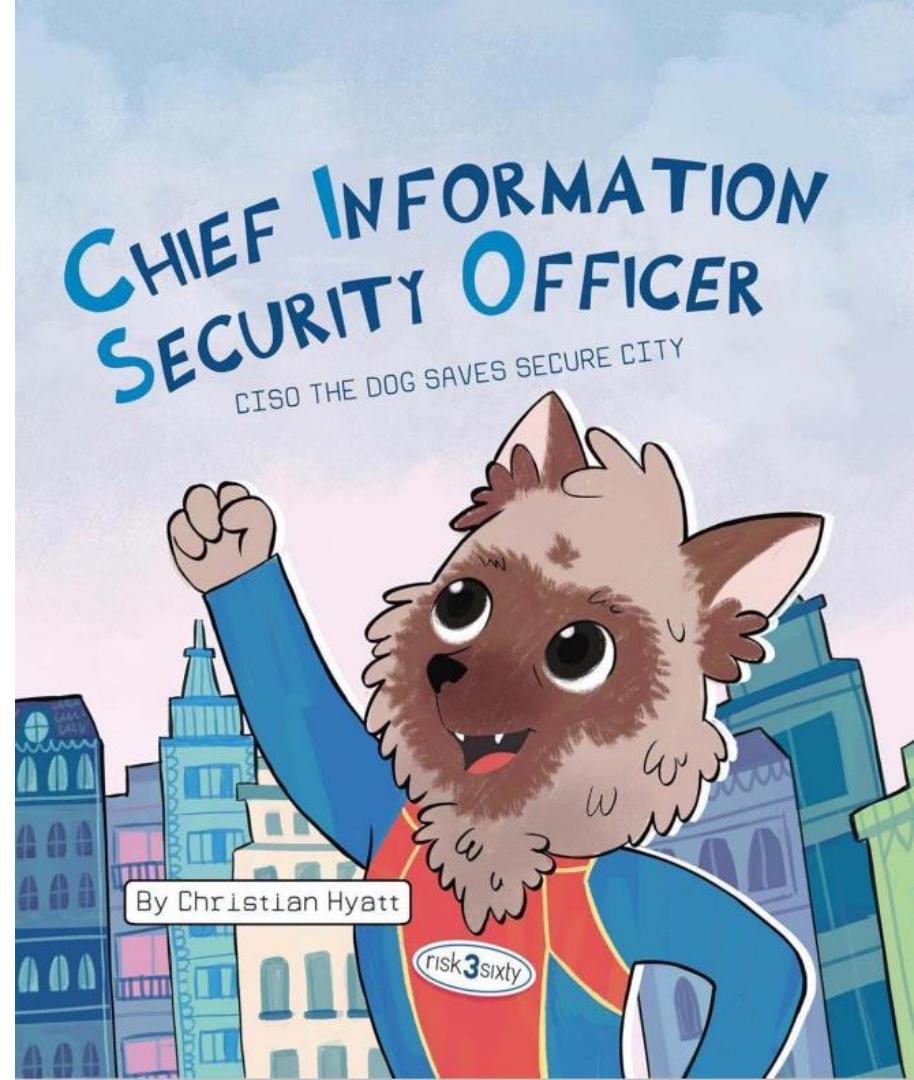


# Первые шаги в ИБ

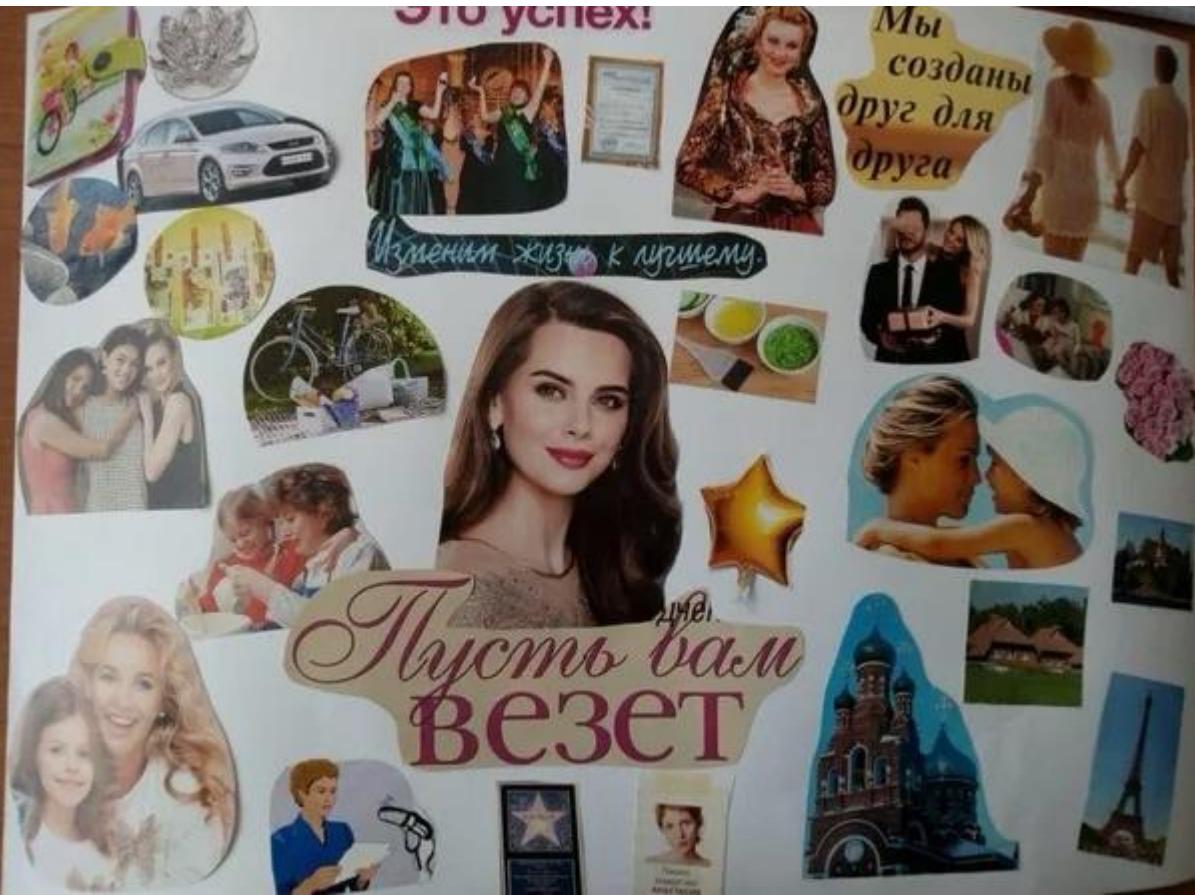


Куличкин Артём Александрович

CISO, CISM, CISA, CEH, CND.



## Карьера карта желаний



# Введение

Связиста замечают только тогда, когда пропадает связь.



# Топ 3 профессий в сфере И

- «[Аналитик SOC](#), инженер информационной безопасности, пентестер».
- «[Фorenзика](#), безопасность разработки, управление в области ИБ».
- «Кроме внедрения СЗИ, безопасной разработки и фorenзики 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%.

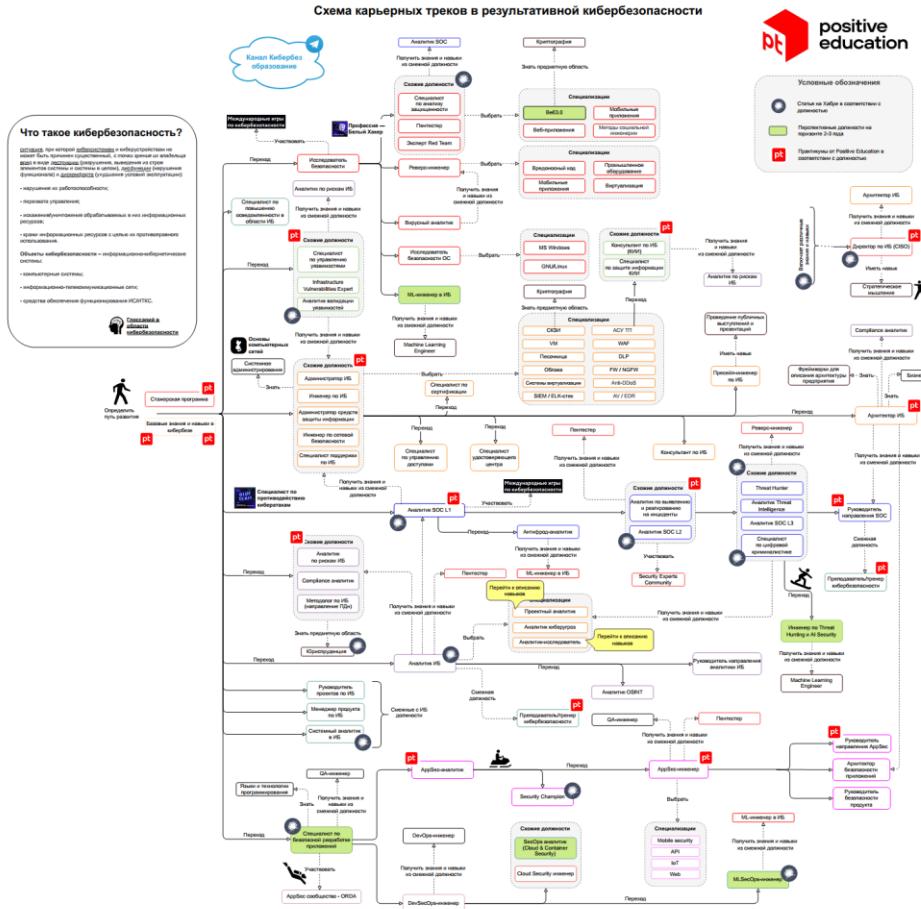
**Рисунок 2. В какой области ИБ вам хотелось бы получить дополнительные знания?**



