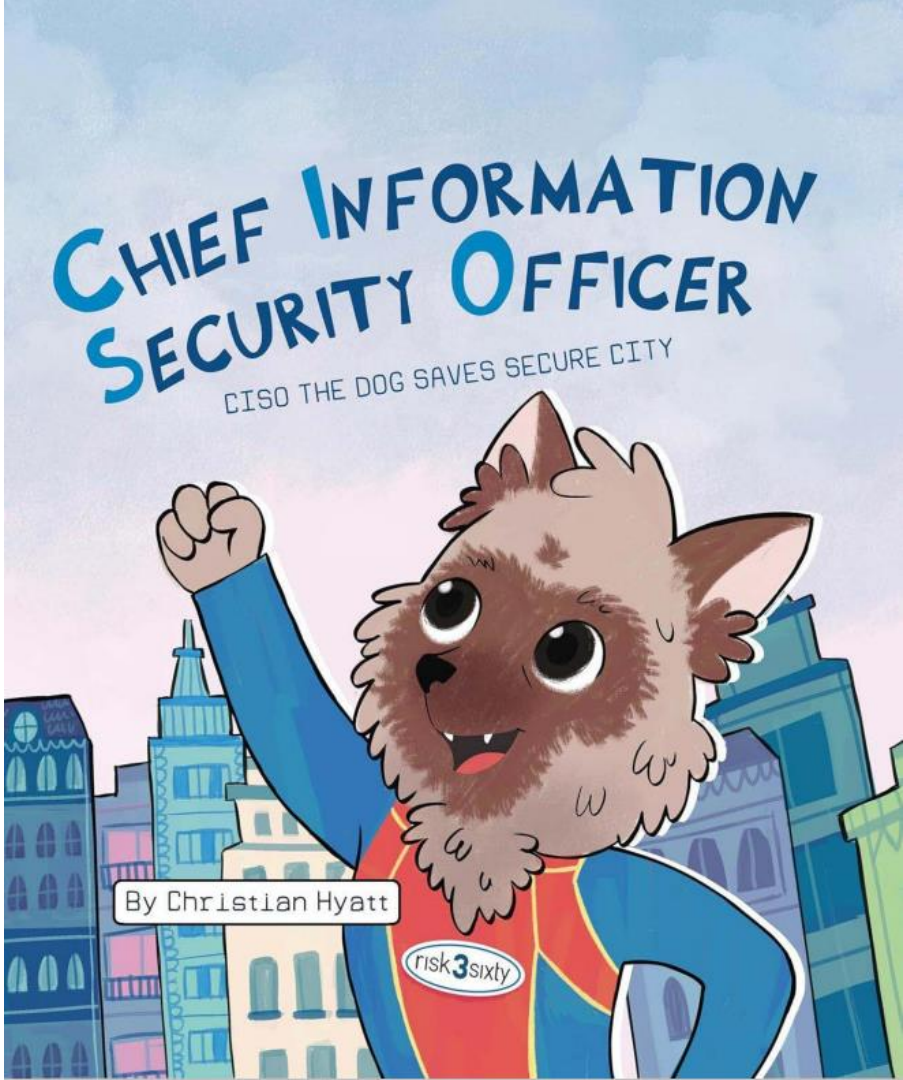
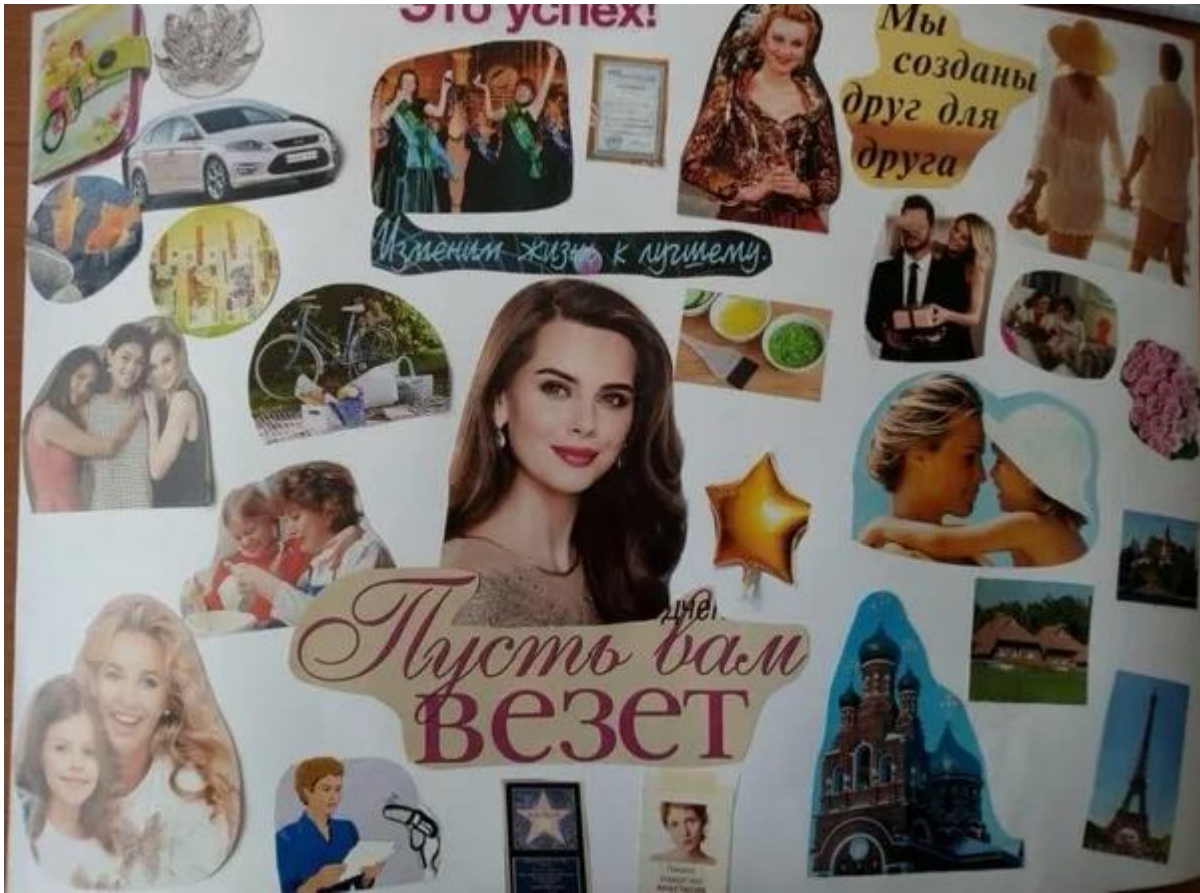
Первые шаги в ИБ



Куличкин Артём Александрович

CISO, CISM, CISA, CEH, CND.

Карьерная карта желаний



Введение

Связиста замечают только тогда, когда пропадает связь.

Топ 3 профессий в сфере И

- «Аналитик SOC, инженер информационной безопасности, пентестер».
- «Форензика, безопасность разработки, управление в области ИБ».
- «Кроме внедрения СЗИ, безопасной разработки и форензики стоит посмотреть в сторону безопасности ИИ».

«Администратор, аналитик, исследователь. В первом случае стоит учить администрирование — системное и сетевое».

Возможности

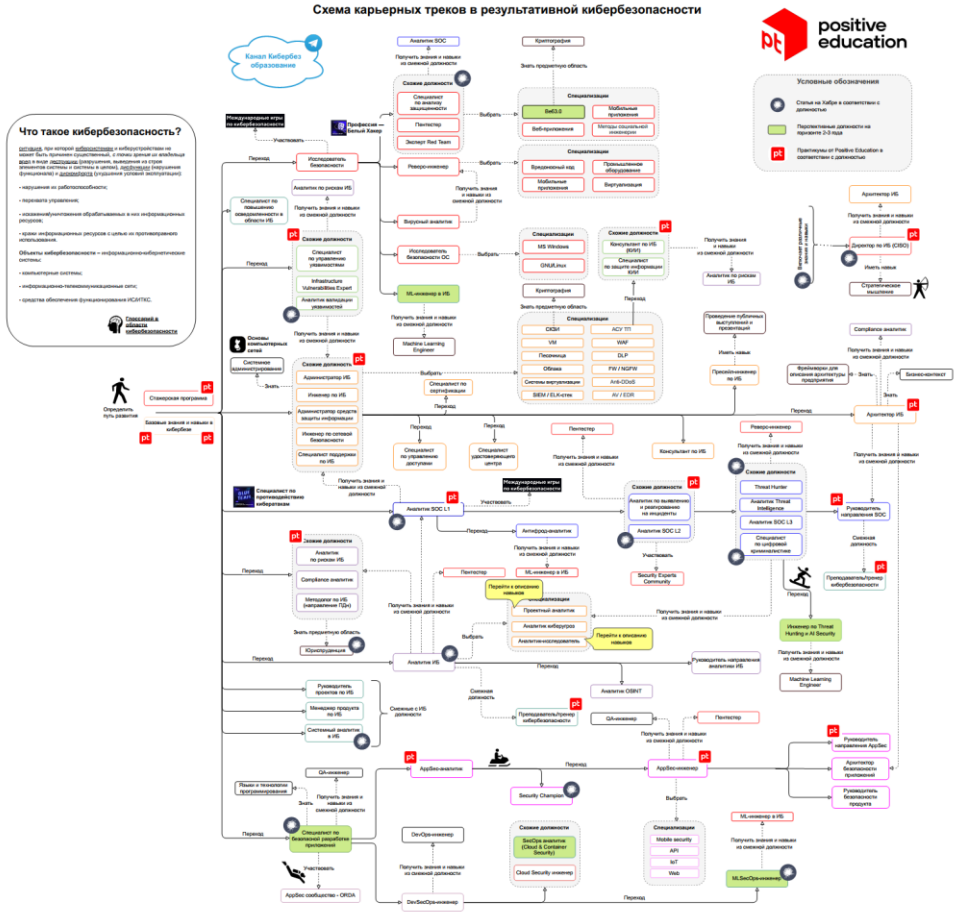
- Обнаружение угроз и активное реагирование — 30%.
- Расследование инцидентов — 17%.
- Безопасная разработка ПО — 16%.
- Наступательная безопасность (Offensive Security) — 14%.
- Управление рисками и соответствие требованиям регуляторов — 13%.
- Защита данных и криптография — 10%.

Рисунок 2. В какой области ИБ вам хотелось бы получить дополнительные знания?

Вуз не может подготовить узкого специалиста под отдельно взятую компанию

Это база

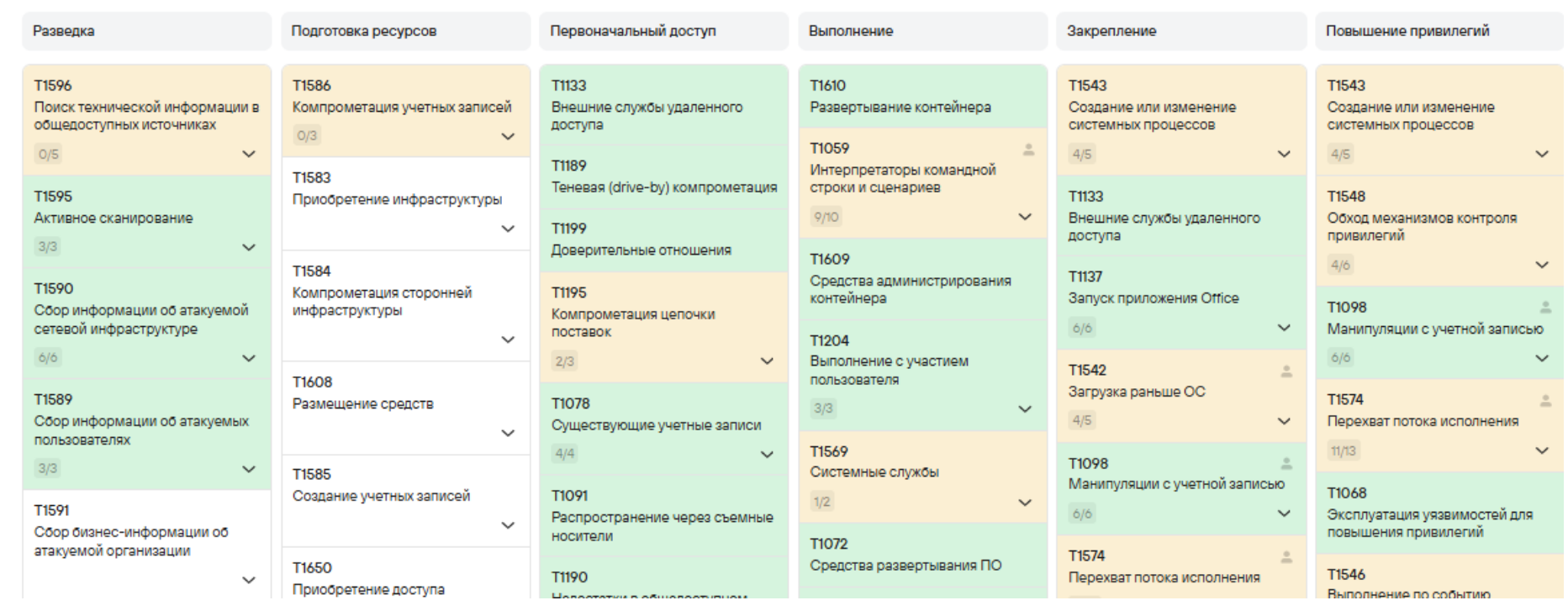
[Схема карьерных треков в кибербезопасности 2025 версия 2]



Вуз не может подготовить узкого специалиста под отдельно взятую компанию

Это база

[Матрица MITRE ATT&CK]



Материалы

База по информационной безопасности

Материалы этого раздела лучше изучать последовательно — так картина будет складываться более полно.

