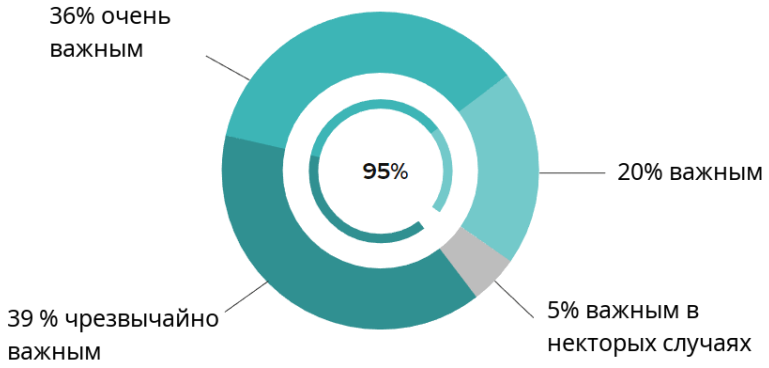
Примеры использования OpenSource-решений для создания безопасной инфраструктуры

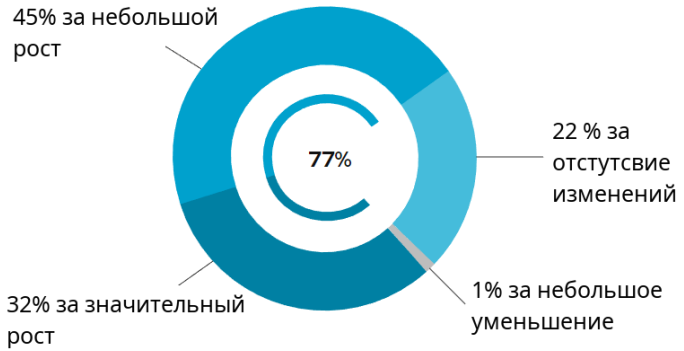
Технический специалист по информационной безопасности
Семенычев А.М.

Open Source. Немного статистики

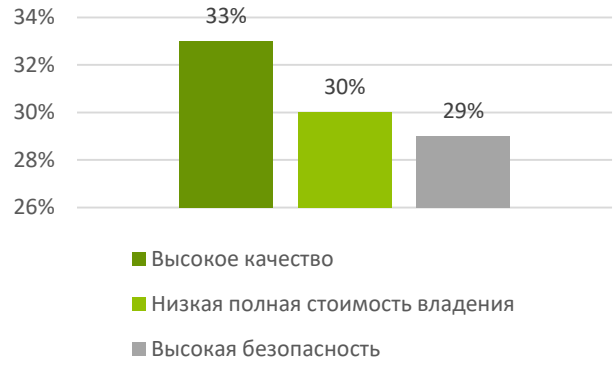
95% респондентов считают open source стратегически важным



