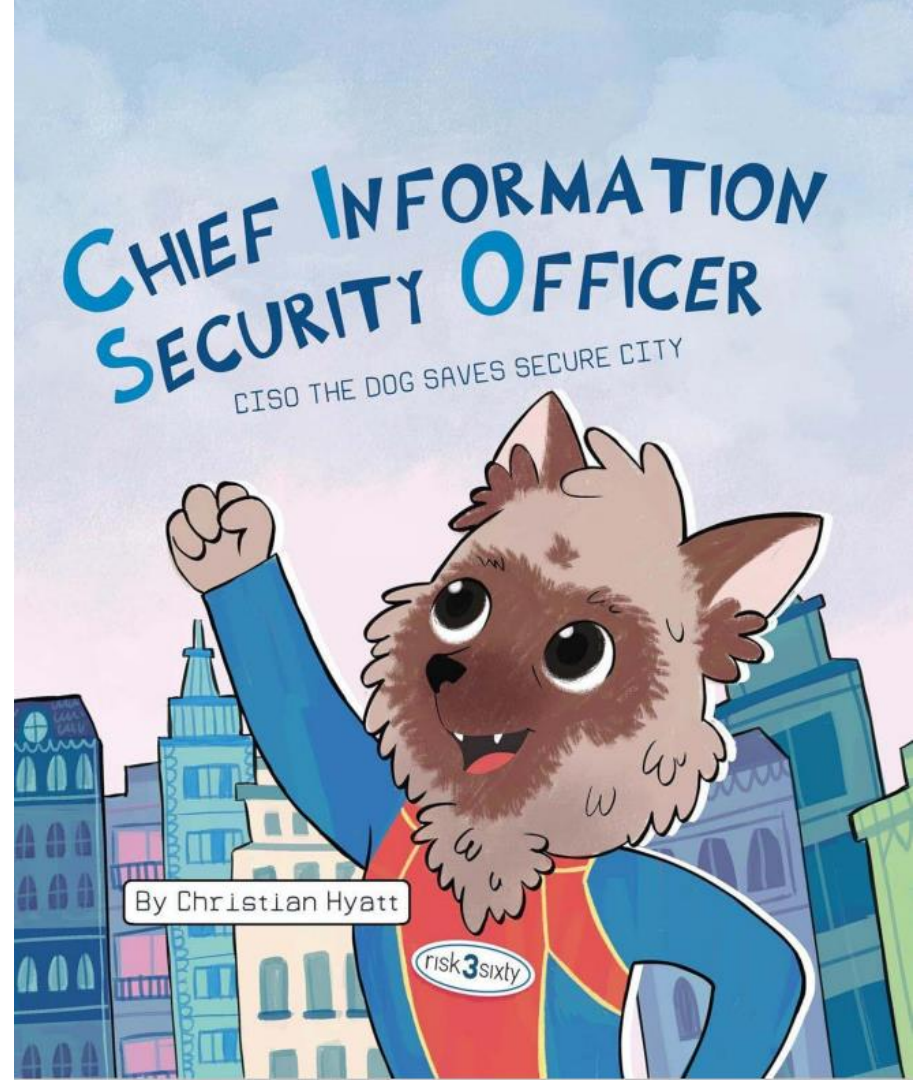


Первые шаги в ИБ

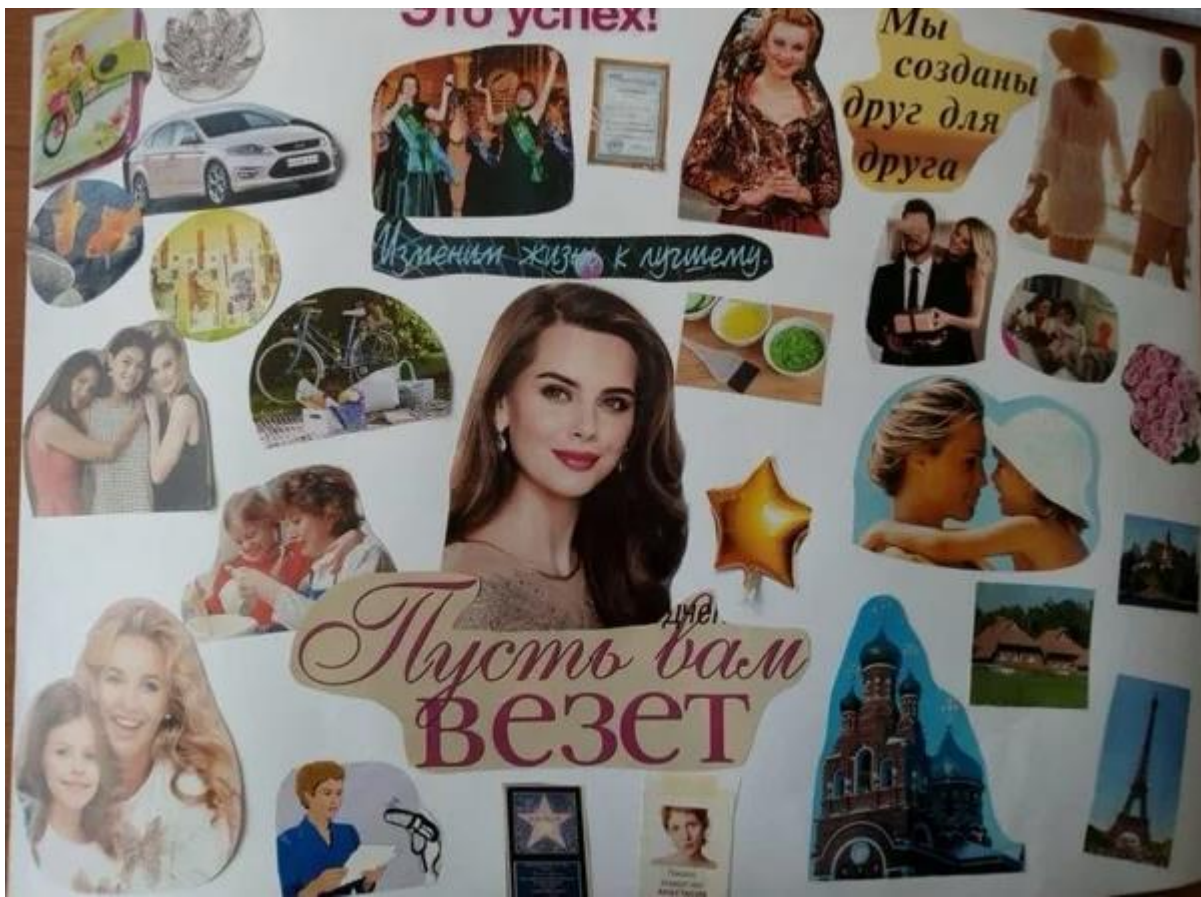


Куличкин Артём Александрович

CISO, CISM, CISA, CEH, CND.



Карьерная карта желаний



Введение

Связиста замечают только тогда, когда пропадает связь.



Топ 3 профессий в сфере И