Выпуски об информационной безопасности на канале «Люди PRO». Канал ведет бывший киберпреступник Сергей Павлович. Рекомендуем следить за обновлениями и посмотреть все выпуски с Сергеем Никитиным — «главным борцом с хакерами», как его называют в интернете. Также подпишитесь на канал Сергея Никитина о цифровой гигиене и кибербезопасности.

Статья Cisco. В обзорной статье рассказывают, что такое кибербезопасность, какие типы киберугроз существуют. Советуем изучить материалы по ссылкам в конце страницы, особенно статьи о безопасности конечных точек, сетевой и облачной безопасности.

Статья «Что такое кибербезопасность» на сайте Positive Technologies. Рассказывает, где применяются практики кибербезопасности, какие типы киберугроз и средства защиты информации существуют.

Сайт Cybersecurity Knowledge Hub. Ресурс, на котором можно найти словарь базовых терминов информационной безопасности.

Сайт Cybersecurity Learning Hub. В разделе Some Common Roles in Cybersecurity дано описание общих ролей специалистов по кибербезопасности.

Издание Anti-Malware. На этом ресурсе есть обзоры на популярные категории средств защиты информации, аналитика рынка кибербезопасности, а также интервью с экспертами отрасли.

Матрица MITRE ATT&CK и статья о ней на русском языке. MITRE ATT&CK — база знаний о тактиках и техниках атак злоумышленников. Она актуализируется компанией MITRE, за ее обновлением следят все специалисты по кибербезопасности. Рекрутерам и сорсерам достаточно иметь представление об этой матрице.

Подкасты «Кверти». Специалист по кибербезопасности рассказывает, как не попасться на уловки мошенников и как им противостоять. Обязателен к прослушиванию выпуск о фишинге.

Выпуск подкаста Podlodka о продуктовой безопасности. Руководитель команды продуктовой безопасности в Acronis Сергей Белов рассказал, какие инструменты используют для анализа кода и поиска уязвимостей. Также Сергей объяснил, как распределять роли и выстроить процессы между разработчиками и инфобезами, чтобы работа была эффективной.

Материалы

Материалы по продуктам и сервисам в сфере кибербезопасности
Обзор технологий кибербезопасности
Вебинар «Обзор технологий кибербезопасности для защиты организации». Архитектор решений по информационной безопасности Positive Technologies Михаил Кадер рассказал об этапах защиты от кибератак и комбинациях технологических решений для противостояния злоумышленникам.

Threat Intelligence
Это сбор и анализ данных о киберугрозах. Обладание такой информацией дает возможность понять злоумышленников, просчитать их намерения и предотвратить угрозу до того, как она реализовалась.
Лекция об основах Threat Intelligence. Аналитик отдела исследования сложных киберугроз Никита Ростовцев рассказал, что такое Threat Intelligence и какие скиллы необходимы, чтобы быть сильным Threat Hunter.
Подкаст «Кверти» о том, как действуют кибернаемники. Руководитель группы исследования сложных угроз Анастасия Тихонова рассказала, что такое охота за угрозами и как обнаружить кибератаку.
Интервью о кибервразведке. Руководитель департамента кибервразведки Дмитрий Шестаков рассказал про способы исследования и атрибуции кибератак, выстраивание проактивной системы информационной безопасности. Также Дмитрий показал, как работает платформа Threat Intelligence.

Материалы

Сетевая защита и безопасность конечных точек

Для сетевой защиты и защиты безопасности конечных точек используют набор методов и инструментов. Вот главное о них, что желательно изучить рекрутеру.

Интервью о XDR. XDR (Extended Detection and Response) — это программные решения, которые помогают обнаруживать и реагировать на сложные угрозы и целевые атаки. В интервью ведущий пресейл-менеджер Павел Остриков делится, для каких задач подходят XDR-решения, как происходит их внедрение и работа.

Статья про SandBox. SandBox — это «песочница», изолированная среда, через которую проходит трафик. Ее необходимо использовать для проверки файлов и ссылок на угрозы. В статье рассказано о принципах работы и моделях поставки песочниц.

Подкаст «Кверти» о SIEM-системах. SIEM-системы — это системы, которые анализируют информацию, реагируют на события и отображают состояние информационной безопасности на текущий момент. В подкасте совладелец компании RuSIEM Максим Степченко рассуждает о пользе этой технологии и о состоянии рынка SIEM-систем в России.

Статья о технологиях XDR, EDR, SIEM и SOAR. В материале сравнивают эти концепции и поясняют их преимущества.

Материалы

Антифрод-системы

Это системы мониторинга и предотвращения мошеннических операций, обычно с помощью анализа транзакций.

Статья про антифрод-системы. Раскрывает принципы работы и сферу применения антифрод-систем.

Видео о противодействии финансовому фроду. Руководитель международного департамента компетенций и сопровождения проектов по противодействию мошенничеству Зафар Астанов рассказывает о способах выявления финансового мошенничества и противодействия ему.

Подкаст Podlodka про антифрод. Алексей Тощаков из команды антифрода в Яндексе объясняет, как работают такие системы.

Статья об умном антифроде: как Big Data и Machine Learning защищают ваши деньги. Материал объясняет, где используется антифрод, как устроена система Fraud Detection и при чем здесь машинное обучение. Чтобы открыть страницу со статьей, нужно использовать VPN.

Материалы

Security Operation Center

Это структурное подразделение, которое проводит мониторинг работы систем защиты информации и реагирует на инциденты.

Статья о SOC. В материале описано, с какими задачами справляется SOC, как подключать и использовать услуги SOC-центра, а также какие роли специалистов бывают.

Первый сезон подкаста медиагруппы «Авангард» о SOC и Threat Intelligence. Послушать подкаст можно на Яндекс Музыке и в Apple Podcasts. Самые важные выпуски:

о начале пути специалиста по информационной безопасности;

о кибербдительности в России;

о Thread Intelligence.

Антивирусы

Подкаст Podlodka про антивирусы. Главный эксперт Лаборатории Касперского Александр Гостев помог разобраться в видах вредоносных программ: вирусах, червях, троянских программах. Также Александр рассказал о видах борьбы с ними.

Технический аудит

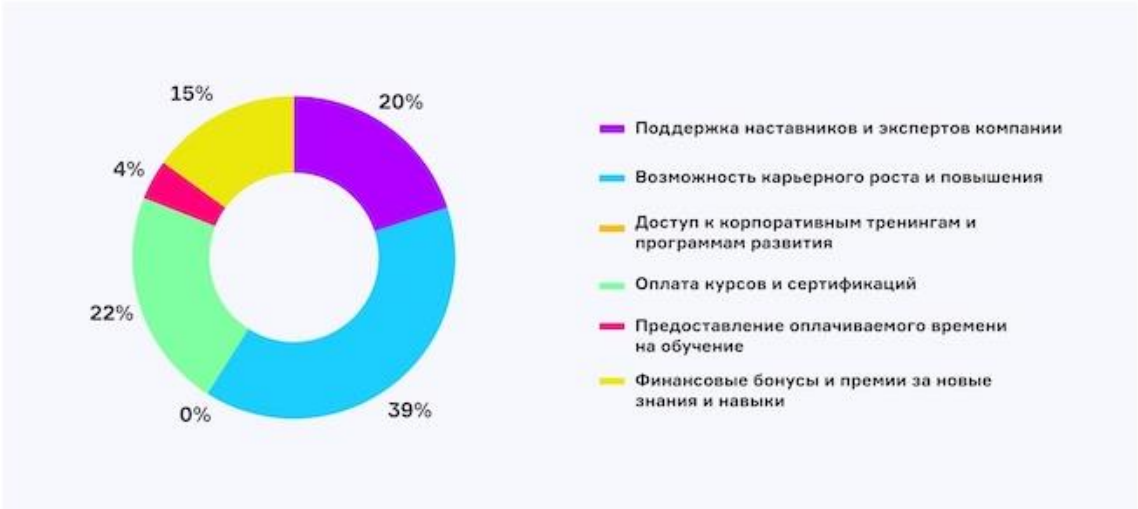
Это анализ защищенности приложений, тестирование на проникновение и Red Teaming — имитация атак для оценки кибербезопасности систем.

Статья об особенностях технического аудита. В статье освещены подходы к исследованию безопасности на уязвимости: пен-тест, аудит и анализ защищенности.

Мотивация

- Возможность карьерного роста и повышения — 39%.
- Оплата курсов и сертификаций — 22%.
- Поддержка наставников и экспертов компании — 20%.
- Финансовые бонусы и премии за новые знания и навыки — 15%.

Рисунок 4. Какие действия работодателя мотивируют вас на дополнительное обучение?



Куда дальше?

Компании

Финансовый сектор — банки, страховые компании и финтех-стартапы нуждаются в защите данных.
ИТ и телеком — интернет-провайдеры, облачные сервисы, дата-центры и разработчики ПО нуждаются в постоянной защите инфраструктуры и клиентов.
Промышленность — Газпром, Роснефть, РЖД внедряют системы защиты АСУ ТП.

Государственные учреждения

Защита критической информационной инфраструктуры — ФНС, Росреестр, министерства требуют специалистов для защиты государственных систем и объектов.
Обеспечение безопасности цифровых продуктов — например, портала государственных услуг, портала «Моя школа» Московской области.

Консалтинговые фирмы

Аутсорсинг задач — многие компании предпочитают аутсорсить часть задач: аудит, пентесты, настройку защиты. Это даёт возможность строить карьеру в консалтинговых компаниях или работать проектно.
Разработка документации — модели угроз, политики информзащиты — компании нанимают экспертов, которые занимаются этим.

Фриланс

Участие в программах Bug Bounty — специалисты по ИБ могут работать как независимые эксперты, искать уязвимости в информационных системах и получать вознаграждение от компаний.
Консультации для заказчиков — можно предлагать услуги по обеспечению безопасности, например, прописывать процедуры и бумаги для постановки системы безопасности.

AD

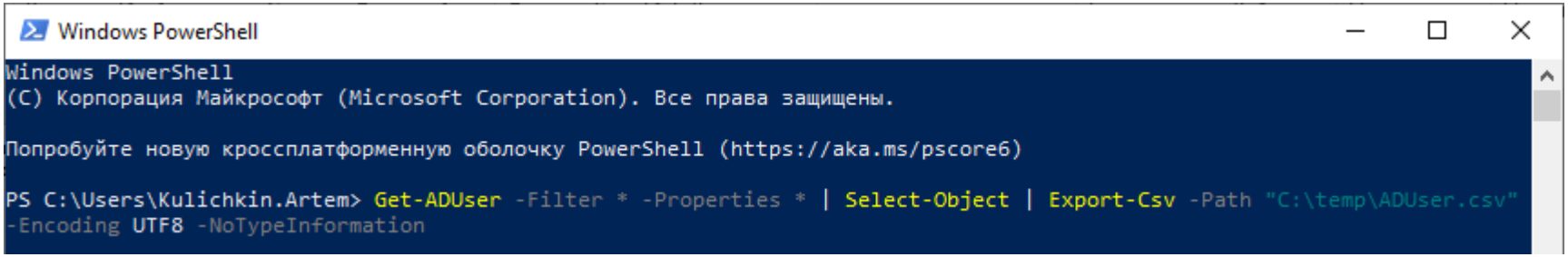
Аудит + доработка AD:

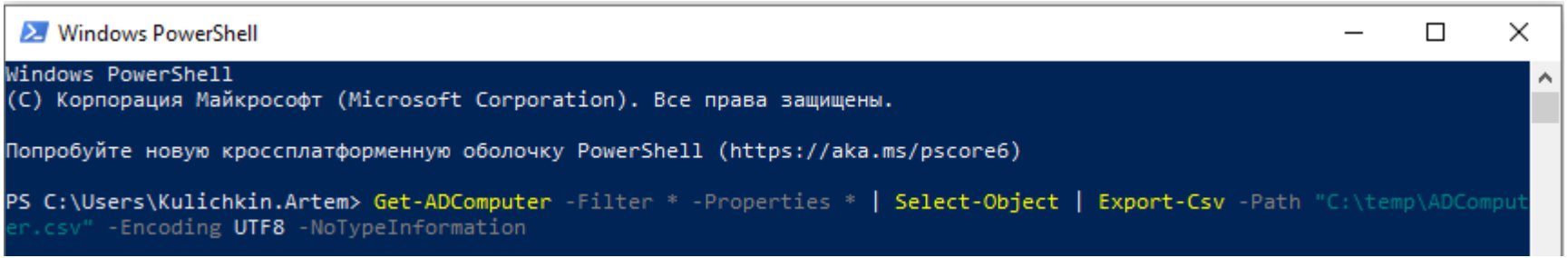
- Учётные записи
- Брут паролей
- Lithnet Password Protection
- Хосты
- Неправильное наследование
- Пилоты DCAP
- AD Audit Plus

AD

Аудит + доработка AD:

- **Учётные записи** (Password ,Password never expires, last logon)





[Аудит пользователей AD с помощью Powershell / Хабр]

AD

Admin Accounts With SPN

0.22%

3 Admin Accounts With SPN

Accounts That Do Not Require Kerberos Pre-Authentication

0.43%

6 Accounts That Do Not Require Kerberos Pre-Authentication

Accounts With Passwords That Never Expire

1,158

Users

84% Accounts With Passwords That Never Expire

Accounts With No Password Policy

91%

1,255 Accounts With No Password Policy

AD

Аудит + доработка AD:

- Учётные записи
- **Брут паролей**

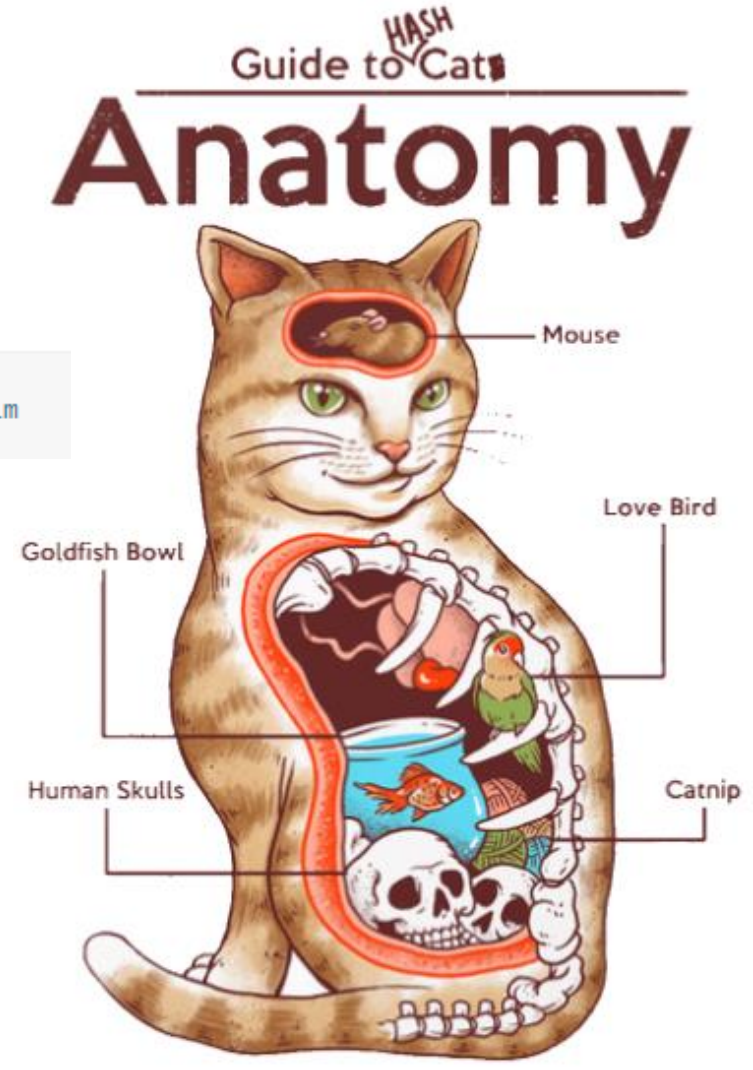
```
secretsdump.exe deiteriy.local/Administrator@192.168.88.32 -just-dc-ntlm
```

```
hashcat.exe -m 1000 E:\hashs.txt --show
```

```
E:\hashcat>hashcat.exe -m 1000 E:\hashs.txt --show
31d6cfe0d16ae931b73c59d7e0c089c0:
70b209a9e0b3739ed78b1fff628723a6:liverpool_fc5
5623bc6dcf13012f77f1bc6e867e4f9f:fr!3ndss
```

Поиск хэшей в pot-файле

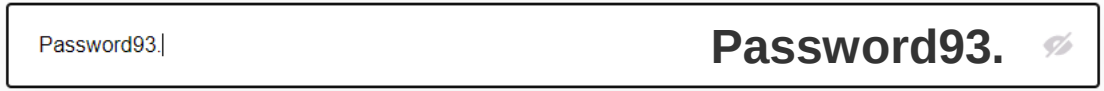
[Брутфорс хэшей в Active Directory / Хабр]

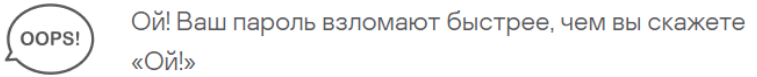


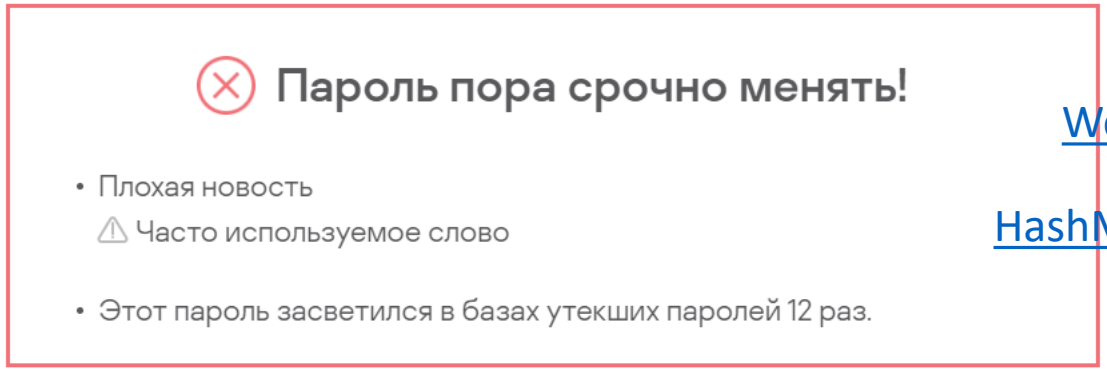
AD

Аудит + доработка AD:

- Учётные записи
- Брут паролей
- **Lithnet Password Protection**







[Weakpass: biggest wordlists collection]

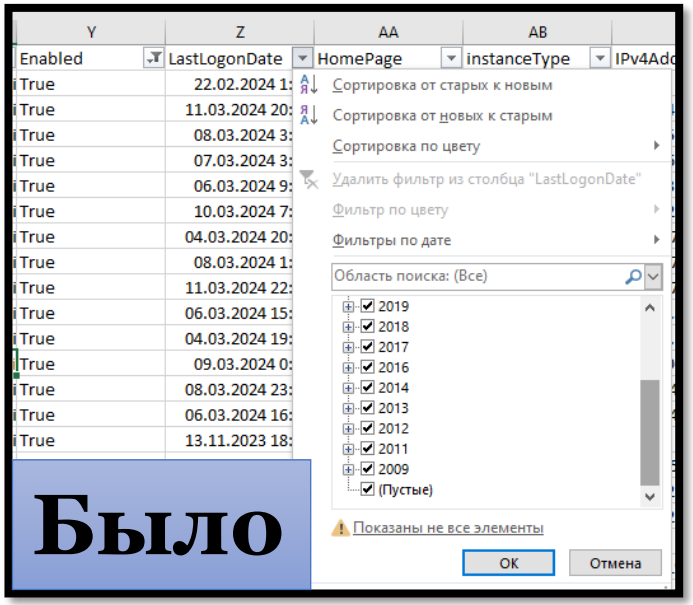
[HashMob | Resources | HashMob Wordlists]

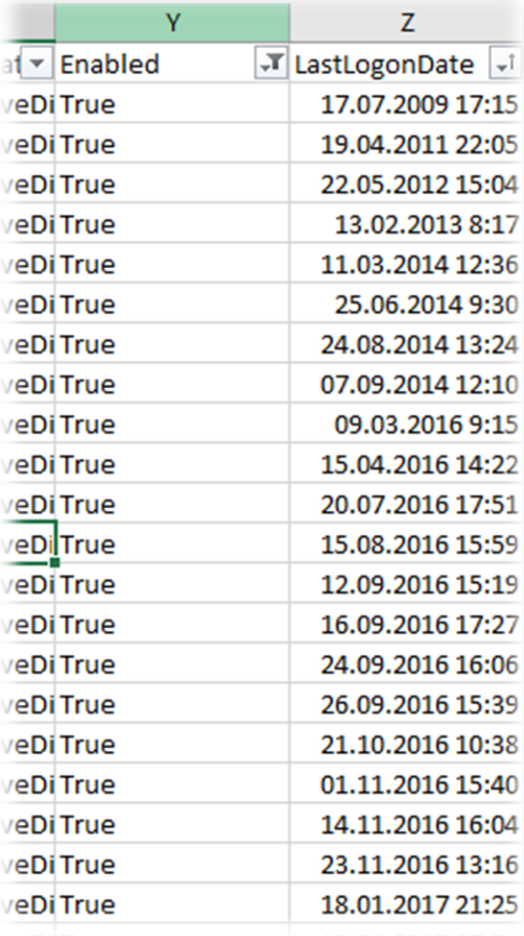
[Защита паролем AD — Lithnet]

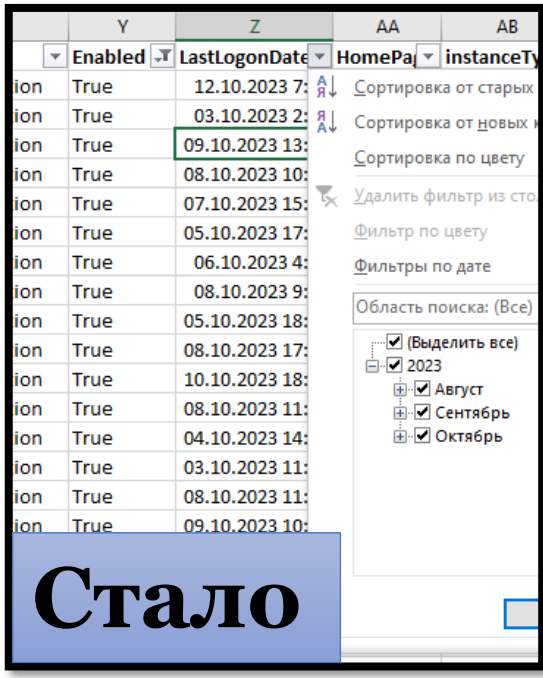
AD

Аудит + доработка AD:

- Учётные записи
- Брут паролей
- Lithnet Password Protection
- **Хосты**







AD

Аудит + доработка AD:

- Учётные записи
- Брут паролей
- Lithnet Password Protection
- Хосты
- **Неправильное наследование**

Компьютер	Путь	Применяется к	Пользователь/группа	Состояние наследования	Права объекта	Права родителя
ts.sus.local	\\ts.sus.loca	Для этой папки, ее подп	пользователи@builtin	Наследуется	F M X W R L S	F M X W R L S
ts.sus.local	\\ts.sus.loca	Для этой папки, ее подп	пользователи@builtin	Права преобразованы	F M X W R L S	F M X W R L S
		Для этой папки, ее подп	все	Права преобразованы	F M X W R L S	F M X W R L S
ts.sus.local	\\ts.sus.loca	Для этой папки, ее подп	пользователи@builtin	Права удалены		F M X W R L S
		Для этой папки, ее подп	все	Права удалены		F M X W R L S
ts.sus.local	\\ts.sus.loca	Для этой папки, ее подп	пользователи@builtin	Неверные флаги наследования	F M X W R L S	F M X W R L S
		Для этой папки, ее подп	пользователи@builtin	Наследование без родителя	F M X W R L S	
ts.sus.local	\\ts.sus.loca	Для этой папки, ее подп	пользователи@builtin	Ложное наследование		F M X W R L S
		Для этой папки, ее подп	все	Добавлен пользователь	F M X W R L S	
		Для этой папки, ее подп	служба@nt authority	Наследуется	F M X W R L S	F M X W R L S

AD

Аудит + доработка AD:

- Учётные записи
- Брут паролей
- Lithnet Password Protection
- Хосты
- Неправильное наследование
- **Пилоты DCAP**

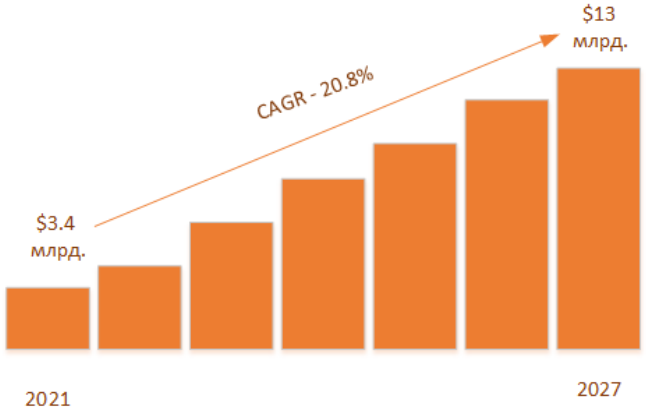
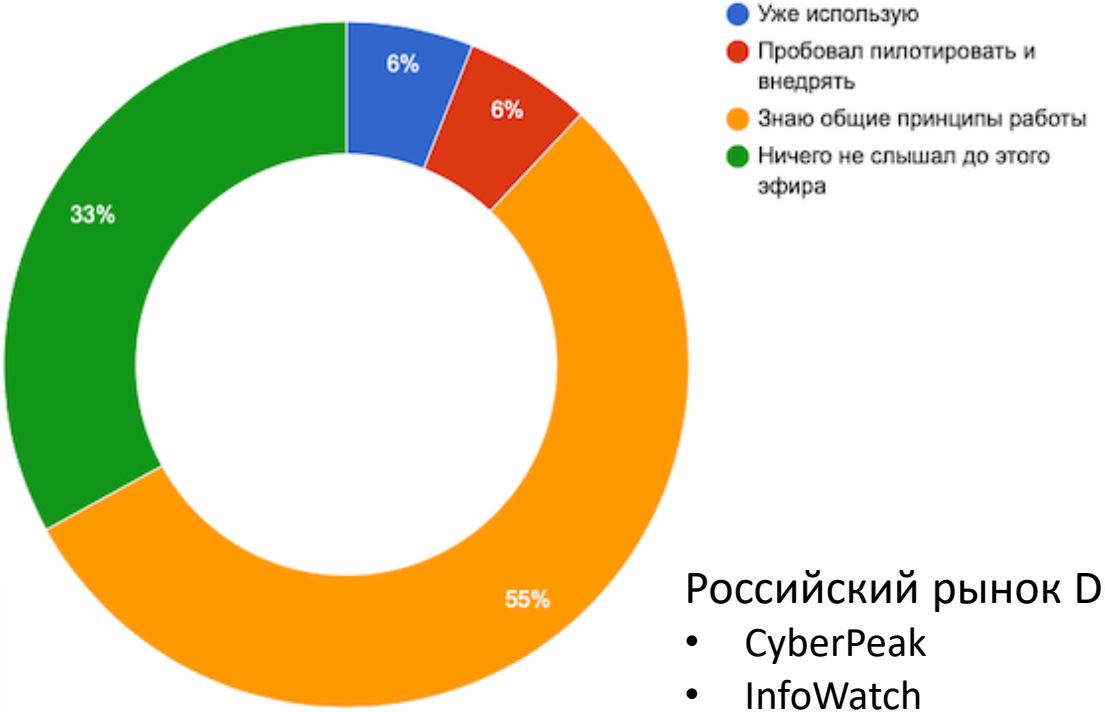


Рисунок 1. Насколько хорошо вы знакомы с решениями DCAP?