77% респондентов считают, что доля open source на рынке будет расти

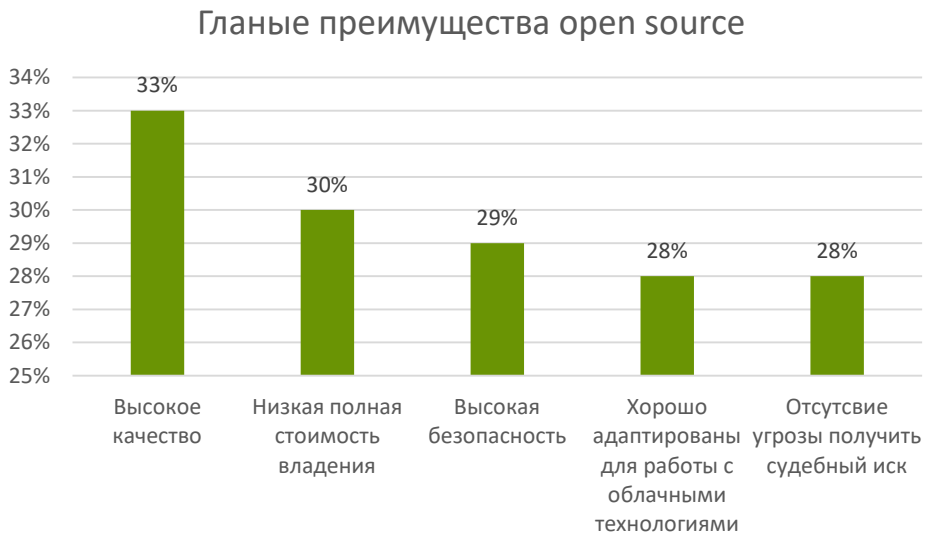


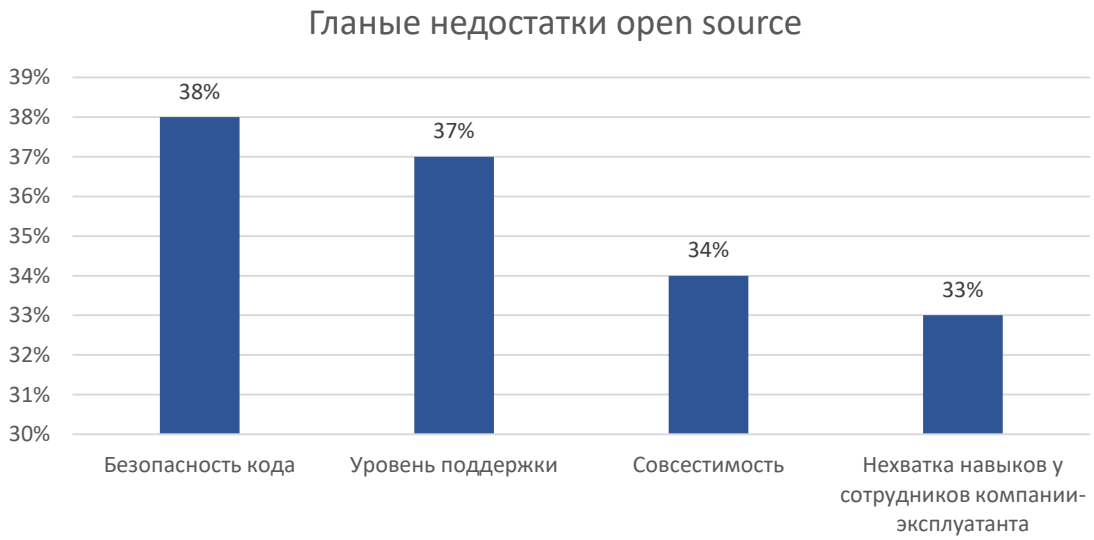
Снижение доли проприетарного ПО в корпоративном сегменте



Состояние Enterprise Open Source, согласно опросу RedHat 2020 года.

Open Source. Немного статистики





Состояние Enterprise Open Source, согласно опросу RedHat 2020 года.

Примеры использования Open Source. Удаленный доступ для контрагента.

Задача:
Как обеспечить удаленный доступ сотрудника контрагента к инфраструктуре субъекта КИИ?

Пункт 31 Приказа ФСТЭК № 239 от 25 декабря 2017 г. содержит:

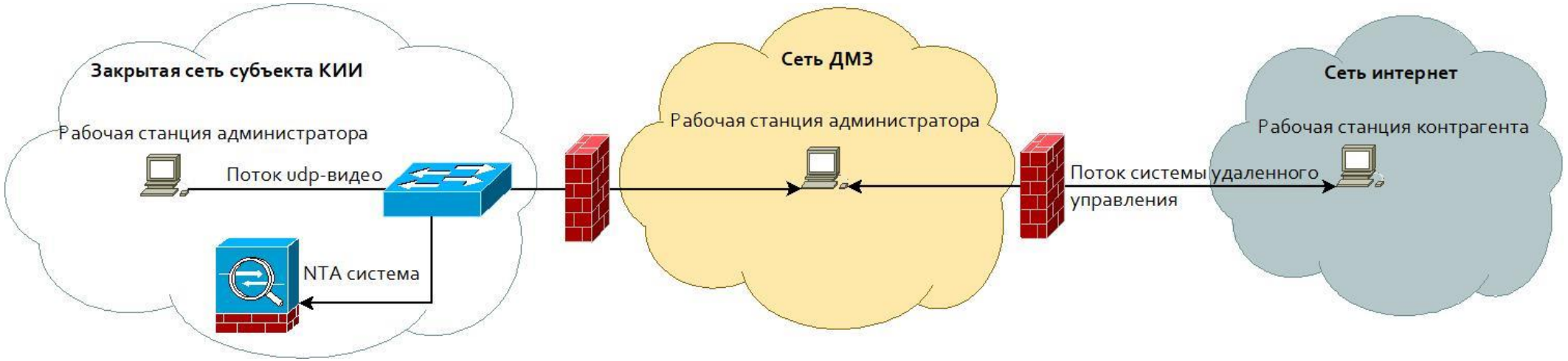
«*В значимом объекте не допускаются:*
наличие удаленного доступа к программным и программно-аппаратным средствам, в том числе средствам защиты информации, для обновления или управления со стороны лиц, не являющихся работниками субъекта критической информационной инфраструктуры, а также работниками его дочерних и зависимых обществ;»