**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

Разведка	Подготовка ресурсов	Первоначальный доступ	Выполнение	Закрепление	Повышение привилегий
T1596 Поиск технической информации в общедоступных источниках  0/5	T1586 Компрометация учетных записей  0/3	T1133 Внешние службы удаленного доступа	T1610 Развертывание контейнера	T1543 Создание или изменение системных процессов  4/5	T1543 Создание или изменение системных процессов  4/5
T1595 Активное сканирование  3/3	T1583 Приобретение инфраструктуры  ▼	T1189 Теневая (drive-by) компрометация	T1059 Интерпретаторы командной строки и сценариев  9/10	T1133 Внешние службы удаленного доступа  ▼	T1548 Обход механизмов контроля привилегий  4/6
T1590 Сбор информации об атакуемой сетевой инфраструктуре  6/6	T1584 Компрометация сторонней инфраструктуры  ▼	T1199 Доверительные отношения	T1609 Средства администрирования контейнера	T1137 Запуск приложения Office  0/6	T1098 Манипуляции с учетной записью  6/6
T1589 Сбор информации об атакуемых пользователях  3/3	T1608 Размещение средств  ▼	T1195 Компрометация цепочки поставок  2/3	T1204 Выполнение с участием пользователя  3/3	T1542 Загрузка раньше ОС  4/5	T1574 Перехват потока исполнения  11/13
T1591 Сбор бизнес-информации об атакуемой организации  ▼	T1585 Создание учетных записей  ▼	T1078 Существующие учетные записи  4/4	T1569 Системные службы  1/2	T1098 Манипуляции с учетной записью  0/6	T1068 Эксплуатация уязвимостей для повышения привилегий  T1546 Выполнение по событию
	T1650 Приобретение доступа  ▼	T1091 Распространение через съемные носители	T1072 Средства развертывания ПО  ▼	T1574 Перехват потока исполнения	
		T1190 Нестатистика обнаружения			

# 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 киберразведке](#). Руководитель департамента киберразведки 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 рекрутёру.

[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 антифрога 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**

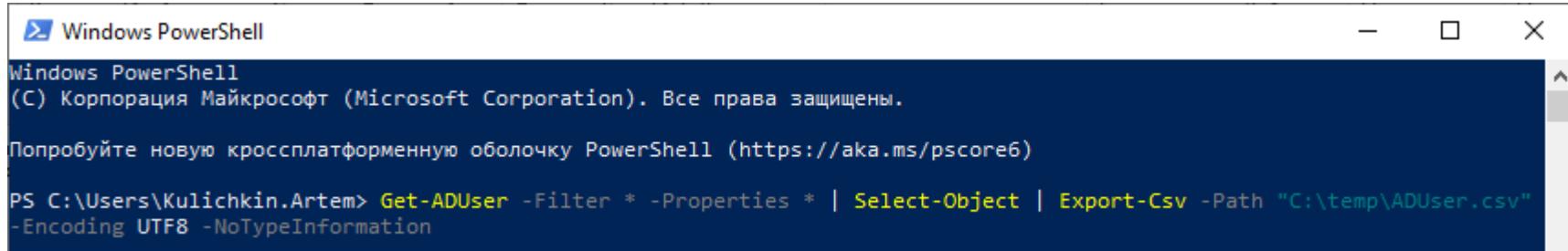
Аудит + доработка AD:

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

# AD

Аудит + доработка AD:

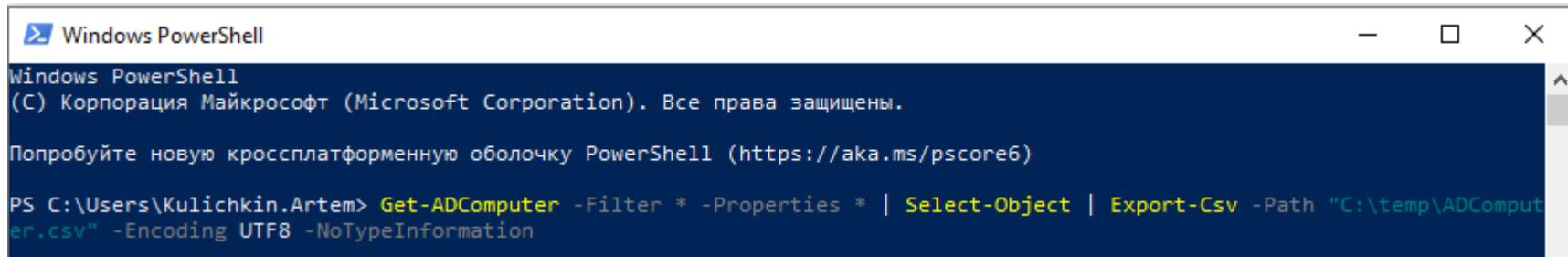
- Учётные записи (Password never expires, last logon)



```
Windows PowerShell
(C) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

Попробуйте новую кроссплатформенную оболочку PowerShell (https://aka.ms/pscore6)

PS C:\Users\Kulichkin.Artem> Get-ADUser -Filter * -Properties * | Select-Object | Export-Csv -Path "C:\temp\ADUser.csv" -Encoding UTF8 -NoTypeInformation
```



```
Windows PowerShell
(C) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

Попробуйте новую кроссплатформенную оболочку PowerShell (https://aka.ms/pscore6)

PS C:\Users\Kulichkin.Artem> Get-ADComputer -Filter * -Properties * | Select-Object | Export-Csv -Path "C:\temp\ADComputer.csv" -Encoding UTF8 -NoTypeInformation
```

[Аудит пользователей AD с помощью Powershell / Хабр](#)