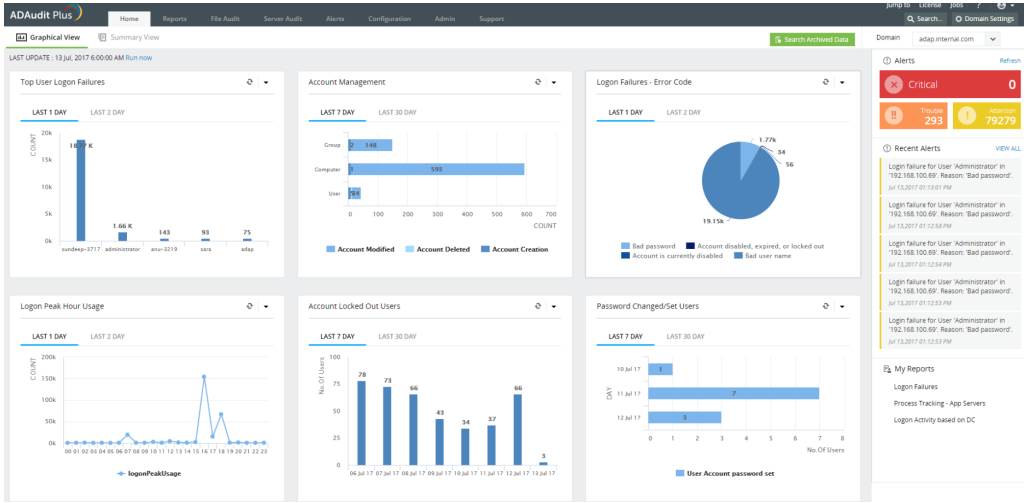
Российский рынок DCAP

- CyberPeak
- InfoWatch
- MAKVES
- Zecurion
- Орлан
- СёрчИнформ

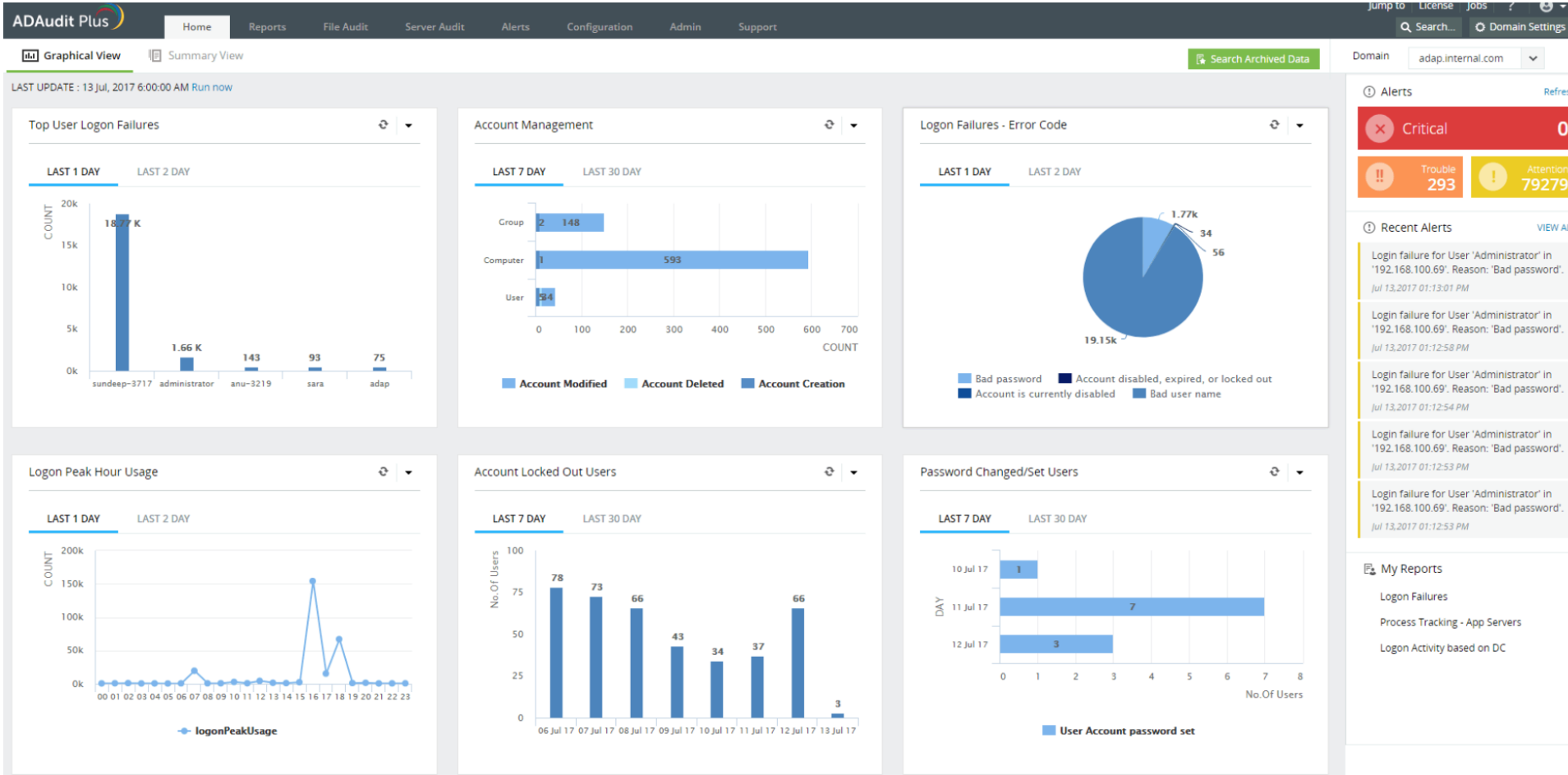
AD

Аудит + доработка AD:

- Учётные записи
- Брут паролей
- Lithnet Password Protection
- Хосты
- Неправильное наследование
- Пилоты DCAP
- **AD Audit Plus**



AD Audit plus



Анализ инфраструктуры

Аудит + доработка инфраструктуры:

- Аудит всех хостов в сети (Masscan + Nmap)
- Аудит всех портов в сети
- Аудит того, что торчит в интернет
- Аудит установленного ПО на хостах, каталог разрешённого
- IT CMDB актуальность
- Мониторинг инфраструктуры + аномальное поведение (Zabbix)

Анализ инфраструктуры

Аудит + доработка инфраструктуры:

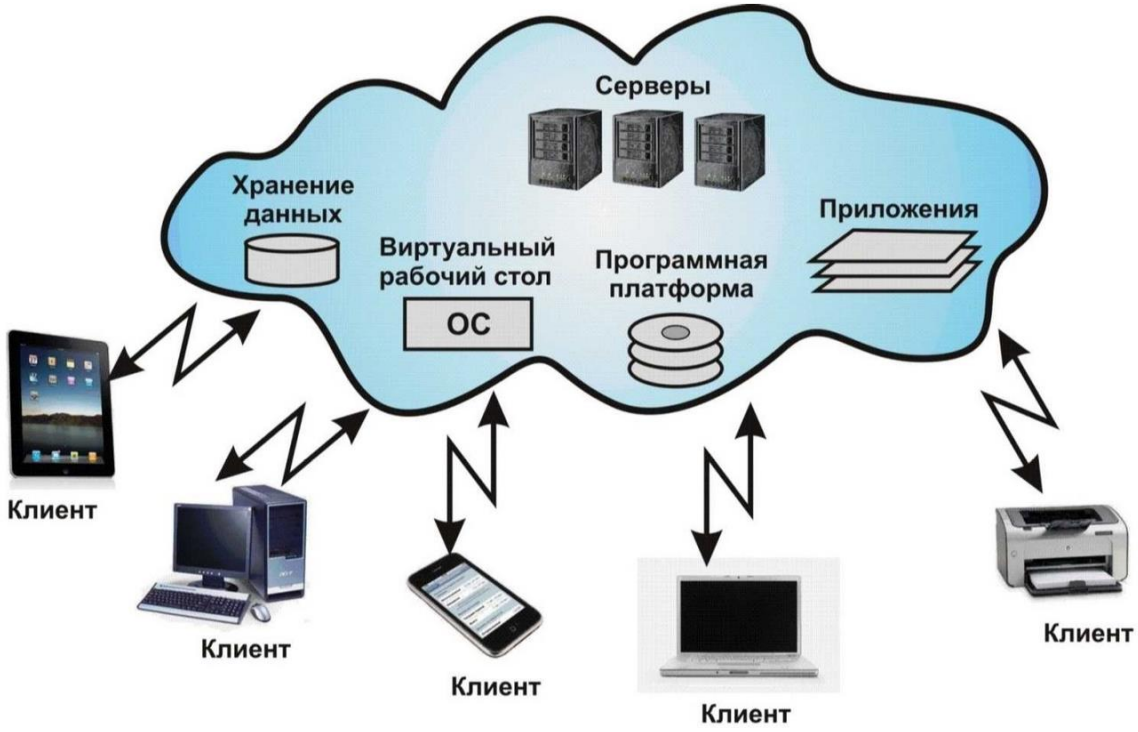
- **Аудит всех хостов в сети** (Masscan + Nmap)

MassCAN
Massachusetts Computing Attainment Network

+

NMAP

=



Анализ инфраструктуры

Аудит + доработка инфраструктуры:

- Аудит всех хостов в сети (Masscan + Nmap)
- **Аудит всех портов в сети**

		AB3	SOC	FLEET	EDR
ПК	200	200 (100%)	180 (90%)	160 (80%)	160 (80%)
Сервера	20				
?					
Всего	220				

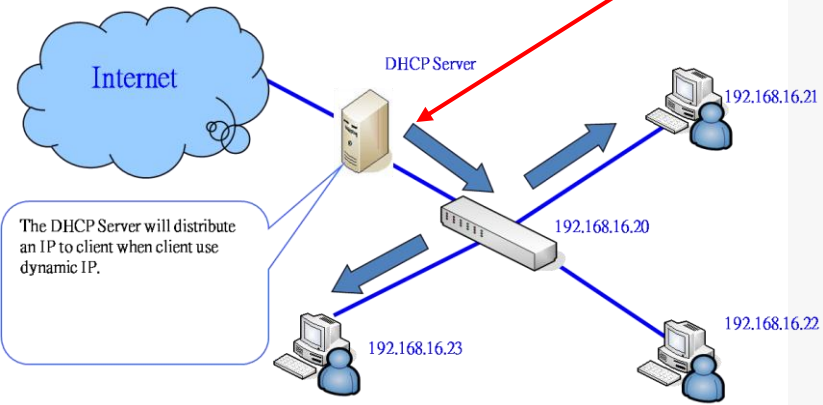
10.22.11.18	FLEET		
10.22.11.18	PORT		21/ftp/vsftpd/2.0.5/cpe:/a:vsftpd:vsftpd:2.0.5 | 21/
10.22.11.18	PORT		23/telnet/Linux telnetd//cpe:/o:linux:linux_kernel | 23/
10.22.11.18	PORT		80/http/mini_httpd/1.19 19dec2003/cpe:/a:acme:mini_httpd:1.19_19dec2003 | 80/{"http-server-header": "mini_httpd/1.19 19dec2003", "http-title": "Site
10.22.11.18	PORT		427/svrloc/// | 427/
10.22.11.18	PORT		1720/h323q931/// | 1720/
10.22.11.18	PORT		5000/reverse-ssl/SSL/TLS ClientHello// | 5000/{"fingerprint-strings": "\n ZendJavaBridge: \n GetClassName"}
10.22.11.18	PORT		5988/http/Web-Based Enterprise Management CIM serverOpenPegasus WBEM httpd//cpe:/o:linux:linux_kernel | 5988/{"http-title": "Site doesn't have
10.22.11.18	MAIN_DATA		
10.22.11.18	KSC		
10.22.11.18	FLEET		
10.0.55.112	PORT		135/msrpc/// | 135/
10.0.55.112	PORT		139/netbios-ssn/Microsoft Windows netbios-ssn//cpe:/o:microsoft:windows | 139/
10.0.55.112	PORT		445/microsoft-ds/// | 445/
10.0.55.112	PORT		1720/h323q931/// | 1720/
10.0.55.112	PORT		1947/sentinelsrm/// | 1947/{"fingerprint-strings": "\n FourOhFourRequest: \n HTTP/1.0 403 Forbidden\n Server: HASP LM/24.00\n Date: Sat, 02 No
10.0.55.112	PORT		2701/cmrcservice/Microsoft Configuration Manager Remote Control service//cpe:/o:microsoft:windows | 2701/
10.0.55.112	PORT		3389/ms-wbt-server/Microsoft Terminal Services//cpe:/o:microsoft:windows | 3389/{"ssl-cert": "Subject: commonName=OLEG-VOLKOV.domen.local\nN
10.0.55.112	PORT		5040/unknown/// | 5040/
10.0.55.112	PORT		5357/http/Microsoft HTTPAPI httpd/2.0/cpe:/o:microsoft:windows | 5357/{"http-title": "Service Unavailable"}
10.0.55.112	PORT		7680/pando-pub/// | 7680/
10.0.55.112	PORT		8005/http/Microsoft HTTPAPI httpd/2.0/cpe:/o:microsoft:windows | 8005/{"http-title": "Bad Request"}
10.0.55.112	PORT		47001/http/Microsoft HTTPAPI httpd/2.0/cpe:/o:microsoft:windows | 47001/{"http-title": "Not Found"}
10.0.55.112	PORT		47546/msrpc/Microsoft Windows RPC//cpe:/o:microsoft:windows | 47546/
10.0.55.112	PORT		49664/msrpc/Microsoft Windows RPC//cpe:/o:microsoft:windows | 49664/
10.0.55.112	PORT		49665/msrpc/Microsoft Windows RPC//cpe:/o:microsoft:windows | 49665/
10.0.55.112	PORT		49666/msrpc/Microsoft Windows RPC//cpe:/o:microsoft:windows | 49666/
10.0.55.112	PORT		49667/msrpc/Microsoft Windows RPC//cpe:/o:microsoft:windows | 49667/
10.0.55.112	PORT		49669/msrpc/Microsoft Windows RPC//cpe:/o:microsoft:windows | 49669/
10.0.55.112	PORT		49672/msrpc/Microsoft Windows RPC//cpe:/o:microsoft:windows | 49672/
10.0.55.112	PORT		49673/msrpc/Microsoft Windows RPC//cpe:/o:microsoft:windows | 49673/
10.0.55.112	PORT		49674/msrpc/Microsoft Windows RPC//cpe:/o:microsoft:windows | 49674/
10.0.55.112	PORT		49708/msrpc/Microsoft Windows RPC//cpe:/o:microsoft:windows | 49708/