Примеры использования Open Source. Удаленный доступ для контрагента.

Что требуется:		
Коммерческое решение		Open Source решение
• Закупка системы удаленного доступа • Ежегодная закупка для продления доступа		Приложение для трансляции видеопотока по протоколу udp • ffmpeg (https://ffmpeg.org/) • OBS Studio (https://obsproject.com/) Приложение для отображения полученного видеопотока • VLC media player (https://www.videolan.org/vlc/) Две рабочие станции.

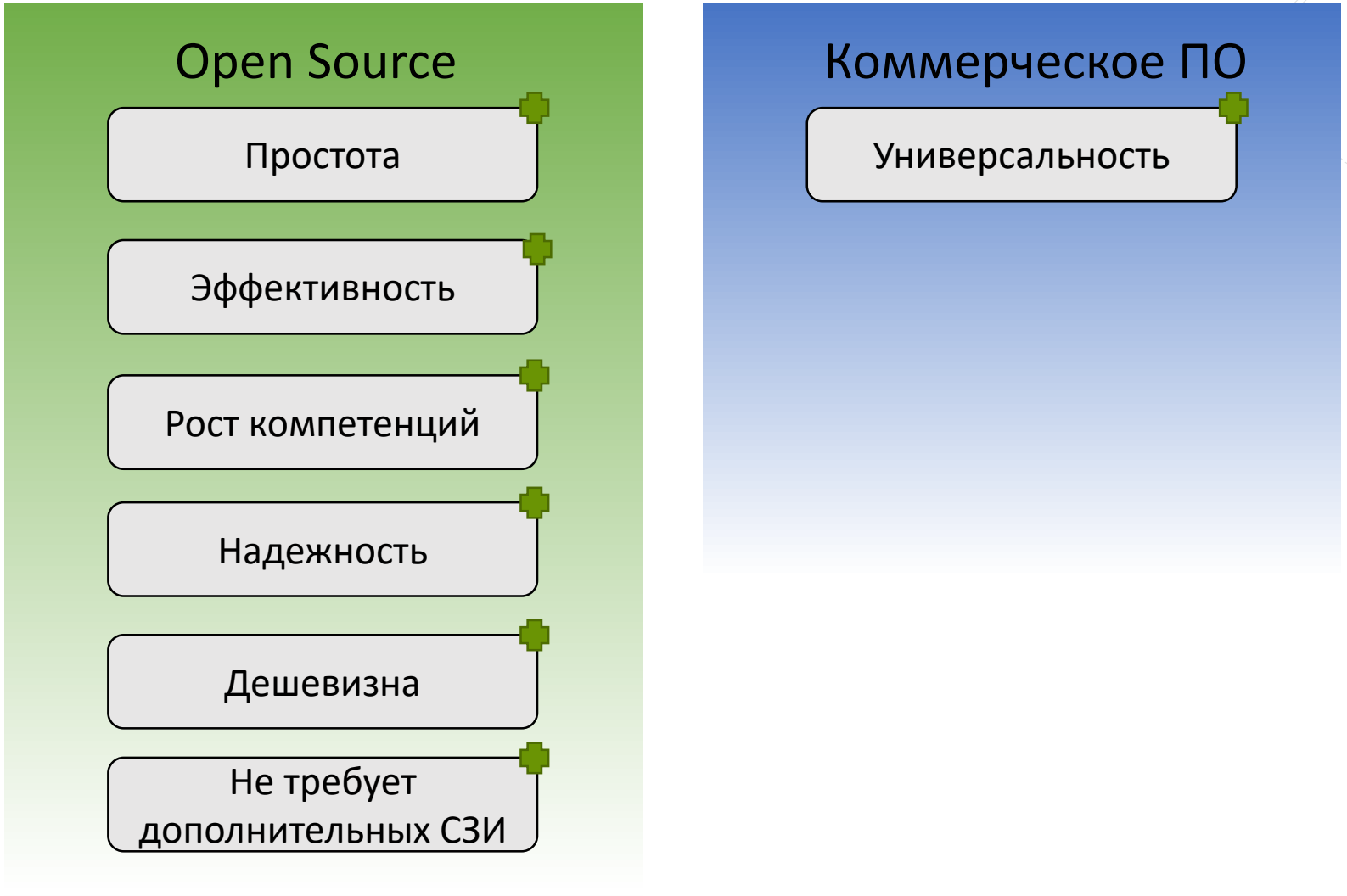
Примеры использования Open Source. Удаленный доступ для контрагента.