Admin Accounts With SPN

**AD**



**0.22%**

3 Admin Accounts With SPN



Accounts With Passwords That Never Expire

**1,158**  
Users

84% Accounts With Passwords That Never Expire



Accounts With No Password Policy

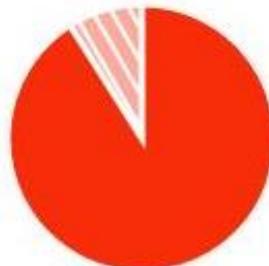


Accounts That Do Not Require Kerberos Pre-Authentication



**0.43%**

6 Accounts That Do Not Require Kerberos Pre-Authentication



**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
```

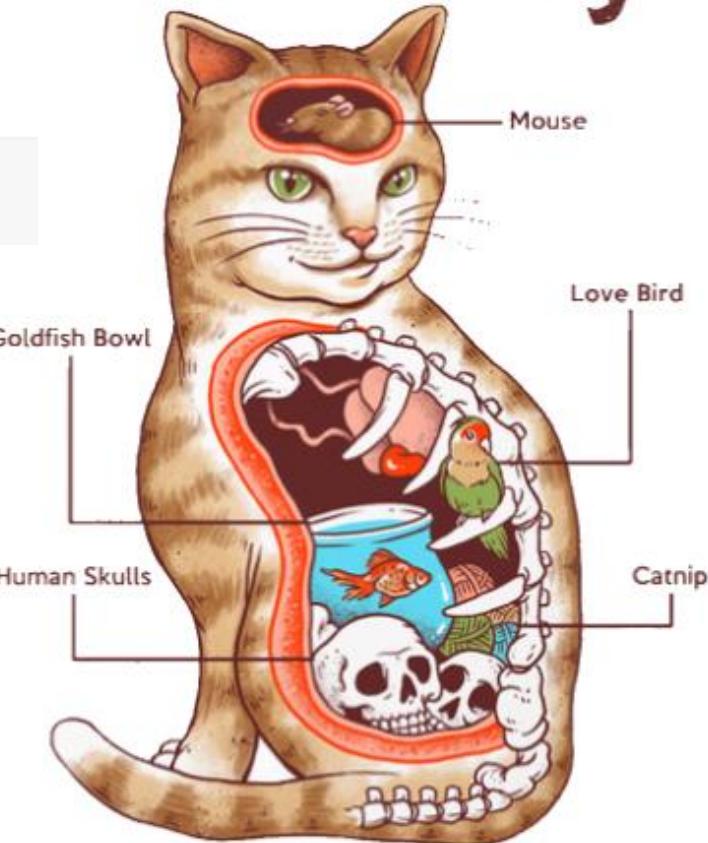
```
hashcat.exe -m 1000 E:\hashs.txt --show
```

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

Поиск хэшей в пот-файле

[Брутфорс хэшей в Active Directory / Хабр](#)

# Anatomy



# AD

Аудит + доработка AD:

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



 Lithnet

## Password Protection for Active Directory

Password93.|

Password93.



Ой! Ваш пароль взломают быстрее, чем вы скажете «Ой!»



Пароль пора срочно менять!

- Плохая новость
- ⚠ Часто используемое слово
- Этот пароль засветился в базах утекших паролей 12 раз.

[Weakpass: biggest wordlists collection](#)

[HashMob | Resources | HashMob Wordlists](#)

[Защита паролем AD — Lithnet](#)

# AD

Аудит + доработка AD:

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

Y	Z	AA	AB
Enabled	LastLogonDate	HomePage	instanceType
True	22.02.2024 1:	Сортировка от старых к новым	
True	11.03.2024 20:	Сортировка от новых к старым	
True	08.03.2024 3:	Сортировка по цвету	
True	07.03.2024 3:	Удалить фильтр из столбца "LastLogonDate"	
True	06.03.2024 9:	Фильтр по цвету	
True	10.03.2024 7:	Фильтры по дате	
True	04.03.2024 20:		
True	08.03.2024 1:		
True	11.03.2024 22:		
True	06.03.2024 15:		
True	04.03.2024 19:		
True	09.03.2024 0:		
True	08.03.2024 23:		
True	06.03.2024 16:		
True	13.11.2023 18:		

Было

Y	Z
Enabled	LastLogonDate
veDi True	17.07.2009 17:15
veDi True	19.04.2011 22:05
veDi True	22.05.2012 15:04
veDi True	13.02.2013 8:17
veDi True	11.03.2014 12:36
veDi True	25.06.2014 9:30
veDi True	24.08.2014 13:24
veDi True	07.09.2014 12:10
veDi True	09.03.2016 9:15
veDi True	15.04.2016 14:22
veDi True	20.07.2016 17:51
veDi True	15.08.2016 15:59
veDi True	12.09.2016 15:19
veDi True	16.09.2016 17:27
veDi True	24.09.2016 16:06
veDi True	26.09.2016 15:39
veDi True	21.10.2016 10:38
veDi True	01.11.2016 15:40
veDi True	14.11.2016 16:04
veDi True	23.11.2016 13:16
veDi True	18.01.2017 21:25

Y	Z	AA	AB
Enabled	LastLogonDate	HomePage	instanceType
ion	True	12.10.2023 7:	Сортировка от старых к новым
ion	True	03.10.2023 2:	Сортировка от новых к старым
ion	True	09.10.2023 13:	Сортировка по цвету
ion	True	08.10.2023 10:	Удалить фильтр из столбца "LastLogonDate"
ion	True	07.10.2023 15:	Фильтр по цвету
ion	True	05.10.2023 17:	Фильтры по дате