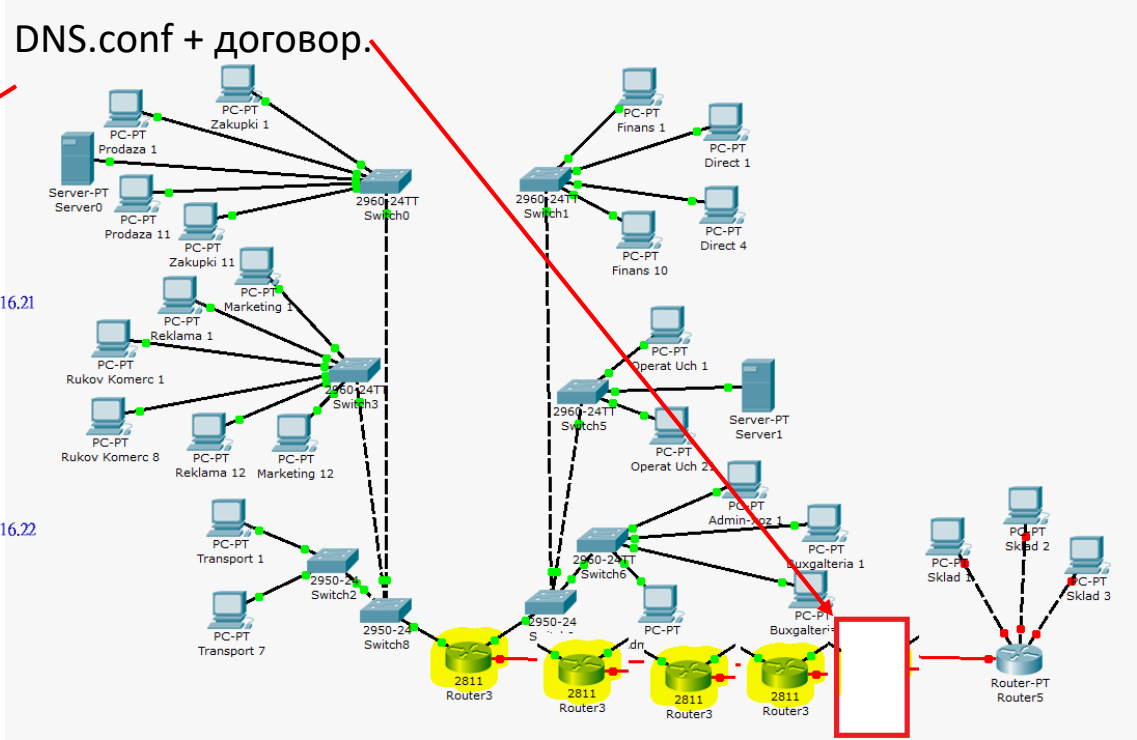
Анализ инфраструктуры

Аудит + доработка инфраструктуры:

- Аудит всех хостов в сети (Masscan + Nmap)
- Аудит всех портов в сети
- **Аудит того, что торчит в интернет**

DNS.conf + договор.

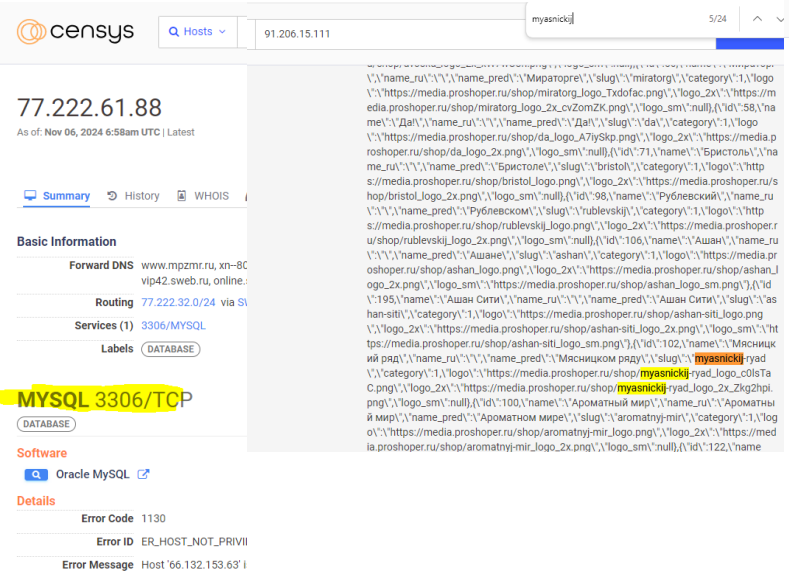


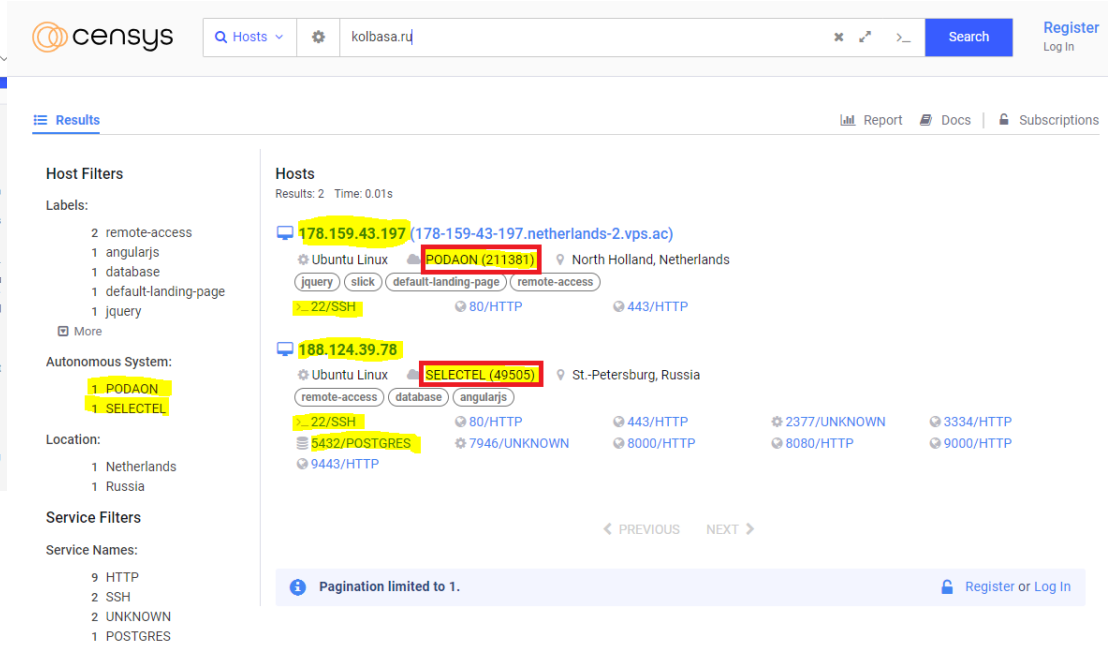


Анализ инфраструктуры

Аудит + доработка инфраструктуры:

- Аудит всех хостов в сети (Masscan + Nmap)
- Аудит всех портов в сети
- **Аудит того, что торчит в интернет** Посмотреть OSINT + Scanner

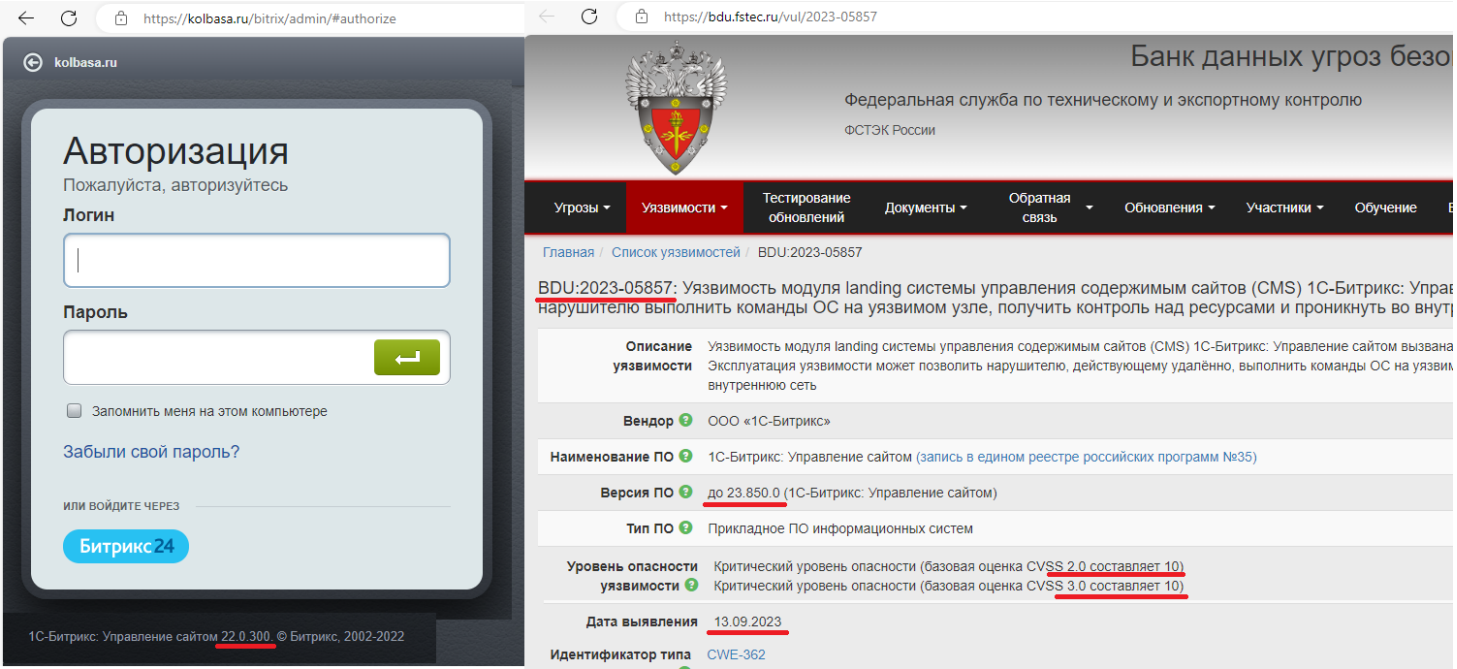


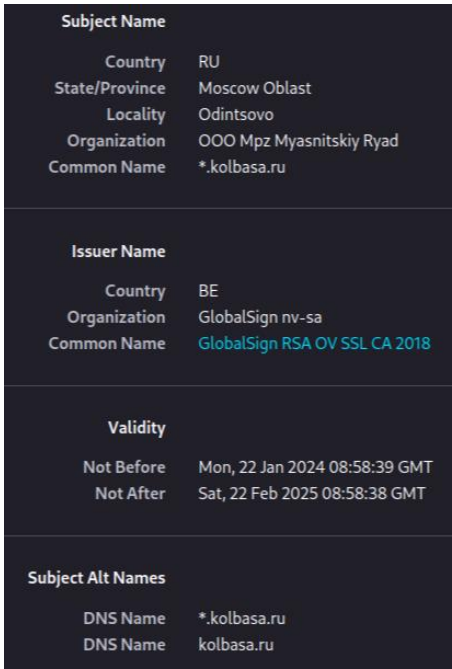


Анализ инфраструктуры

Аудит + доработка инфраструктуры:

- Аудит всех хостов в сети (Masscan + Nmap)
- Аудит всех портов в сети
- **Аудит того, что торчит в интернет** Посмотреть OSINT + Scanner

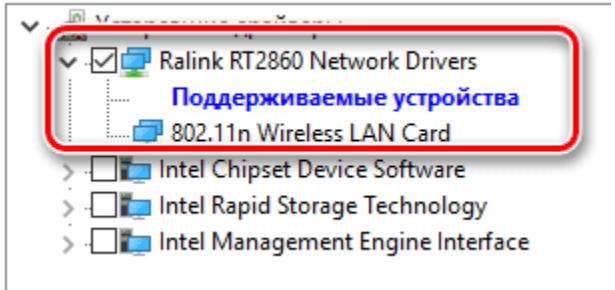




Анализ инфраструктуры

Аудит + доработка инфраструктуры:

- Аудит всех хостов в сети (Masscan + Nmap)
- Аудит всех портов в сети
- Аудит того, что торчит в интернет
- **Аудит установленного ПО на хостах, каталог разрешённого**



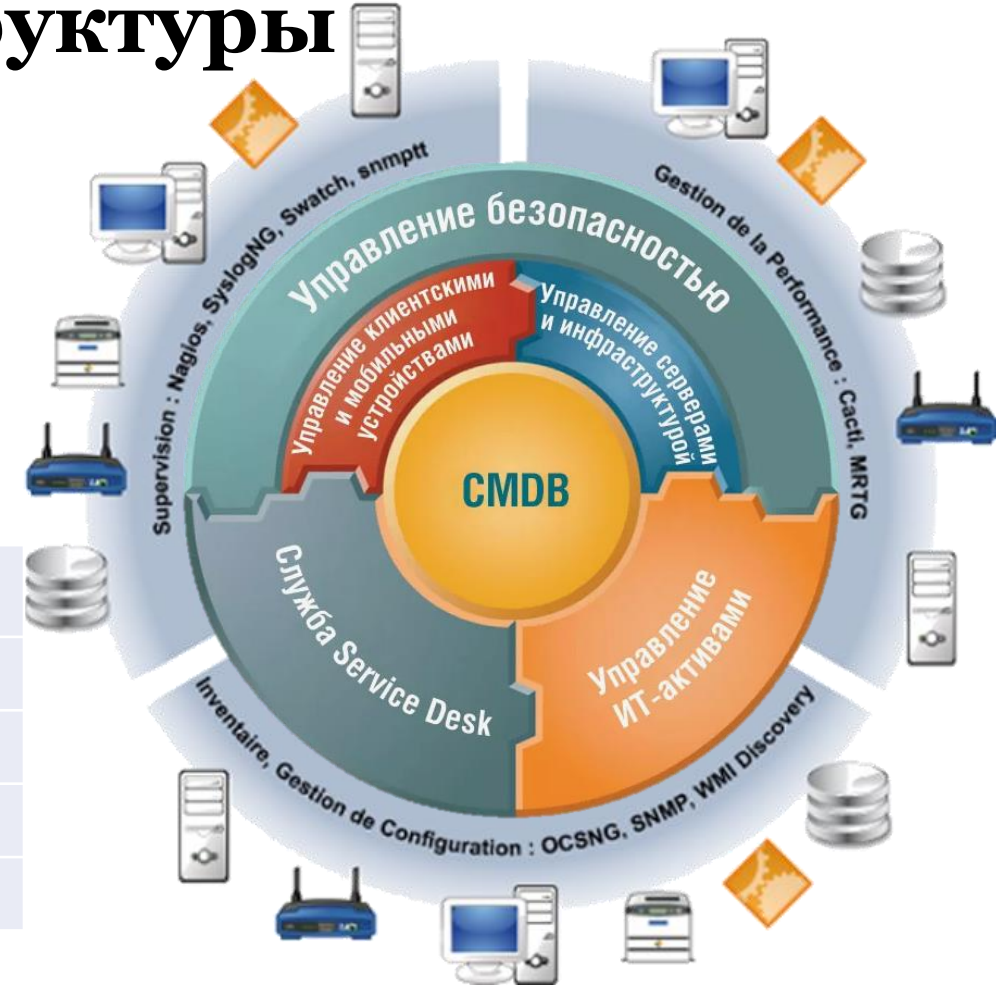
Альт Линукс СПТ
Альт
ОСь
Astra Linux
ROSA Linux
Calculate Linux
Ульяновск BSD
ICLinux
Альфа ОС
Эльбрус
Ред ОС
GosLinux
AlterOS
Мобильная система Вооружённых Сил
Заря
RAIDIX
Kraftway Terminal Linux
WTware
KasperskyOS
ОСРВ «МАКС»
Учетные системы
Складские системы
Логистическое ПО
Склад-15

Анализ инфраструктуры

Аудит + доработка инфраструктуры:

- Аудит всех хостов в сети (Masscan + Nmap)
- Аудит всех портов в сети
- Аудит того, что торчит в интернет
- Аудит установленного ПО на хостах
- **IT CMDB актуальность**

(Покрытие, реагирование на инциденты и др.)

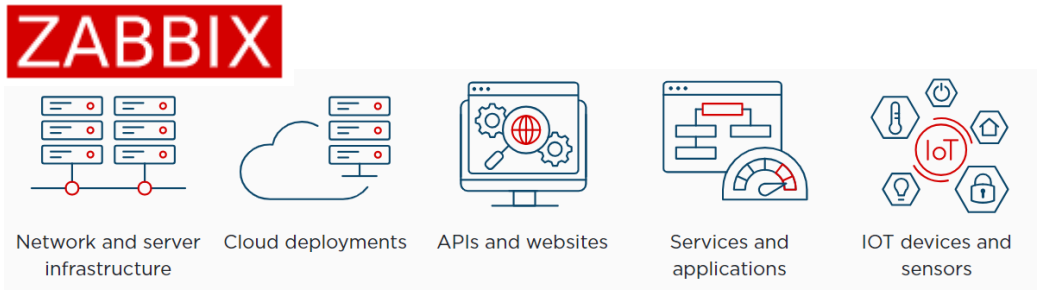


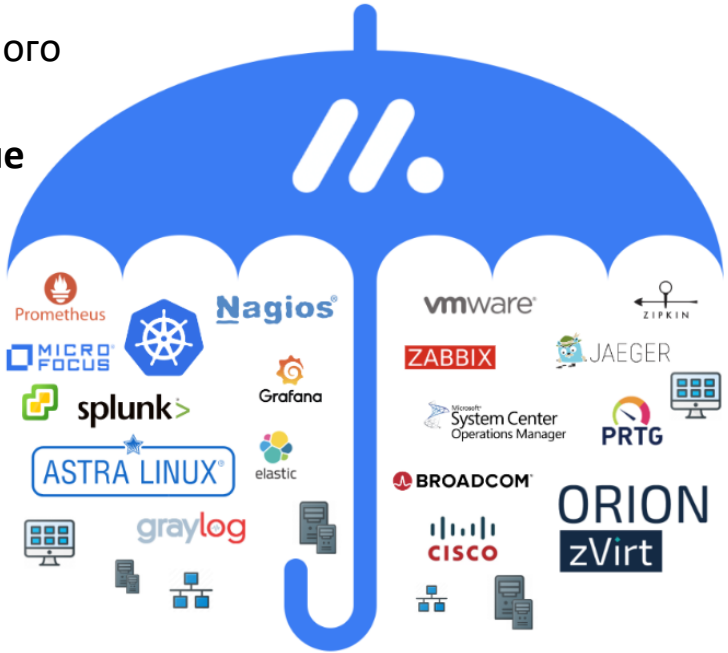
IP	NAME	ССЫЛКА	Владелец
90.90.72.39	G0000-EX31	https://ShowObject.jspa?id=92004	Игорь Игоревич Игорев
90.90.48.39	G-0000-5202	https://ShowObject.jspa?id=92699	Игорь Игоревич Игорев
90.86.4.2	G2800-SQ01	https://ShowObject.jspa?id=99942	Иванов Иван Иванович
90.46.0.57	G6400-DP01	https://ShowObject.jspa?id=92969	Иванов Иван Иванович

Анализ инфраструктуры

Аудит + доработка инфраструктуры:

- Аудит всех хостов в сети (Masscan + Nmap)
- Аудит всех портов в сети
- Аудит того, что торчит в интернет
- Аудит установленного ПО на хостах, каталог разрешённого
- IT CMDB актуальность
- **Мониторинг инфраструктуры + аномальное поведение (история про Zabbix)**





Начальные телодвижения

Установка, настройка, доработка:

- Ограничение физического доступа к инфраструктуре.
- Покрытие СЗИ всех возможных устройств
- Выстраивание правильных метрик покрытия
- Защита почты (Proxmox mail + SMG)
- Менеджеры паролей
- Минимальные права у юзера
- Запрет работать из под администратора администраторам
- Внедрение Local Administrator Password Solution (LAPS)
- VPN + 2ФА - удалённая работа
- 2ФА везде где возможно, 100% внешка.
- Пром данные только в проме

Начальные телодвижения

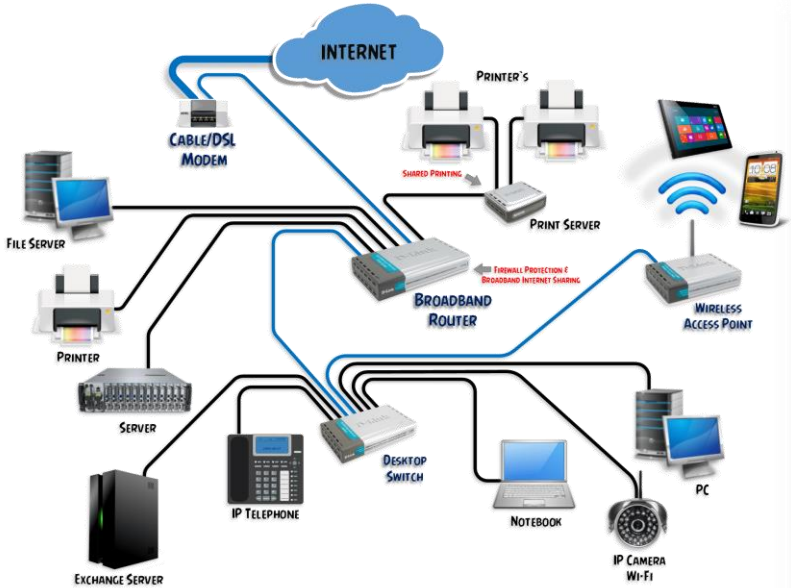
Установка, настройка, доработка:

- **Ограничение физического доступа к инфраструктуре.**

Начальные телодвижения

Установка, настройка, доработка:

- Ограничение физического доступа к инфраструктуре.
- **Покрытие СЗИ всех возможных устройств**



Начальные телодвижения

Установка, настройка, доработка:

- Ограничение физического доступа к инфраструктуре.
- Покрытие СЗИ всех возможных устройств
- **Выстраивание правильных метрик покрытия**

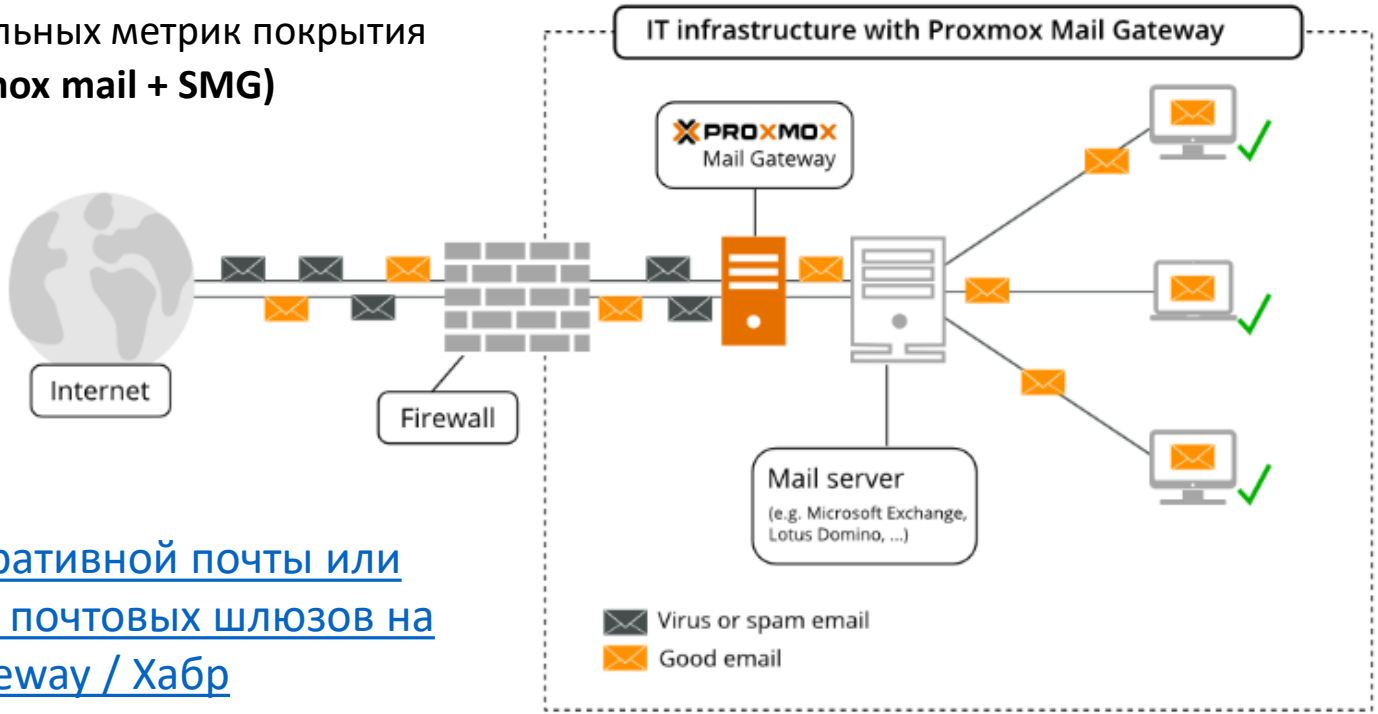
АВЗ EDR SOC IDS DLP …

	Кол-во	АВЗ	SOC	FLEET	EDR
ПК	177	173 (98.3%) Из 176	None	165 (93.75%) Из 176	158 (89.77%) Из 176
Сервера	54	50 (96.15%) Из 52	14 (26.92%) Из 52	38 (73.08%) Из 52	51 (98.08%) Из 52
Прочее	392	None	4	None	None
Всего	624	223, (97.81%) Из 228	14, (8.0%) Из 225	203, (89.04%) Из 228	209, (91.67%) Из 228