Примеры использования Open Source. Удаленный доступ для контрагента.



Примеры использования Open Source. Удаленный доступ для контрагента.

Преимущества



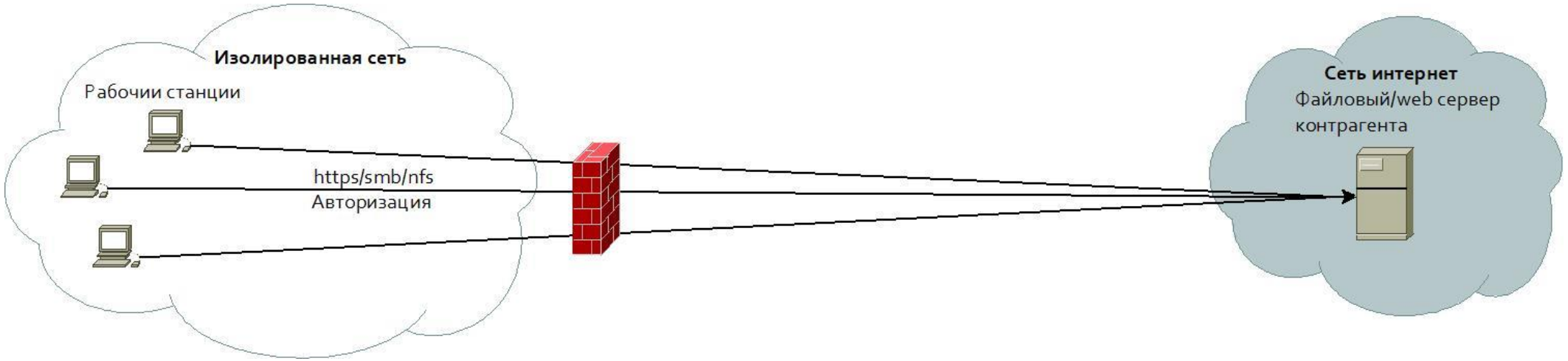
Примеры использования Open Source. Обмен информацией с контрагентом.

Задача:
Как обеспечить обмен открытой информацией между изолированным сегментом сети и контрагентом, через сеть интернет?