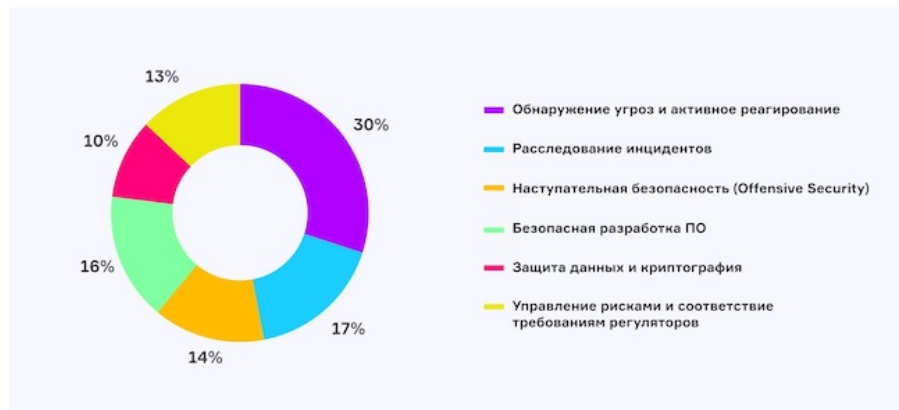
- «Аналитик SOC, инженер информационной безопасности, пентестер».
- «Форензика, безопасность разработки, управление в области ИБ».
- «Кроме внедрения СЗИ, безопасной разработки и форензики стоит посмотреть в сторону безопасности ИИ».