Начальные телодвижения

Установка, настройка, доработка:

- Ограничение физического доступа к инфраструктуре.
- Покрытие СЗИ всех возможных устройств
- Выстраивание правильных метрик покрытия
- **Защита почты (Proxmox mail + SMG)**

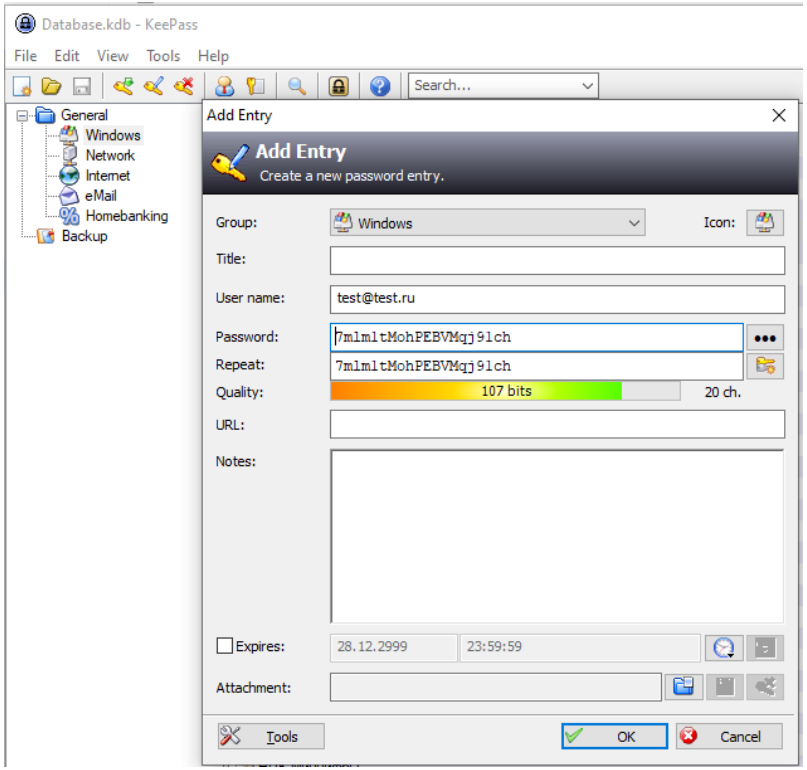


[ЧудESA защиты корпоративной почты или внедрение свободных почтовых шлюзов на базе Proxmox Mail Gateway / Хабр]

Начальные телодвижения

Установка, настройка, доработка:

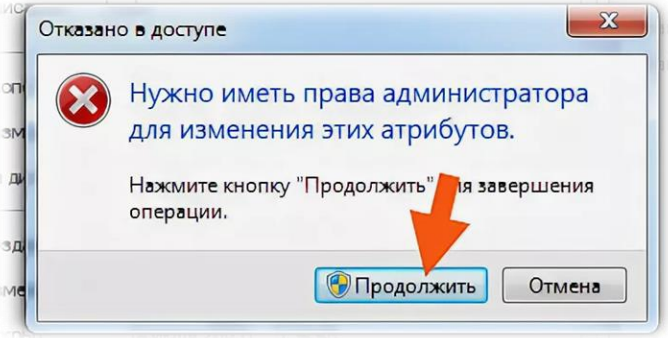
- Ограничение физического доступа к инфраструктуре.
- Покрытие СЗИ всех возможных устройств
- Выстраивание правильных метрик покрытия
- Защита почты (Proxmox mail + SMG)
- **Менеджеры паролей**



Начальные телодвижения

Установка, настройка, доработка:

- Ограничение физического доступа к инфраструктуре.
- Покрытие СЗИ всех возможных устройств
- Выстраивание правильных метрик покрытия
- Защита почты (Proxmox mail + SMG)
- Менеджеры паролей
- **Минимальные права у юзера**



Начальные телодвижения

Установка, настройка, доработка:

- Ограничение физического доступа к инфраструктуре.
- Покрытие СЗИ всех возможных устройств
- Выстраивание правильных метрик покрытия
- Защита почты (Proxmox mail + SMG)
- Менеджеры паролей
- Минимальные права у юзера
- **Запрет работать из под администратора администраторам**

[конспект админа] Меньше администраторов всем / Хабр

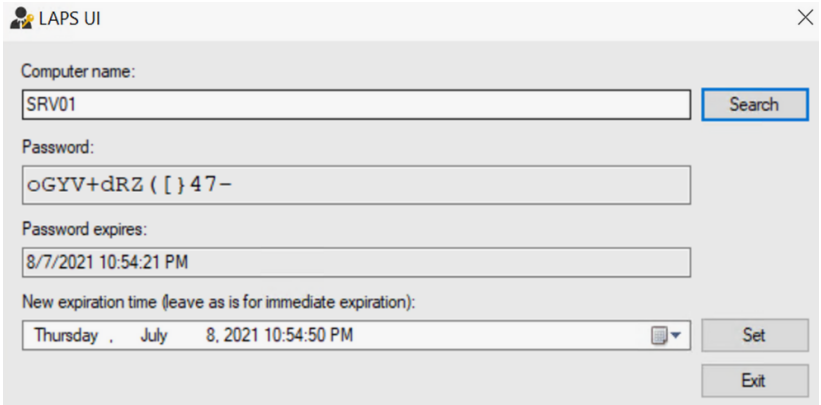
Начальные телодвижения

Установка, настройка, доработка:

- Ограничение физического доступа к инфраструктуре.
- Покрытие СЗИ всех возможных устройств
- Выстраивание правильных метрик покрытия
- Защита почты (Proxmox mail + SMG)
- Менеджеры паролей
- Минимальные права у юзера
- Запрет работать из под администратора администраторам
- **Внедрение Local Administrator Password Solution (LAPS)**

Microsoft LAPS

Local Administrator Password Solution



[Управляем паролем локального администратора с помощью LAPS / Хабр]

Начальные телодвижения

Установка, настройка, доработка:

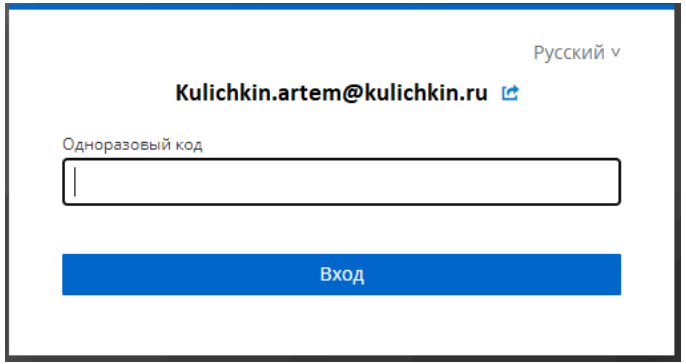
- Ограничение физического доступа к инфраструктуре.
- Покрытие СЗИ всех возможных устройств
- Выстраивание правильных метрик покрытия
- Защита почты (Proxmox mail + SMG)
- Менеджеры паролей
- Минимальные права у юзера
- Запрет работать из под администратора администраторам
- Внедрение Local Administrator Password Solution (LAPS)
- **VPN + 2ФА - удалённая работа**

VPN (**RRAS, CISCO, др.**) + Radius + любой OTP

Начальные телодвижения

Установка, настройка, доработка:

- Ограничение физического доступа к инфраструктуре.
- Покрытие СЗИ всех возможных устройств
- Выстраивание правильных метрик покрытия
- Защита почты (Proxmox mail + SMG)
- Менеджеры паролей
- Минимальные права у юзера
- Запрет работать из под администратора администраторам
- Внедрение Local Administrator Password Solution (LAPS)
- VPN + 2ФА - удалённая работа
- **2ФА везде где возможно, 100% внешка**



Начальные телодвижения

Установка, настройка, доработка:

- Ограничение физического доступа к инфраструктуре.
- Покрытие СЗИ всех возможных устройств
- Выстраивание правильных метрик покрытия
- Защита почты (Proxmox mail + SMG)
- Менеджеры паролей
- Минимальные права у юзера
- Запрет работать из под администратора администраторам
- Внедрение Local Administrator Password Solution (LAPS)
- VPN + 2ФА - удалённая работа
- 2ФА везде где возможно, 100% внешка
- **Пром. данные только в проме**

Администрирование

Установка, настройка, доработка:

- Администрирование только из специального сегмента с отдельными учётками и правами
- Включить расширенный аудит eventlog, Symon, auditd.
- Менеджер паролей KeePass
- Минимальные права доступа
- Tier 1, Tier 2, Tier 3, Tier 4
- SSH авторизация по ключам
- Патч менеджемент, обновление ОС, ПО.
- Бекап и восстановление + проверка.
- Запретить вход через рут по ssh

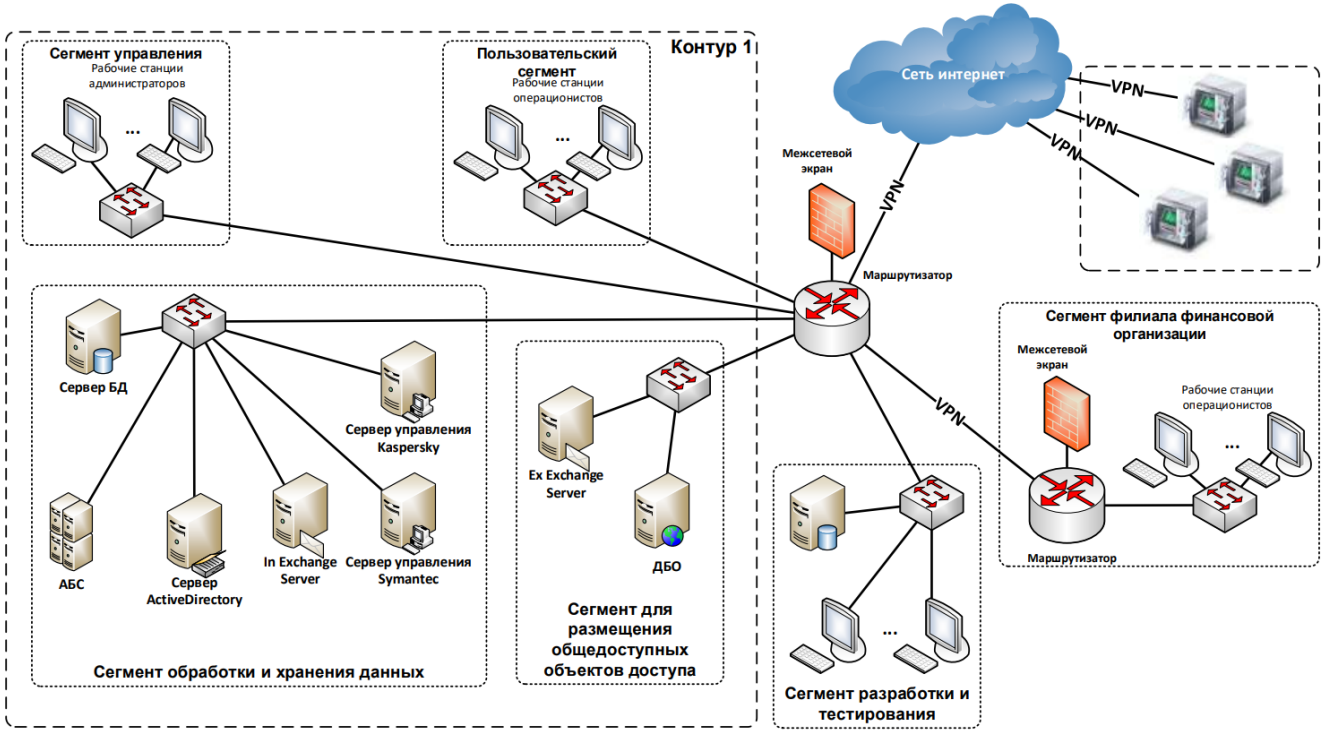
Прописать в ОРД спина болеть не будет

Администрирование

Установка, настройка, доработка:

- **Администрирование только из специального сегмента с отдельными учётками и правами**