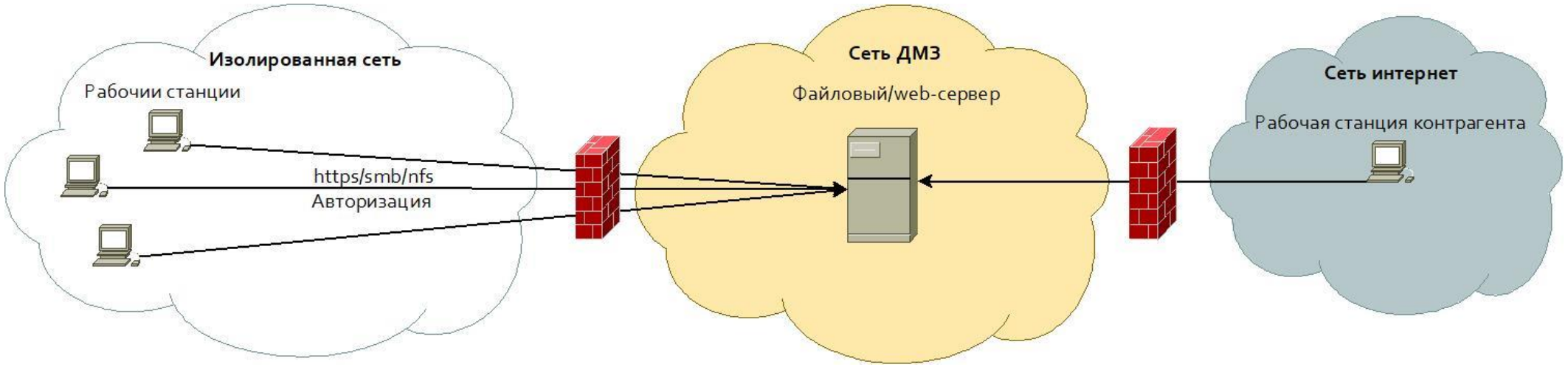
Примеры использования Open Source. Обмен информацией с контрагентом.

Что требуется:		
Open Source решение		Коммерческое решение
Два Linux сервера в различных сегментах сети.		Закупка и ежегодные траты на тех.поддержку.

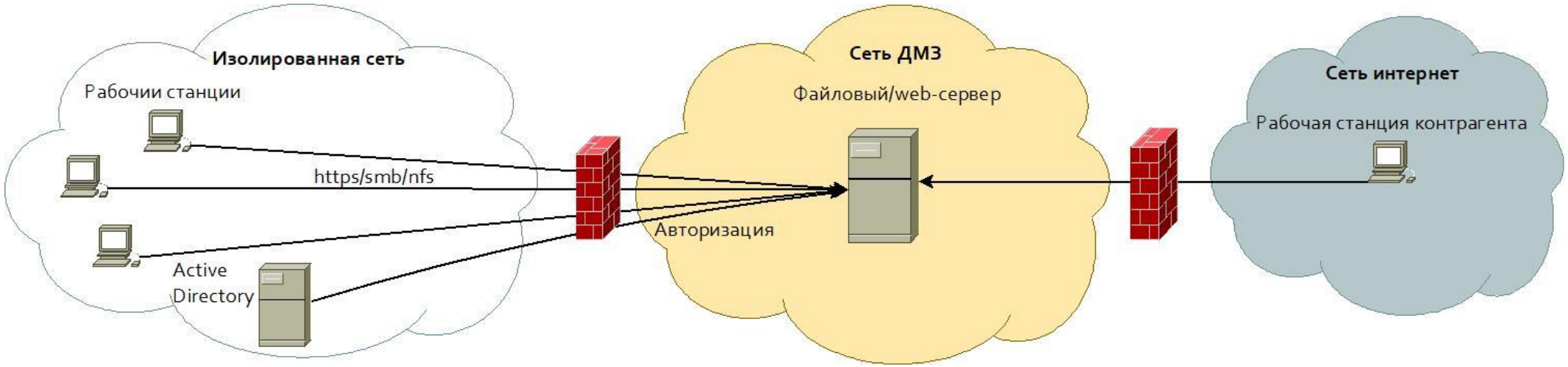
Примеры использования Open Source. Обмен информацией с контрагентом.