«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?



Это база

Что такое кибербезопасность?


Что такое кибербезопасность?

Кибербезопасность – это способность информационных систем и сетей противостоять и восстанавливаться от вредоносных действий злоумышленников, а также обеспечивать конфиденциальность, целостность и доступность информации.

- обеспечение информационной безопасности;
- защита информации;
- обеспечение безопасности информации в сети информационных ресурсов;
- защита информационных ресурсов с целью их правильного использования.

Объекты кибербезопасности – информационно-кибернетические системы:

- компьютерные системы;
- информационно-телекоммуникационные сети;
- средства обеспечения функционирования ИС/ИТКС.

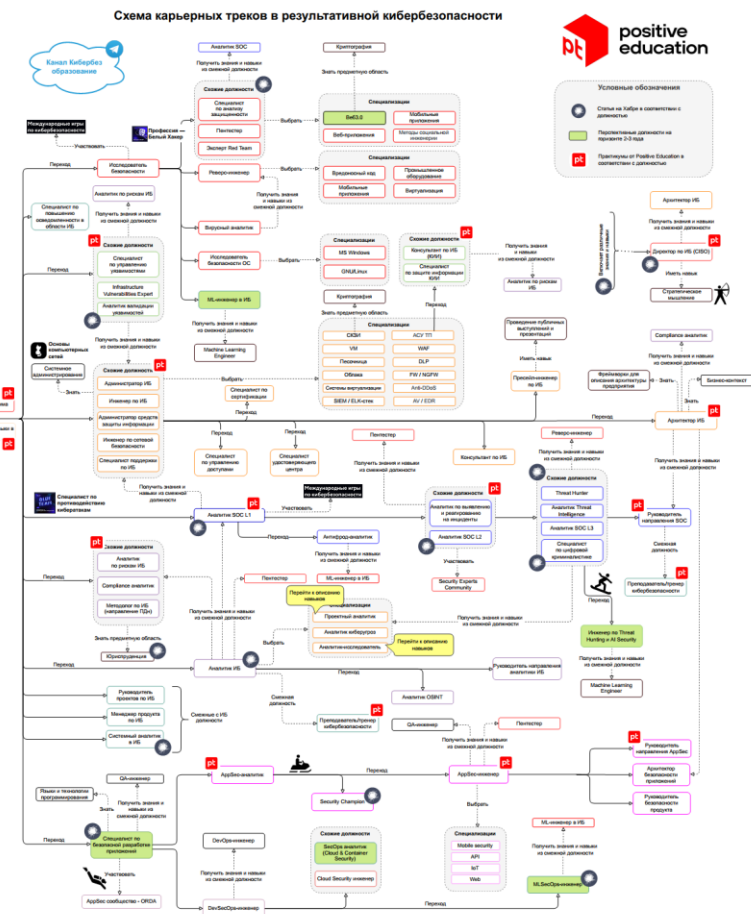


Министерство
Внутренних
Дел
Республики
Казахстан

Определить
пути развития

Спортивная программа

Базовые знания и навыки
координаторов



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

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 навыки 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 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 Тошаков 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