ion	True	06.10.2023 4:	Область поиска: (Все)
ion	True	08.10.2023 9:	<input checked="" type="checkbox"/> Выделить все
ion	True	05.10.2023 18:	<input checked="" type="checkbox"/> 2023
ion	True	08.10.2023 17:	<input checked="" type="checkbox"/> Август
ion	True	10.10.2023 18:	<input checked="" type="checkbox"/> Сентябрь
ion	True	08.10.2023 11:	<input checked="" type="checkbox"/> Октябрь
ion	True	04.10.2023 14:	
ion	True	03.10.2023 11:	
ion	True	08.10.2023 11:	
ion	True	09.10.2023 10:	

Стало

# AD

Аудит + доработка AD:

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



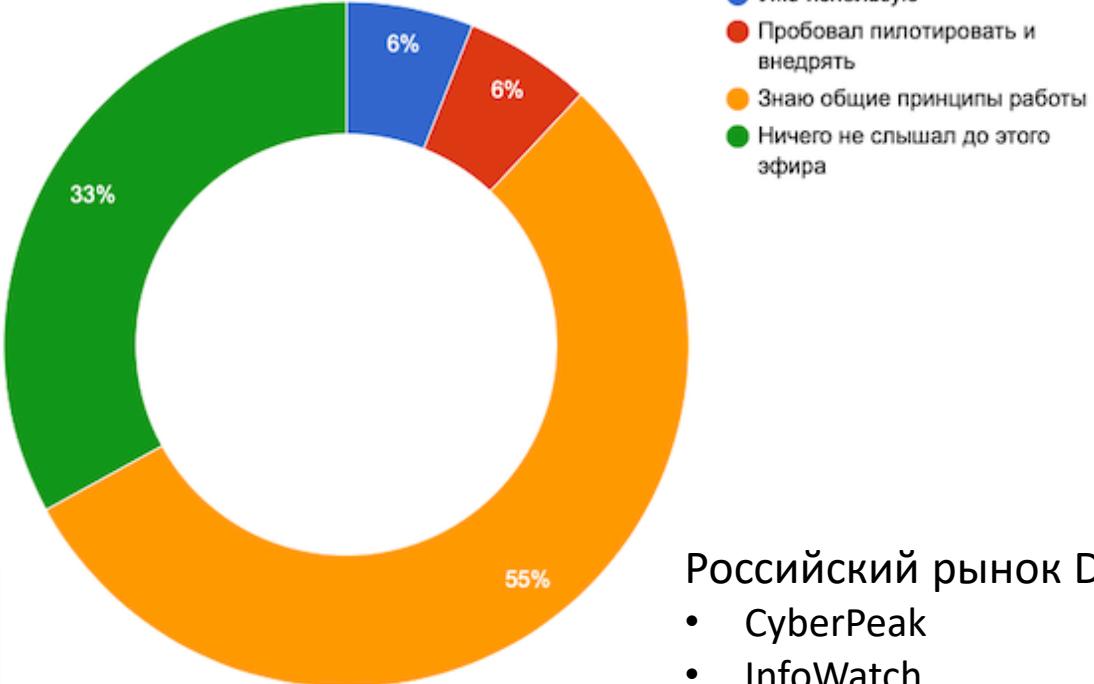
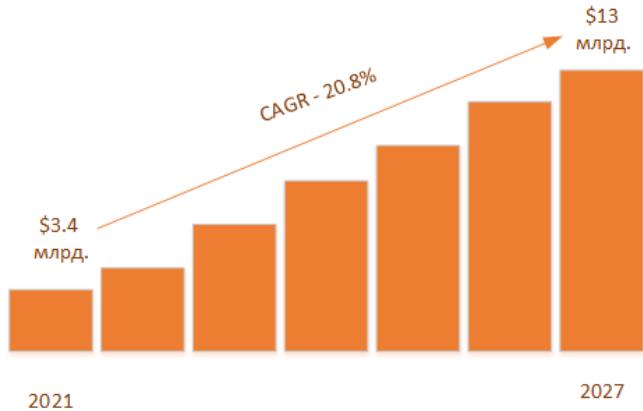
Компьютер	Путь	Применяется к	Пользователь/группа	Состояние наследования	Права объекта	Права родителя
ts.sus.local	\\\ts.sus.local\	Для этой папки, ее поди	пользователи@builtin	✓ Наследуется	F M X W R L S	F M X W R L S
ts.sus.local	\\\ts.sus.local\	Для этой папки, ее поди	пользователи@builtin	✗ Права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

Рисунок 1. Насколько хорошо вы знакомы с решениями DCAP?

# AD

Аудит + доработка AD:

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



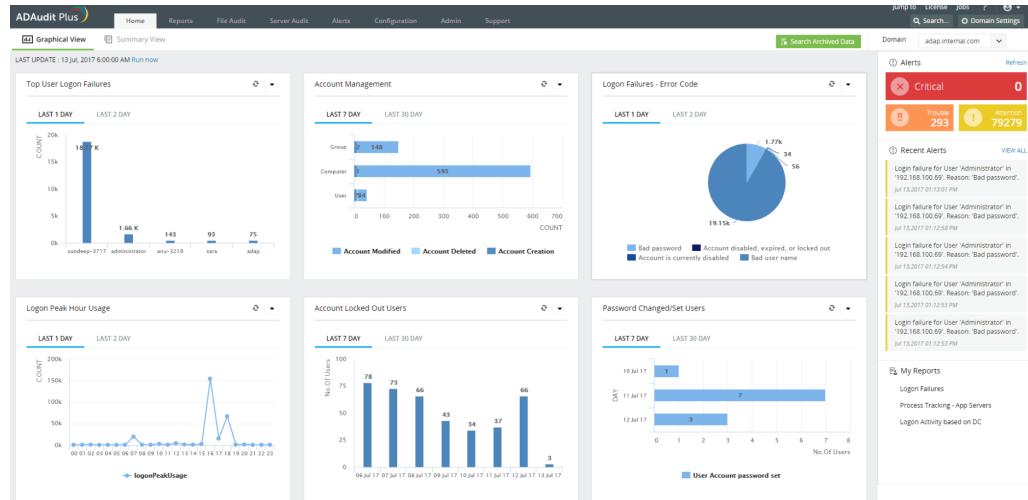
## Российский рынок DCAP

- 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

ADAudit Plus

Home Reports File Audit Server Audit Alerts Configuration Admin Support

Jump to License Jobs ?

Search... Domain Settings

LAST UPDATE : 13 Jul, 2017 6:00:00 AM Run now

Graphical View Summary View

Search Archived Data

Domain adap.internal.com

Alerts

Critical Trouble 293 Attention 79279

Recent Alerts

Login failure for User 'Administrator' in '192.168.100.69'. Reason: 'Bad password'.  
Jul 13,2017 01:13:01 PM

Login failure for User 'Administrator' in '192.168.100.69'. Reason: 'Bad password'.  
Jul 13,2017 01:12:58 PM

Login failure for User 'Administrator' in '192.168.100.69'. Reason: 'Bad password'.  
Jul 13,2017 01:12:54 PM

Login failure for User 'Administrator' in '192.168.100.69'. Reason: 'Bad password'.  
Jul 13,2017 01:12:53 PM

My Reports

Logon Failures Process Tracking - App Servers Logon Activity based on DC

### Top User Logon Failures

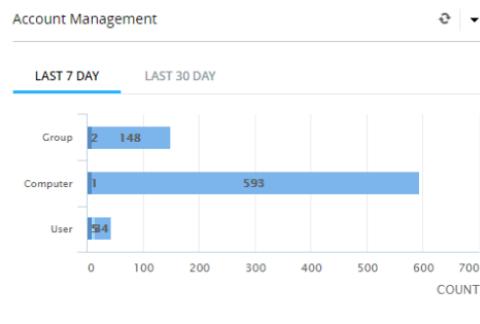
LAST 1 DAY LAST 2 DAY



User	COUNT
sundeepl-3717	18.77 K
administrator	1.66 K
anu-3219	143
sara	93
adap	75

### Account Management

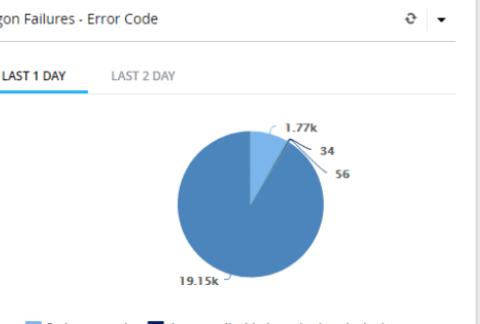
LAST 7 DAY LAST 30 DAY



Category	Account Modified	Account Deleted	Account Creation
Group	2	148	
Computer	1		593
User	54		

### Logon Failures - Error Code

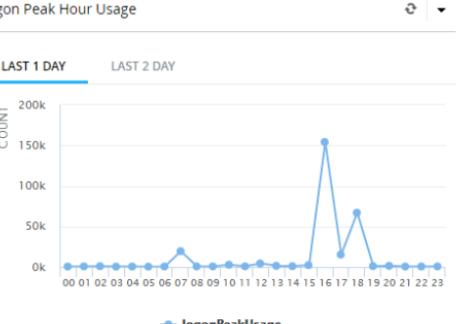
LAST 1 DAY LAST 2 DAY



Error Code	COUNT
Bad password	1.77k
Account disabled, expired, or locked out	34
Account is currently disabled	56