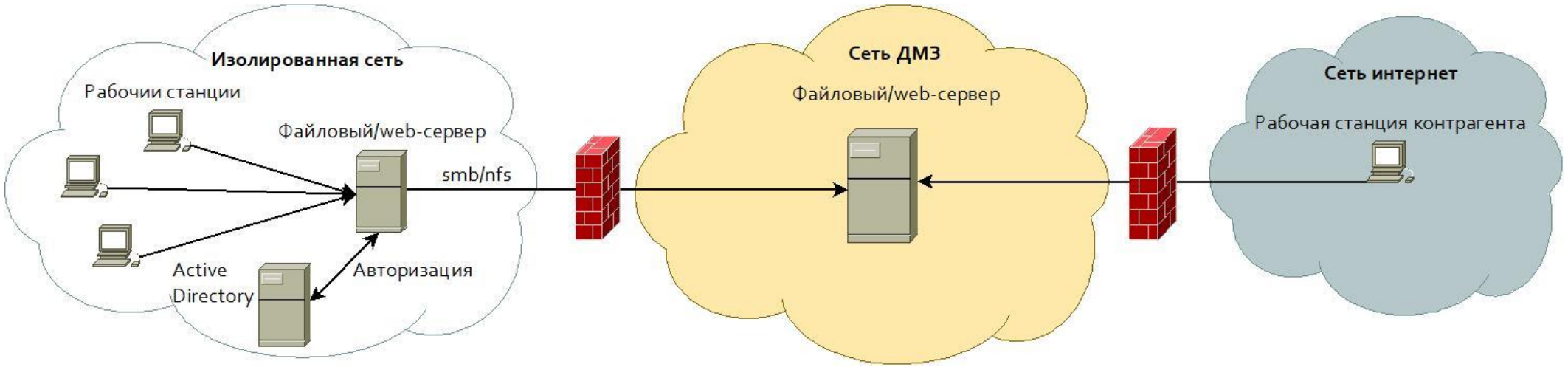
Примеры использования Open Source. Обмен информацией с контрагентом.



Примеры использования Open Source. Обмен информацией с контрагентом.