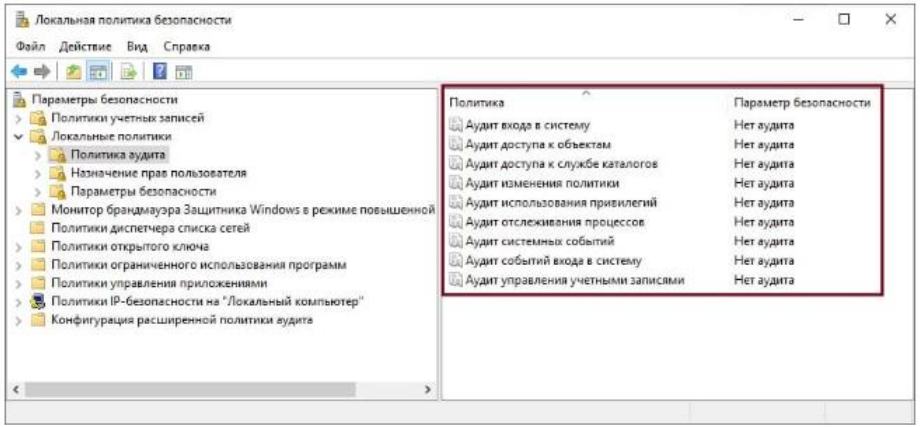
- ✓ Сегментирование сети
- ✓ Разделять прод, тест, деф.
- ✓ Запретить выход в интернет из серверного сегмента
- ✓ Выход в интернет через единый прокси с авторизацией



Администрирование

Установка, настройка, доработка:

- Администрирование только из специального сегмента с отдельными учётками и правами
- **Включить расширенный аудит eventlog, Symon, auditd.**



Настройка аудита в Windows для полноценного SOC-мониторинга

Основы аудита. Настраиваем журналирование важных событий в Linux — Хакер

Администрирование

Установка, настройка, доработка:

- Администрирование только из специального сегмента с отдельными учётками и правами
- Включить расширенный аудит eventlog, Symon, auditd.
- **Менеджер паролей KeePass**

Администрирование

Установка, настройка, доработка:

- Администрирование только из специального сегмента с отдельными учётками и правами
- Включить расширенный аудит eventlog, Symon, auditd.
- Менеджер паролей KeePass
- **Минимальные права доступа**

Администрирование

Установка, настройка, доработка:

- Администрирование только из специального сегмента с отдельными учётками и правами
- Включить расширенный аудит eventlog, Symon, auditd.
- Менеджер паролей KeePass
- Минимальные права доступа
- **Tier 0, Tier 1, Tier 2, Tier 3**

Tier 0

Tier 1

Tier 2

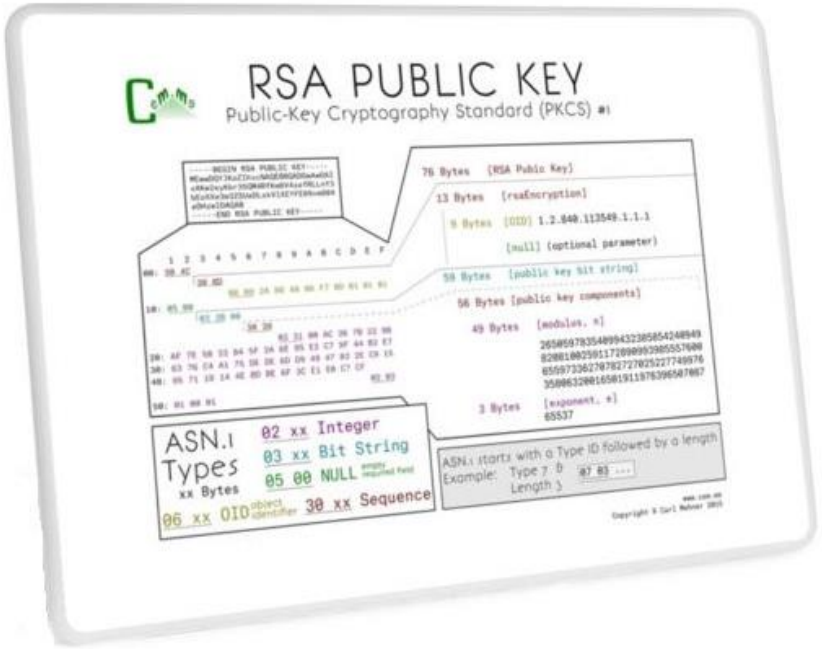
Tier 3

[Многоуровневая модель среды PAM | Microsoft Learn]

Администрирование

Установка, настройка, доработка:

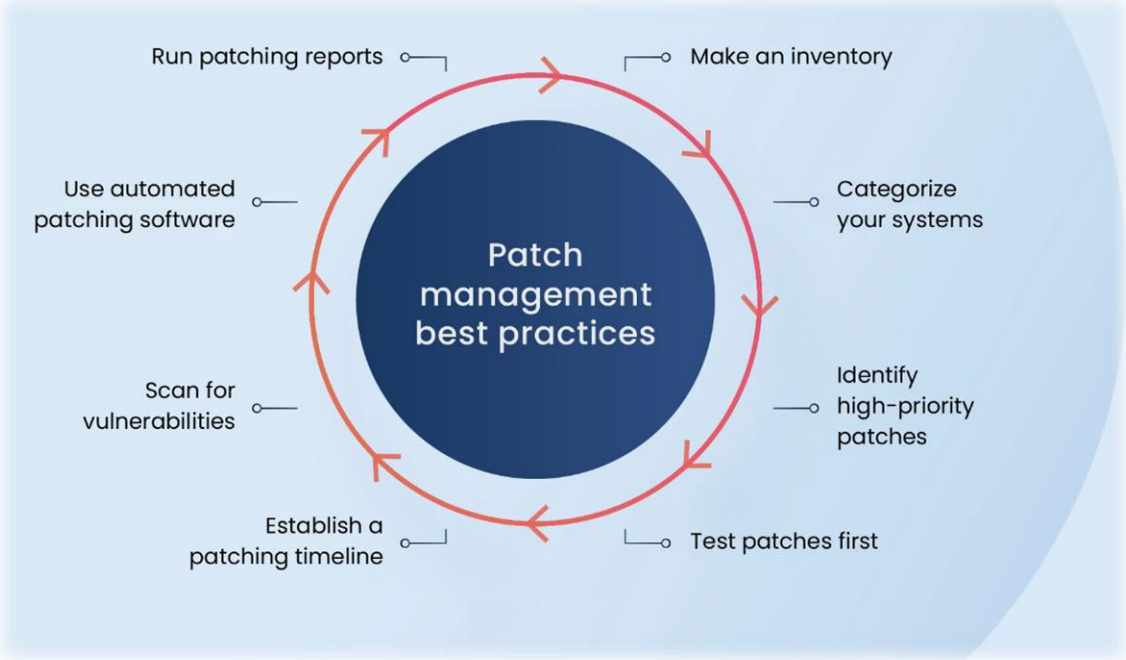
- Администрирование только из специального сегмента с отдельными учётками и правами
- Включить расширенный аудит eventlog, Symon, auditd.
- Менеджер паролей KeePass
- Минимальные права доступа
- Tier 1, Tier 2, Tier 3, Tier 4
- **SSH авторизация по ключам**



Администрирование

Установка, настройка, доработка:

- Администрирование только из специального сегмента с отдельными учётками и правами
- Включить расширенный аудит eventlog, Symon, auditd.
- Менеджер паролей KeePass
- Минимальные права доступа
- Tier 1, Tier 2, Tier 3, Tier 4
- SSH авторизация по ключам
- **Патч менеджемент**



Администрирование

Установка, настройка, доработка:

- Администрирование только из специального сегмента с отдельными учётками и правами
- Включить расширенный аудит eventlog, Symon, auditd.
- Менеджер паролей KeePass
- Минимальные права доступа
- Tier 1, Tier 2, Tier 3, Tier 4
- SSH авторизация по ключам
- Патч менеджемент
- **Бекап и восстановление + проверка.**

Администрирование

Установка, настройка, доработка:

- Администрирование только из специального сегмента с отдельными учётками и правами
- Включить расширенный аудит eventlog, Symon, auditd.
- Менеджер паролей KeePass
- Минимальные права доступа
- Tier 1, Tier 2, Tier 3, Tier 4
- SSH авторизация по ключам
- Патч менеджемент
- Бекап и восстановление + проверка.
- **Запретить вход через рут по ssh**

Прописать в ОРД спина болеть не будет

Администрирование

Установка, настройка, доработка:

- Администрирование только из специального сегмента с отдельными учётками и правами
- Включить расширенный аудит eventlog, Symon, auditd.
- Менеджер паролей KeePass
- Минимальные права доступа
- Tier 1, Tier 2, Tier 3, Tier 4
- SSH авторизация по ключам
- Патч менеджемент
- Бекап и восстановление + проверка.
- Запретить вход через рут по ssh

Прописать в ОРД спина болеть не будет

Немного допов

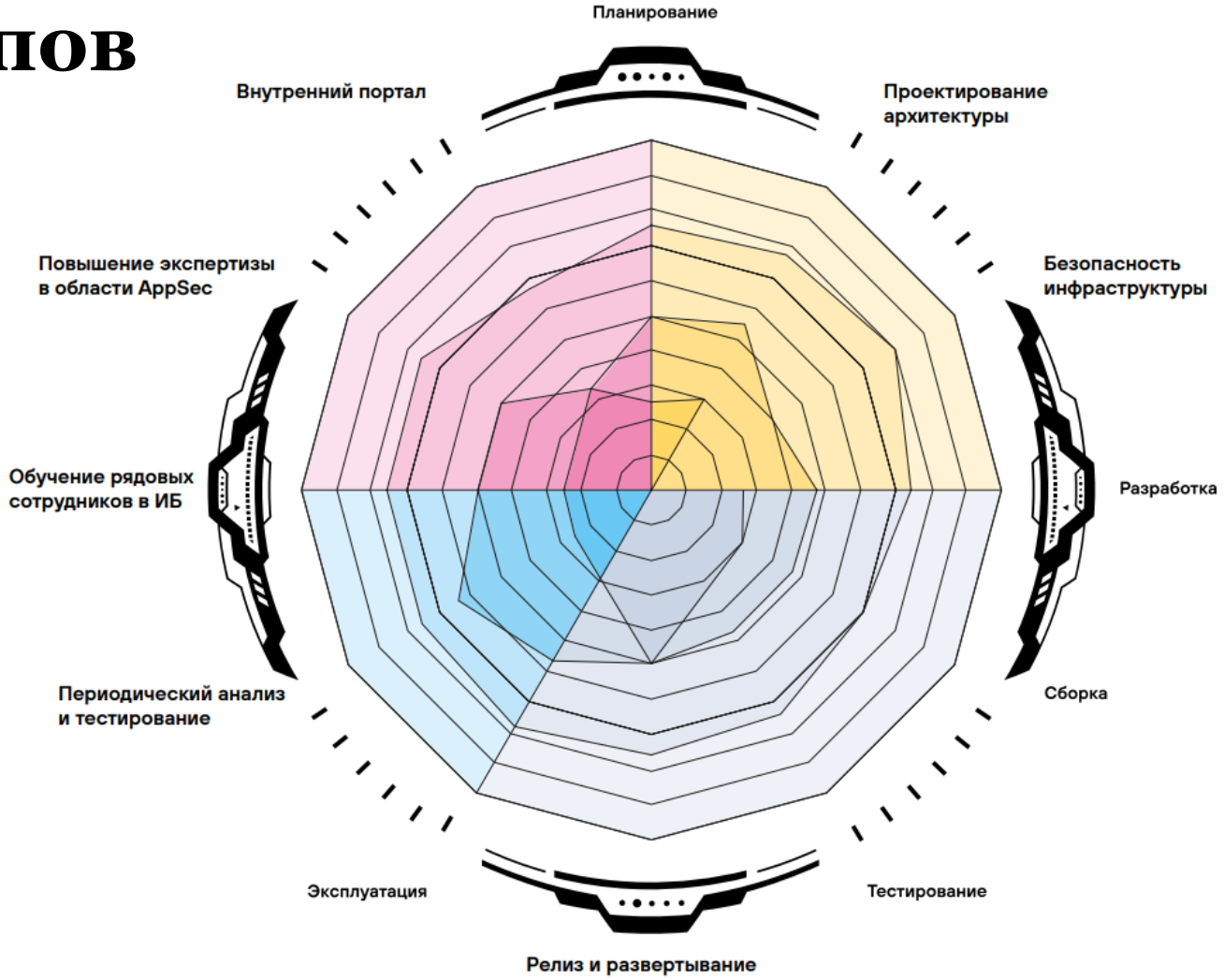
Установка, настройка, доработка:

- Процесс безопасной разработки opensource решениями. (metodologiya-appsec-table-top.pdf)
- Запрет запуска из “Download”
- Нет секретов в коде
- Hardening fleet
- AntiDDos на уровне провайдера
- Обучение работников, тестовый фишинг (Используйте доступные онлайн-ресурсы и руководства, пилоты)
- Анализ утечек «haveibeenpwned.com»
- Проверка ПО в песочнице: кукушка, энираn.
- Wazuh
- Пилоты! DCAP и тд…

Немного допов

Установка, настройка, доработка:

- Процесс безопасной разработки opensource решениями. (metodologiya-appsec-table-top.pdf)



Заключение

Даже при ограниченном бюджете можно обеспечить достаточный уровень информационной безопасности. Ключ к успеху – это проактивный подход, использование бесплатных инструментов и постоянное обучение. Помните, что информационная безопасность – это непрерывный процесс, требующий постоянного внимания и адаптации к новым угрозам.