Bad user name	19.15k

### Logon Peak Hour Usage

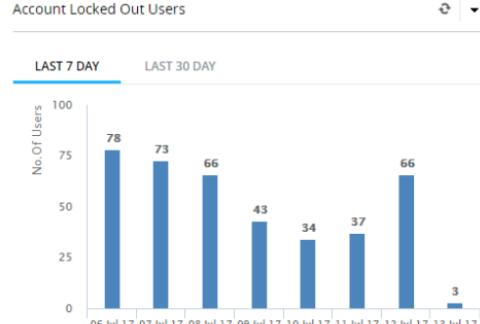
LAST 1 DAY LAST 2 DAY



Hour	COUNT
00	~10k
01	~10k
02	~10k
03	~10k
04	~10k
05	~10k
06	~10k
07	~10k
08	~10k
09	~10k
10	~10k
11	~10k
12	~10k
13	~10k
14	~10k
15	~150k
16	~20k
17	~10k
18	~50k
19	~10k
20	~10k
21	~10k
22	~10k
23	~10k

### Account Locked Out Users

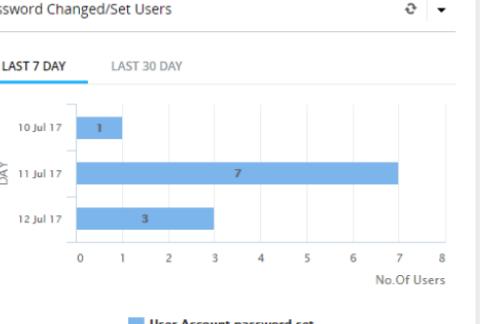
LAST 7 DAY LAST 30 DAY



Date	No. Of Users
06 Jul 17	78
07 Jul 17	73
08 Jul 17	66
09 Jul 17	43
10 Jul 17	34
11 Jul 17	37
12 Jul 17	66
13 Jul 17	3

### Password Changed/Set Users

LAST 7 DAY LAST 30 DAY



Day	No. Of Users
10 Jul 17	1
11 Jul 17	7
12 Jul 17	3

# Анализ инфраструктуры

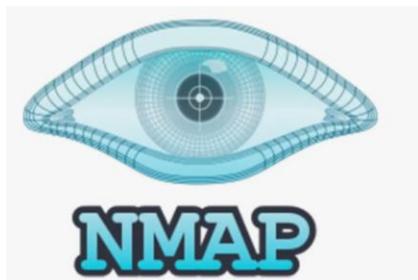
Аудит + доработка инфраструктуры:

- 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)



# Анализ инфраструктуры

Аудит + доработка инфраструктуры:

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

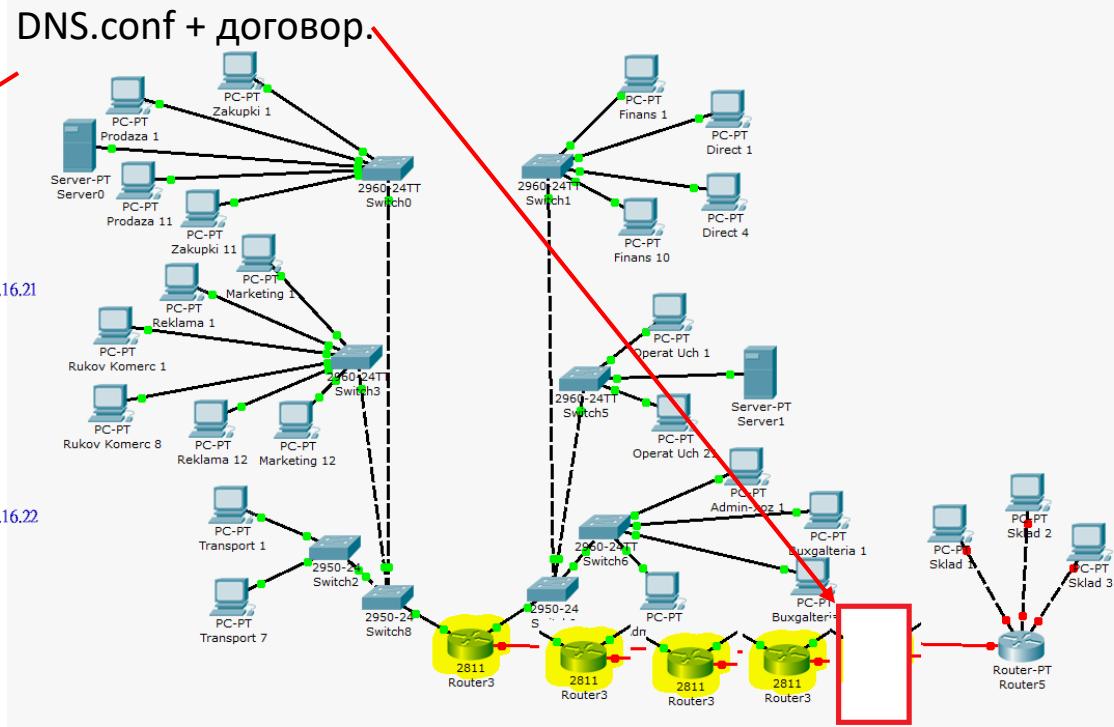
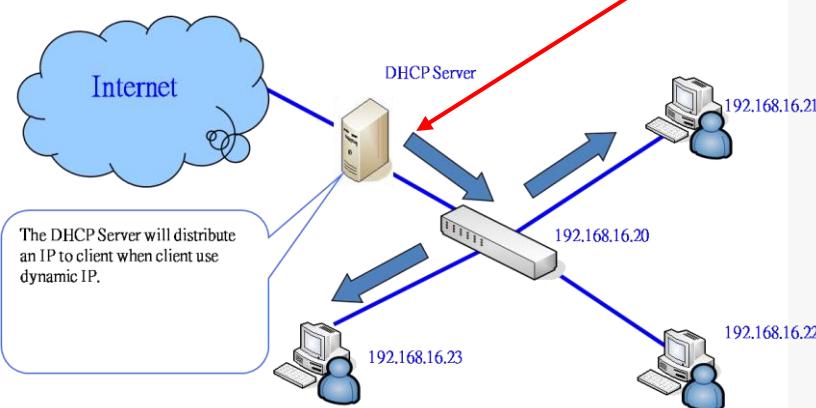
10.22.11.18	FLEET	
10.22.11.18	PORT	21/ftp/vsftpd/2.0.5/cpe:/a:vsftpd:vsftpd:2.0.5   21/
10.22.11.18	PORT	23/telnet/Linux telnetd//cpe:/o:linux:linux_kernel   23/
10.22.11.18	PORT	80/http/mini_httpd/1.19 19dec2003/cpe:/a:acme:mini_httpd:1.19_19dec2003   80/{"http-server-header": "mini_httpd/1.19 19dec2003", "http-title": "Site doesn't have a certificate"}
10.22.11.18	PORT	427/svrlloc///   427/
10.22.11.18	PORT	1720/h323g931///   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/ <a href="#">Web-Based Enterprise Management CIM serverOpenPegasus WBEM</a> http://cpe:/o:linux:linux_kernel   5988/{"http-title": "Site doesn't have a certificate"}
10.22.11.18	KSC	
10.22.11.18	FLEET	
10.0.55.112	□+IT	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/h323g931///   1720/
10.0.55.112	PORT	1947/sentinelrm///   1947/{"fingerprint-strings": "\n FourOhFourRequest: \n HTTP/1.0 403 Forbidden\n Server: HASP LM/24.00\n Date: Sat, 02 Nov 2018 10:22:00 GMT"}
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\\N"}
10.0.55.112	PORT	5040/unknown///   5040/
10.0.55.112	PORT	5357/http/Microsoft HTTPAPI http/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 http/2.0/cpe:/o:microsoft:windows   8005/{"http-title": "Bad Request"}
10.0.55.112	PORT	47001/http/Microsoft HTTPAPI http/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/

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

# Анализ инфраструктуры

Аудит + доработка инфраструктуры:

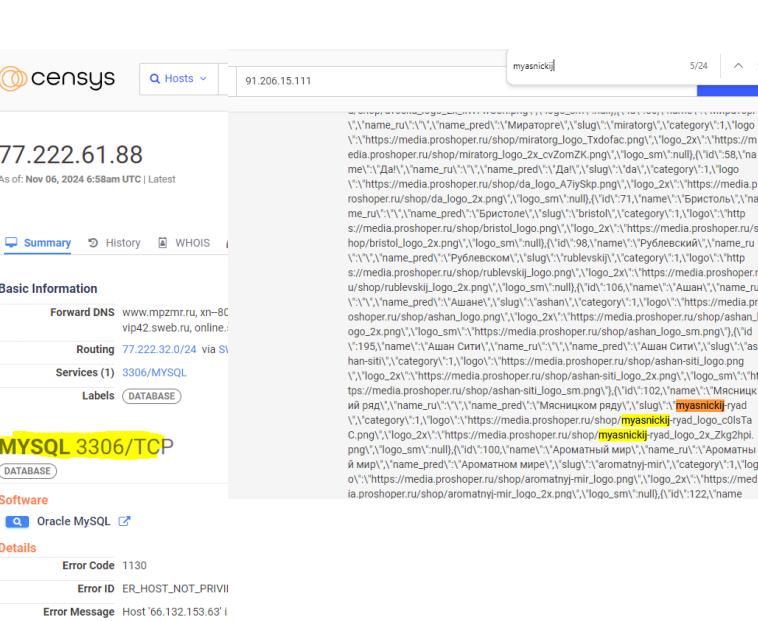
- Аудит всех хостов в сети (Masscan + Nmap)
- Аудит всех портов в сети
- **Аудит того, что торчит в интернет**

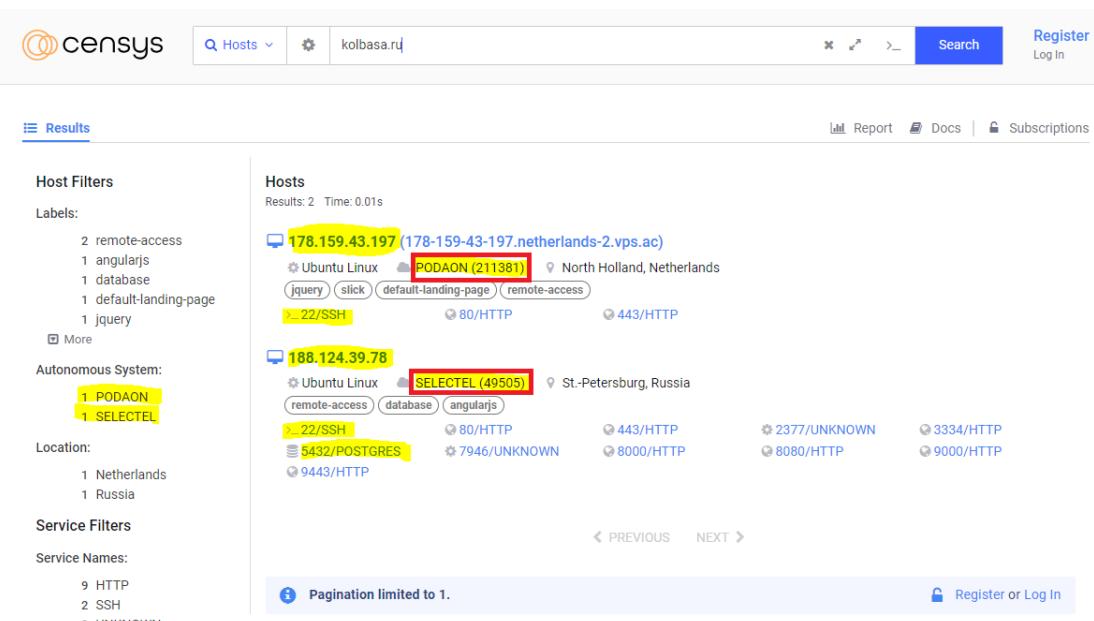


# Анализ инфраструктуры

Аудит + доработка инфраструктуры:

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

A screenshot of the Censys web interface. At the top, there's a search bar with 'myasnicki' and a dropdown menu for 'Hosts'. Below it, a table shows a single host entry: '91.206.15.111' with a status of 'Up' and '5/24' ports scanned. The main pane displays detailed information about this host, including its IP address (77.222.61.88), last seen on Nov 06, 2024 at 6:58am UTC, and a 'Latest' timestamp. It includes sections for 'Summary', 'History', 'WHOIS', 'Basic Information', 'Forward DNS' (mpzmr.ru, xn--8Cvip2.sweb.ru, online.), 'Routing' (77.222.32.0/24 via SI), 'Services (1) 3306/MySQL', and 'Labels' (DATABASE). A large yellow box highlights the 'MySQL 3306/TCP' service. The bottom section shows 'Software' (Oracle MySQL) and 'Details' (Error Code: 1130, Error ID: ER\_HOST\_NOT\_PRIVILEGED, Error Message: Host '66.132.153.63'!).

A screenshot of the Censys search results page for 'myasnicki'. The search bar has 'myasnicki' and 'kolbasa.ru' entered. The results table shows two entries: '178.159.43.197 (178-159-43-197.netherlands-2.vps.ac)' and '188.124.39.78 (188-124-39-78.st-petersburg-1.vps.ac)'. Both hosts are running Ubuntu Linux. The first host is associated with 'PODAON (211381)' and the second with 'SELECTEL (49505)'. They both have open ports 22/SSH, 80/HTTP, and 443/HTTP. Other services listed include 5432/POSTGRES and 9443/HTTP. The results table includes columns for 'Hosts' (2), 'Time' (0.01s), and various service details like 'remote-access', 'angularjs', 'database', etc.

# 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

https://kolbasa.ru/bitrix/admin/#authorize

kolbasa.ru

## Авторизация

Пожалуйста, авторизуйтесь

### Логин

Пароль

Запомнить меня на этом компьютере

Забыли свой пароль?

или войдите через

Битрикс24

1С-Битрикс: Управление сайтом 22.0.300. © Битрикс, 2002-2022

https://bdu.fstec.ru/vul/2023-05857

Банк данных угроз безо

Федеральная служба по техническому и экспортному контролю  
ФСТЭК России

Угрозы Уязвимости Тестирование оснований Документы Обратная связь Обновления Участники Обучение

Главная / Список уязвимостей / BDU:2023-05857

**BDU:2023-05857: Уязвимость модуля landing системы управления содержимым сайтов (CMS) 1С-Битрикс: Управление сайтом**

нарушителю выполнить команды ОС на уязвимом узле, получить контроль над ресурсами и проникнуть во внутреннюю сеть

