИБ,
НОУ «Академия Информационных Систем»

http://kunzite.ru

kun@li.ru