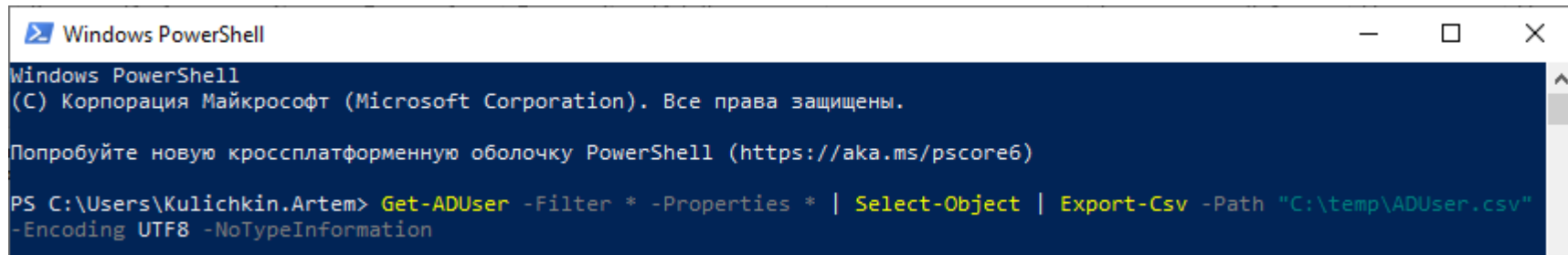
Аудит + доработка AD:

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

AD

Аудит + доработка AD:

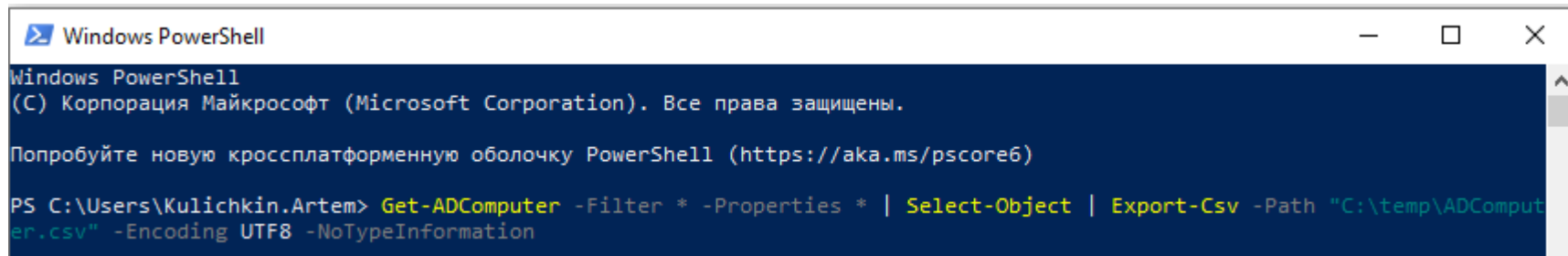
- **Учётные записи** (Password ,Password never expires, last logon)



```
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 -NoTypeInfoInformation
```



```
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 -NoTypeInfoInformation
```

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



AD

Admin Accounts With SPN



0.22%

3 Admin Accounts With SPN



Accounts With Passwords That Never Expire

1,158

Users

84% Accounts With Passwords That Never Expire



Accounts That Do Not Require Kerberos Pre-Authentication

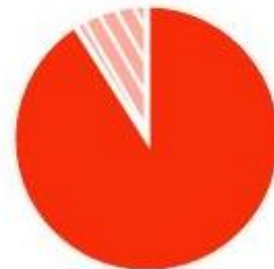


0.43%

6 Accounts That Do Not Require Kerberos Pre-Authentication



Accounts With No Password Policy



91%

1,255 Accounts With No Password Policy

AD

Аудит + доработка AD:

- Учётные записи
- Брут паролей

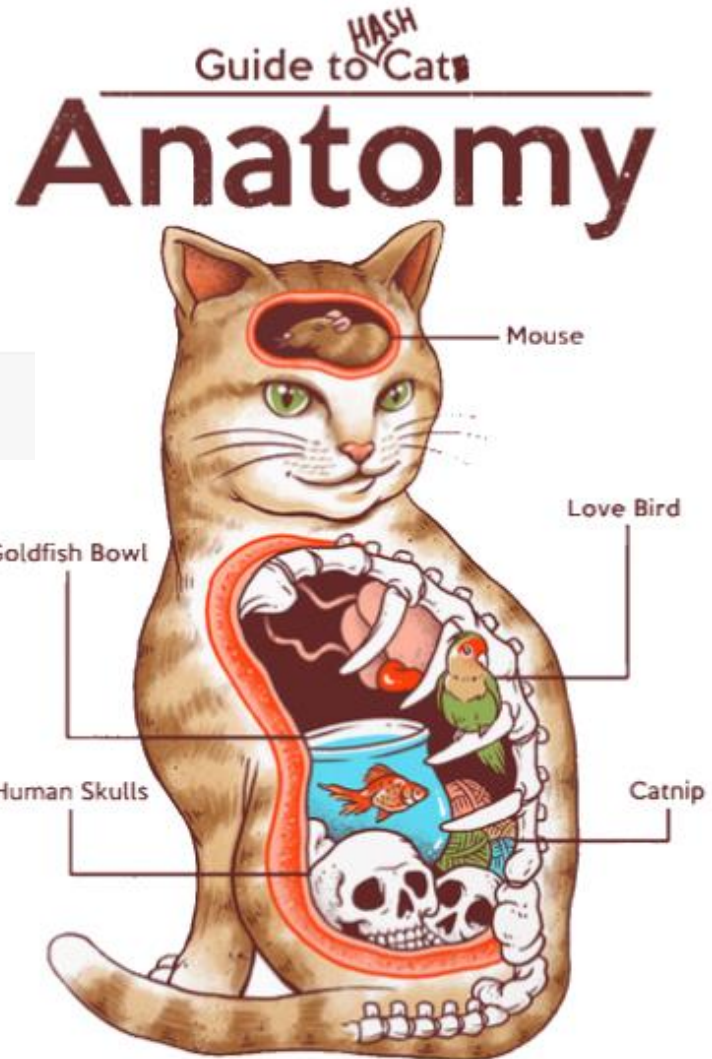
```
secretsdump.exe deiteriy.local/Administrator@192.168.88.32 -just-dc-ntlm
```

```
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**



 Lithnet

Password Protection for Active Directory

Password93.]


Password93. 

ооPS!

Ой! Ваш пароль взламывают 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:	Область поиска: (Все)	
True	08.03.2024 1:	<input checked="" type="checkbox"/> 2019	
True	11.03.2024 22:	<input checked="" type="checkbox"/> 2018	
True	06.03.2024 15:	<input checked="" type="checkbox"/> 2017	
True	04.03.2024 19:	<input checked="" type="checkbox"/> 2016	
True	09.03.2024 0:	<input checked="" type="checkbox"/> 2014	
True	08.03.2024 23:	<input checked="" type="checkbox"/> 2013	
True	06.03.2024 16:	<input checked="" type="checkbox"/> 2012	
True	13.11.2023 18:	<input checked="" type="checkbox"/> 2011	
		<input checked="" type="checkbox"/> 2009	
		<input checked="" type="checkbox"/> (Пустые)	

Показаны не все элементы

OK Отмена

Было

	Y	Z
at	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
True	12.10.2023 7:	Сортировка от старых	
True	03.10.2023 2:	Сортировка от новых к	
True	09.10.2023 13:	Сортировка по цвету	
True	08.10.2023 10:	Удалить фильтр из сто	
True	07.10.2023 15:	Фильтр по цвету	
True	05.10.2023 17:	Фильтры по дате	
True	06.10.2023 4:	Область поиска: (Все)	
True	08.10.2023 9:	<input checked="" type="checkbox"/> (Выделить все)	
True	05.10.2023 18:	<input checked="" type="checkbox"/> 2023	