**Описание уязвимости** Уязвимость модуля landing системы управления содержимым сайтов (CMS) 1С-Битрикс: Управление сайтом вызвана эксплуатацией уязвимости может позволить нарушителю, действующему удалённо, выполнить команды ОС на уязвимом узле

**Вендор** ООО «1С-Битрикс»

**Наименование ПО** 1С-Битрикс: Управление сайтом (запись в едином реестре российских программ №35)

**Версия ПО** до 23.850.0 (1С-Битрикс: Управление сайтом)

**Тип ПО** Прикладное ПО информационных систем

**Уровень опасности уязвимости** Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10)

**Дата выявления** 13.09.2023

**Идентификатор типа** CWE-362

Subject Name	
Country	RU
State/Province	Moscow Oblast
Locality	Odintsovo
Organization	ООО Mpz Myasnitskiy Ryad
Common Name	*.kolbasa.ru
Issuer Name	
Country	BE
Organization	GlobalSign nv-sa
Common Name	GlobalSign RSA OV SSL CA 2018
Validity	
Not Before	Mon, 22 Jan 2024 08:58:39 GMT
Not After	Sat, 22 Feb 2025 08:58:38 GMT
Subject Alt Names	
DNS Name	*.kolbasa.ru
DNS Name	kolbasa.ru

# 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**



AnyDesk



TeamViewer



Chrome  
Remote  
Desktop



TightVNC



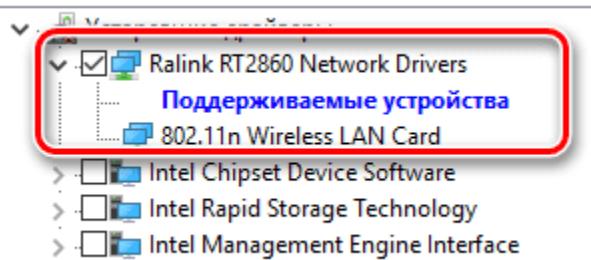
Virtual  
Network  
Computing



UltraVNC



H



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

RAIDX

Kraftway Terminal Linux

WTware

KasperskyOS

OCPB «МАКС»

Учетные системы

Складские системы

Логистическое ПО

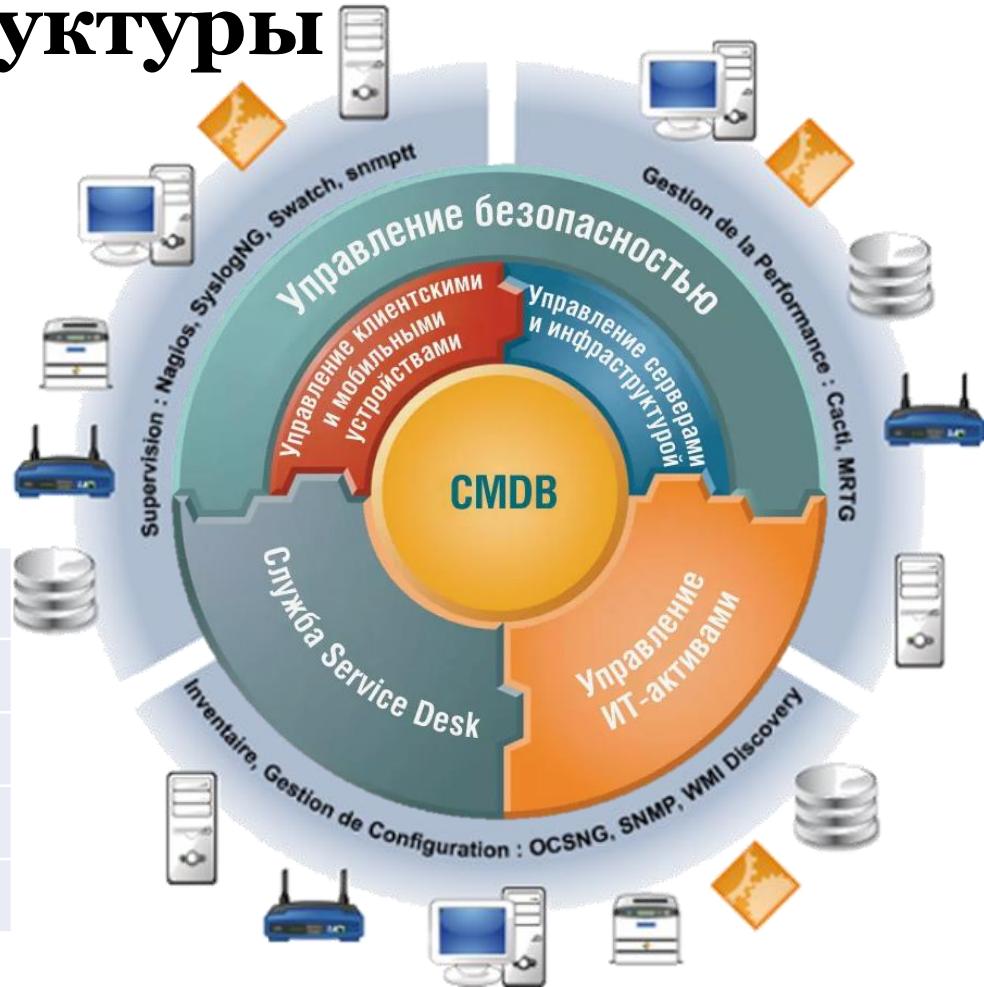
Склад-15

# 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	<a href="https://ShowObject.jspa?id=92004">https://ShowObject.jspa?id=92004</a>	Игорь Игоревич Игорев
90.90.48.39	G-0000-5202	<a href="https://ShowObject.jspa?id=92699">https://ShowObject.jspa?id=92699</a>	Игорь Игоревич Игорев
90.86.4.2	G2800-SQ01	<a href="https://ShowObject.jspa?id=99942">https://ShowObject.jspa?id=99942</a>	Иванов Иван Иванович
90.46.0.57	G6400-DP01	<a href="https://ShowObject.jspa?id=92969">https://ShowObject.jspa?id=92969</a>	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)**

## ZABBIX



Network and server infrastructure



Cloud deployments



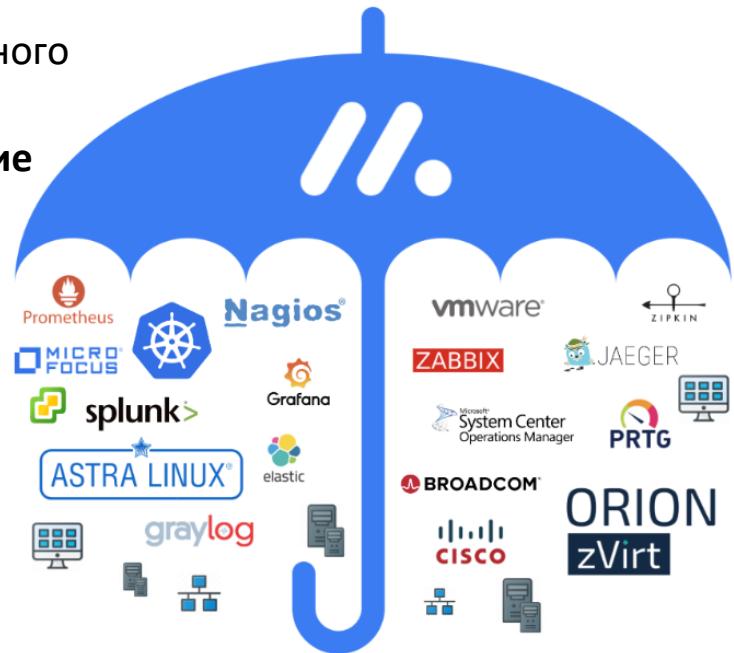
APIs and websites



Services and applications



IOT devices and sensors



# 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:

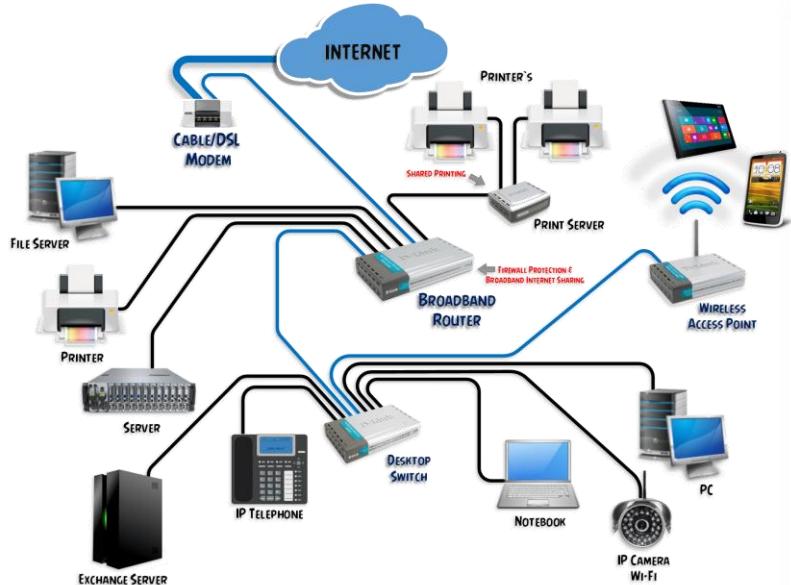
- Ограничение физического доступа к инфраструктуре.



# 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

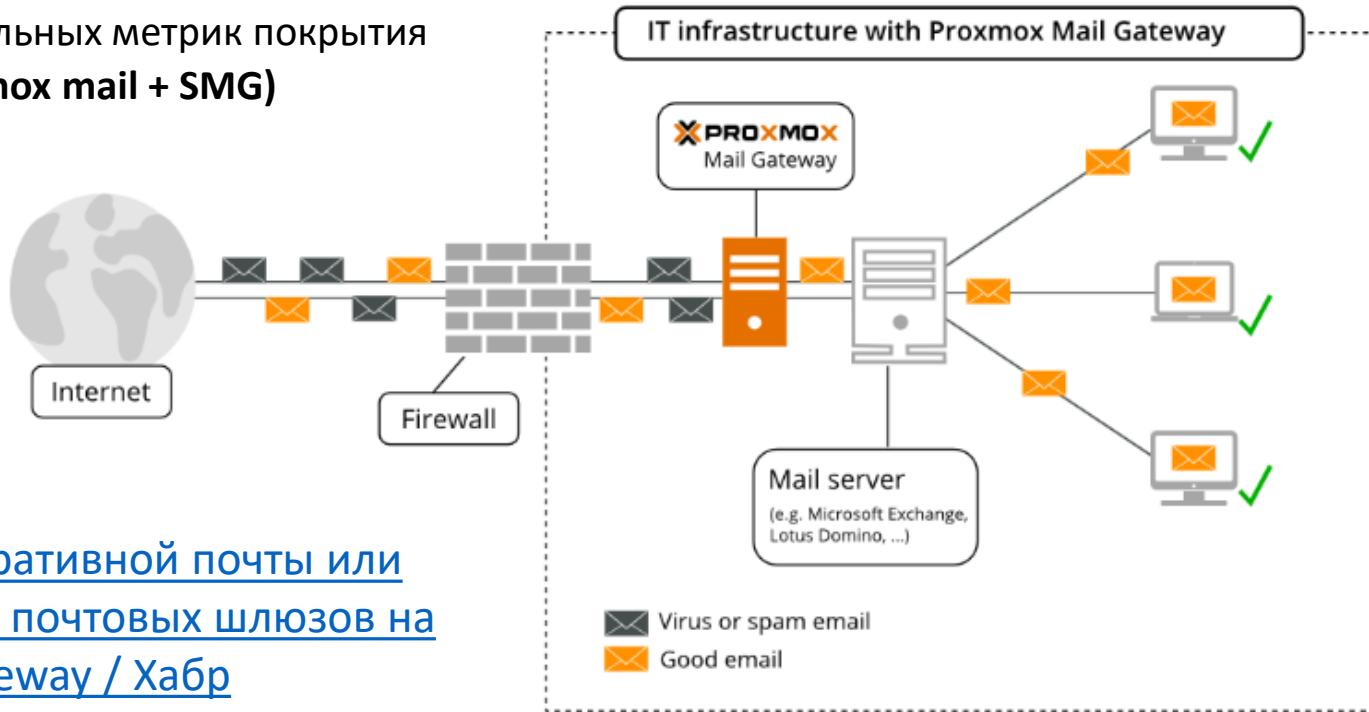
АВЗ EDR SOC IDS DLP ...

	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)**

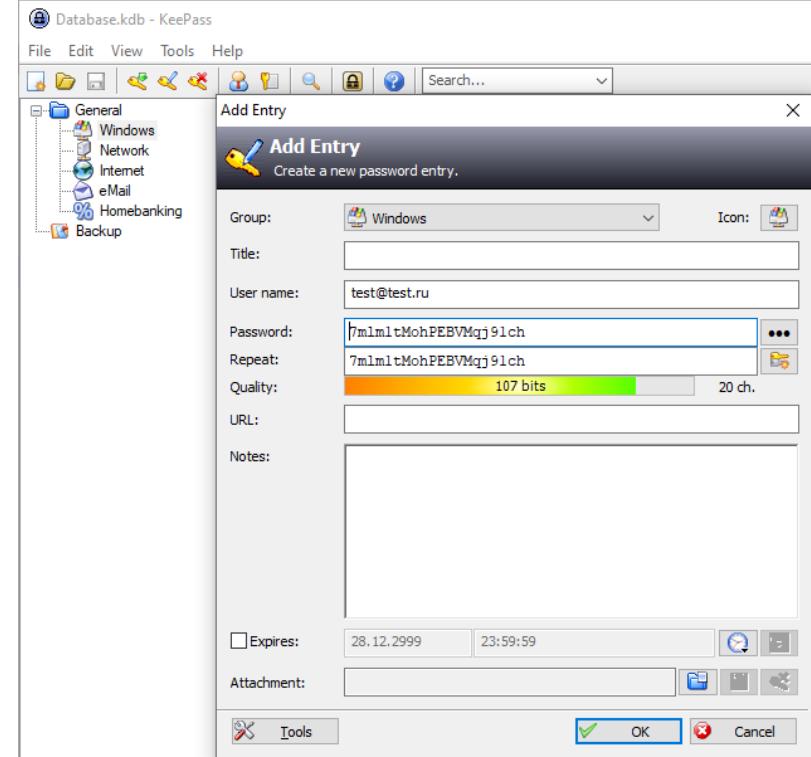


ЧудESA защиты корпоративной почты или  
внедрение свободных почтовых шлюзов на  
базе Proxmox Mail Gateway / Хабр

# Начальные телодвижения

Установка, настройка, доработка:

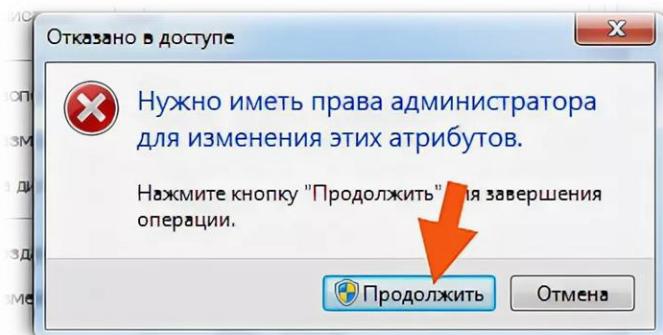
- Ограничение физического доступа к инфраструктуре.
- Покрытие СЗИ всех возможных устройств
- Выстраивание правильных метрик покрытия
- Защита почты (Proxmox mail + SMG)
- **Менеджеры паролей**