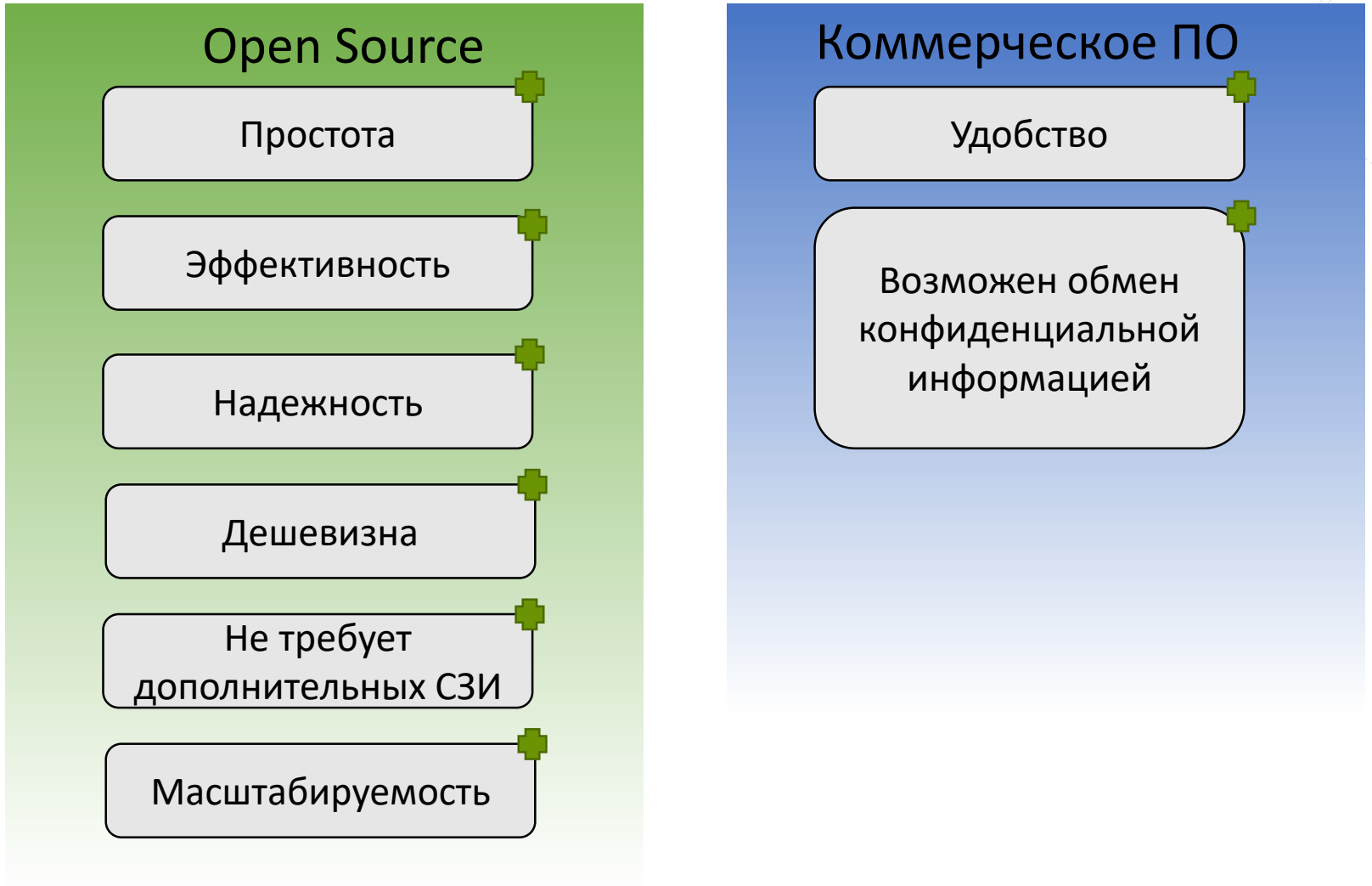


Примеры использования Open Source. Обмен информацией с контрагентом.



Примеры использования Open Source. Обмен информацией с контрагентом.

Преимущества



Средства защиты информации Open Source

СЗИ	Open Source	СЗИ	Open Source	СЗИ	Open Source
Межсетевой экран	pfSence IPFare OPNsense Endian Firewall Community	Encryption At Rest	VeraCrypt	Container Security	Clair Anchore Dagda
IPS/IDS	Snort Suricata	Host IDS	OSSEC Wazuh	Network Monitoring	Nagios Core Zabbix Incinga 2
Web Application Firewall	ModSecurity IronBee WebKnight	Identity and Access Management	Kaycloak OpenIAM	Backup and Recovery	Amanda UrBackup Bacula
SIEM Log Analytics	SIEMonster Elastic Stack OSSIM	Multi-Factor Authentification	LinOTP	Email Antivirus Gateway	MailScanner OrangeAssassin MailCleaner
Log Management	Elastic Stack fluentd	Privileged Access Management (PAM)	N/A	File Integrity Monitoring	OSSEC Tripwire
Threat Intelligence Platform/Feeeds	MIPS YETI	Email Antivirus	ClamAV Armadito	NetFlow	ntop
Data Loss Prevention (DLP)	N/A	Endpoint Protection	ClamAV Armadito	Wireless IDS/IPS	Vistumber Kismet

Средства защиты информации Open Source

СЗИ	Open Source	СЗИ	Open Source	СЗИ	Open Source
Web Filtering	E2guardian ClearOS	PKI	EJBCA OpenXPKI	Network Security Monitor (NSM)	Zeek
Reverse Proxy Load Balancer	Nginx	SSL Decryption	Mitre ChopShop ModSecurity	Deception Honeypots	Tpot Modern Honey Nettwork
VPN	OPenVPN SoftEther Freelan	SSL Certiticates	Let's Encrypt	Patch Management	OPSI
Asset Management	Open-AudIT Snipe-IT Kuwaiba	Secure DNS (DNSSEC)	BIND PowerDNS	Penetration Testing	KaliLinux Commando VM
Key Management	Vault by HashiCorp StrongKey	Vulnerability Management	OpenVAS Nikto	Sandbox	Cuckoo Sandbox Drakvuf
Change Management	N/A	Coverage Risk and Complaince Monitoring	Eramba	Secutiry Orchestration	Patrowl TheHive
Network Access Control	PacketFence openNAC	Security Controls Bundles	Security Onion Prelude Caldera	Application Security Testing	LGTM.com Burp Suite OWASP ZAP

Спасибо за внимание!

Технический специалист по информационной безопасности
Семенычев А.М.
a.semenychev@gardatech.ru