# Начальные телодвижения

Установка, настройка, доработка:

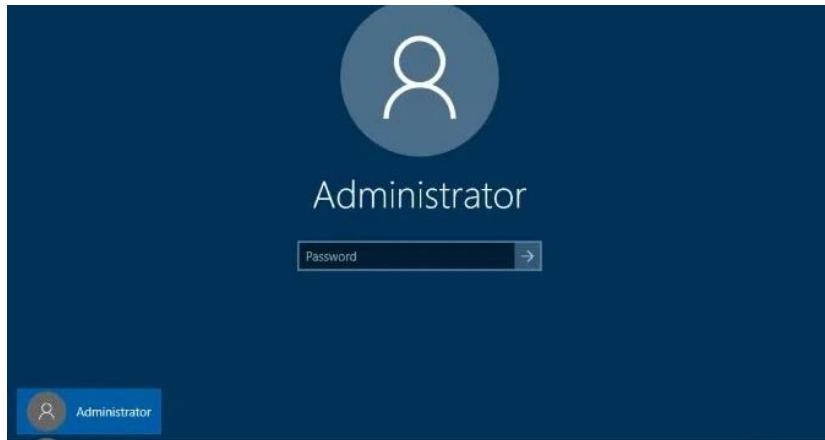
- Ограничение физического доступа к инфраструктуре.
- Покрытие СЗИ всех возможных устройств
- Выстраивание правильных метрик покрытия
- Защита почты (Proxmox mail + SMG)
- Менеджеры паролей
- **Минимальные права у юзера**



# 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**

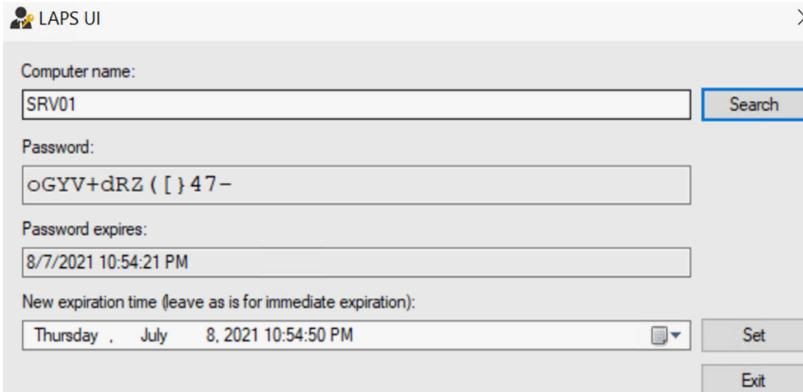


[\[конспект админа\]](#) [Меньше](#)  
[администраторов всем / Хабр](#)

# 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)**



[Управляем паролем локального администратора с помощью LAPS / Хабр](#)

# Начальные телодвижения

Установка, настройка, доработка:

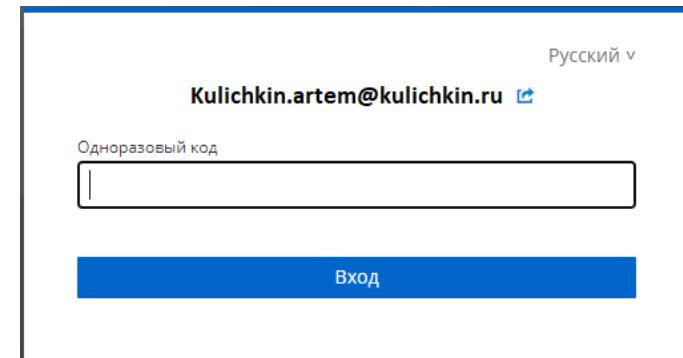
- Ограничение физического доступа к инфраструктуре.
- Покрытие СЗИ всех возможных устройств
- Выстраивание правильных метрик покрытия
- Защита почты (Proxmox mail + SMG)
- Менеджеры паролей
- Минимальные права у юзера
- Запрет работать из под администратора администраторам
- Внедрение Local Administrator 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 менеджмент, обновление ОС, ПО.
- Бекап и восстановление + проверка.
- Запретить вход через рут по ssh

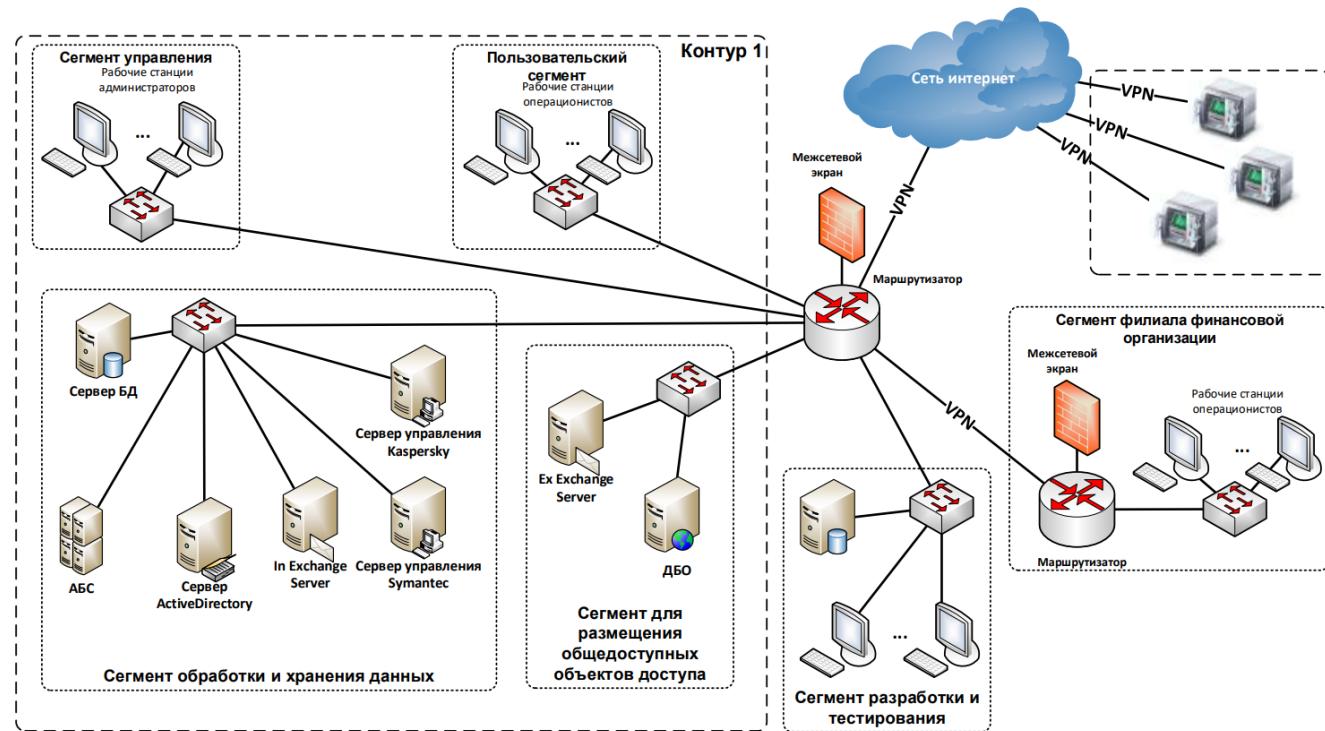
*Прописать в ОРД спина болеть не будет*

# Администрирование

Установка, настройка, доработка:

- Администрирование только из специального сегмента с отдельными учётками и правами

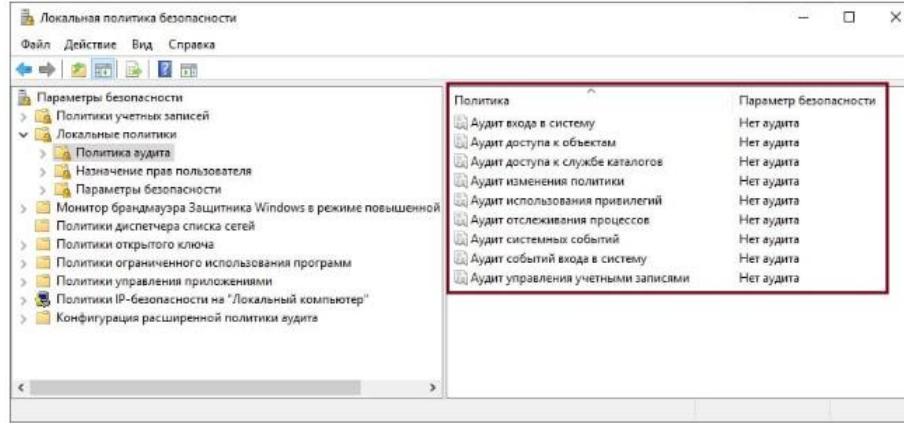
- ✓ Сегментирование сети
- ✓ Разделять прод, тест, деф.
- ✓ Запретить выход в интернет из серверного сегмента
- ✓ Выход в интернет через единый прокси с авторизацией



# 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:

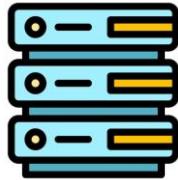
- Администрирование только из специального сегмента с отдельными учётками и правами
- Включить расширенный аудит eventlog, Symon, auditd.
- Менеджер паролей KeePass
- Минимальные права доступа
- **Tier 0, Tier 1, Tier 2, Tier 3**

**Tier 0**



Active Directory

**Tier 1**



**Tier 2**



**Tier 3**

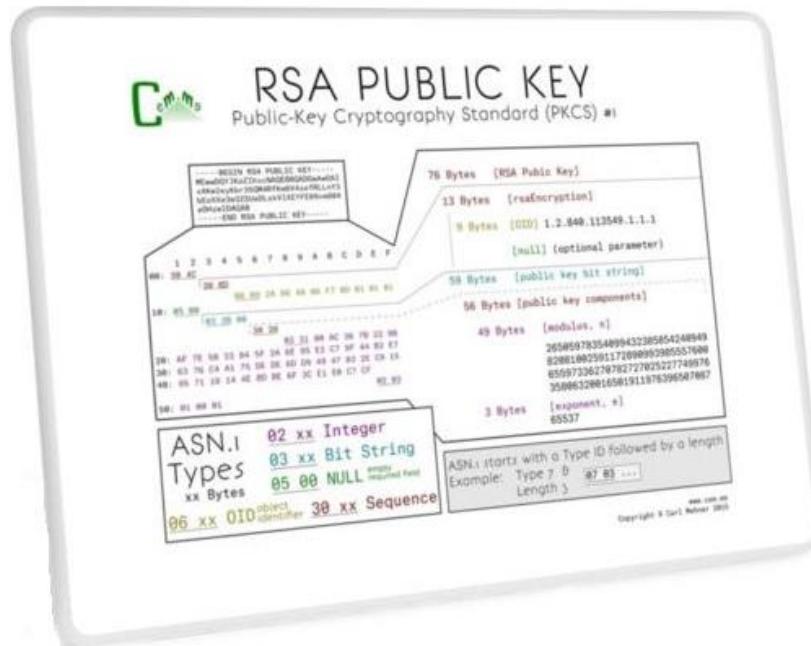


[Многоуровневая модель  
среды PAM | Microsoft  
Learn](#)

# 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 менеджмент**



# 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 менеджмент
- 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 менеджмент
- 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 менеджмент
- Бекап и восстановление + проверка.
- Запретить вход через рут по ssh

*Прописать в ОРД спина болеть не будет*

# Немного допов

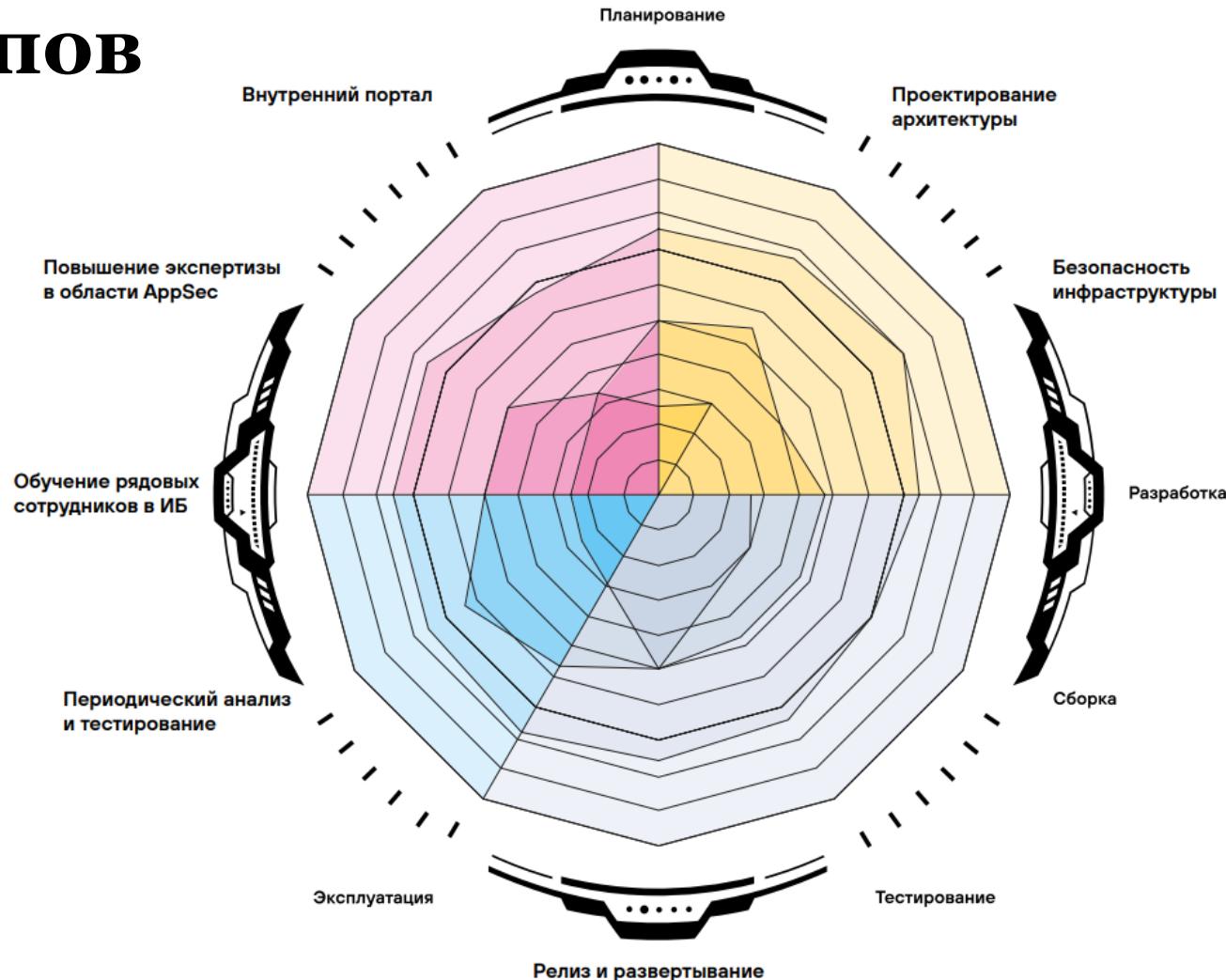
Установка, настройка, доработка:

- 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, эниран.
- 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.