True	08.10.2023 17:	<input checked="" type="checkbox"/> Август	
True	10.10.2023 18:	<input checked="" type="checkbox"/> Сентябрь	
True	08.10.2023 11:	<input checked="" type="checkbox"/> Октябрь	
True	04.10.2023 14:		
True	03.10.2023 11:		
True	08.10.2023 11:		
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 подп...	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 подп...	пользователи@builtin	✗ 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 подп...	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 подп...	пользователи@builtin	✗ Права удалены		F M X W R L S
ts.sus.local	\\ts.sus.local\...	Для этой папки, ее подп...	все	✗ Права удалены		F M X W R L S
ts.sus.local	\\ts.sus.local\...	Для этой папки, ее подп...	пользователи@builtin	⚠ Неверные флаги наследования	F M X W R L S	F M X W R L S
ts.sus.local	\\ts.sus.local\...	Для этой папки, ее подп...	пользователи@builtin	⚠ Наследование без родителя	F M X W R L S	
ts.sus.local	\\ts.sus.local\...	Для этой папки, ее подп...	пользователи@builtin	⚠ Ложное наследование		F M X W R L S
ts.sus.local	\\ts.sus.local\...	Для этой папки, ее подп...	все	⚠ Добавлен пользователь	F M X W R L S	
ts.sus.local	\\ts.sus.local\...	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

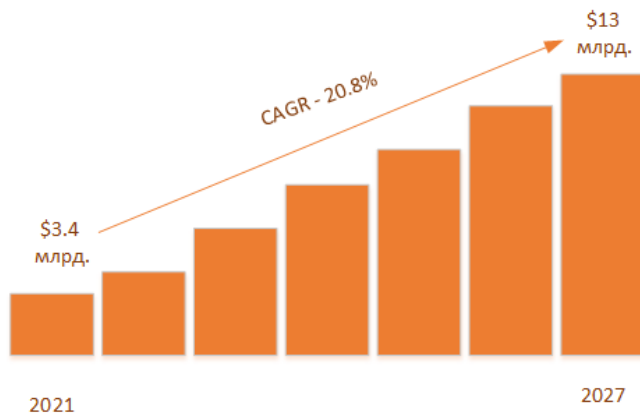


Рисунок 1. Насколько хорошо вы знакомы с решениями DCAP?



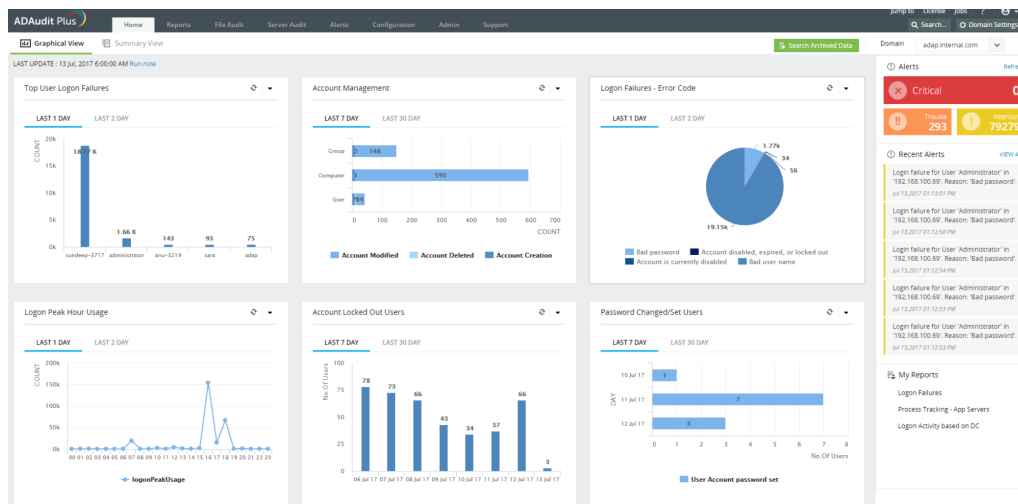
Российский рынок DCAP

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

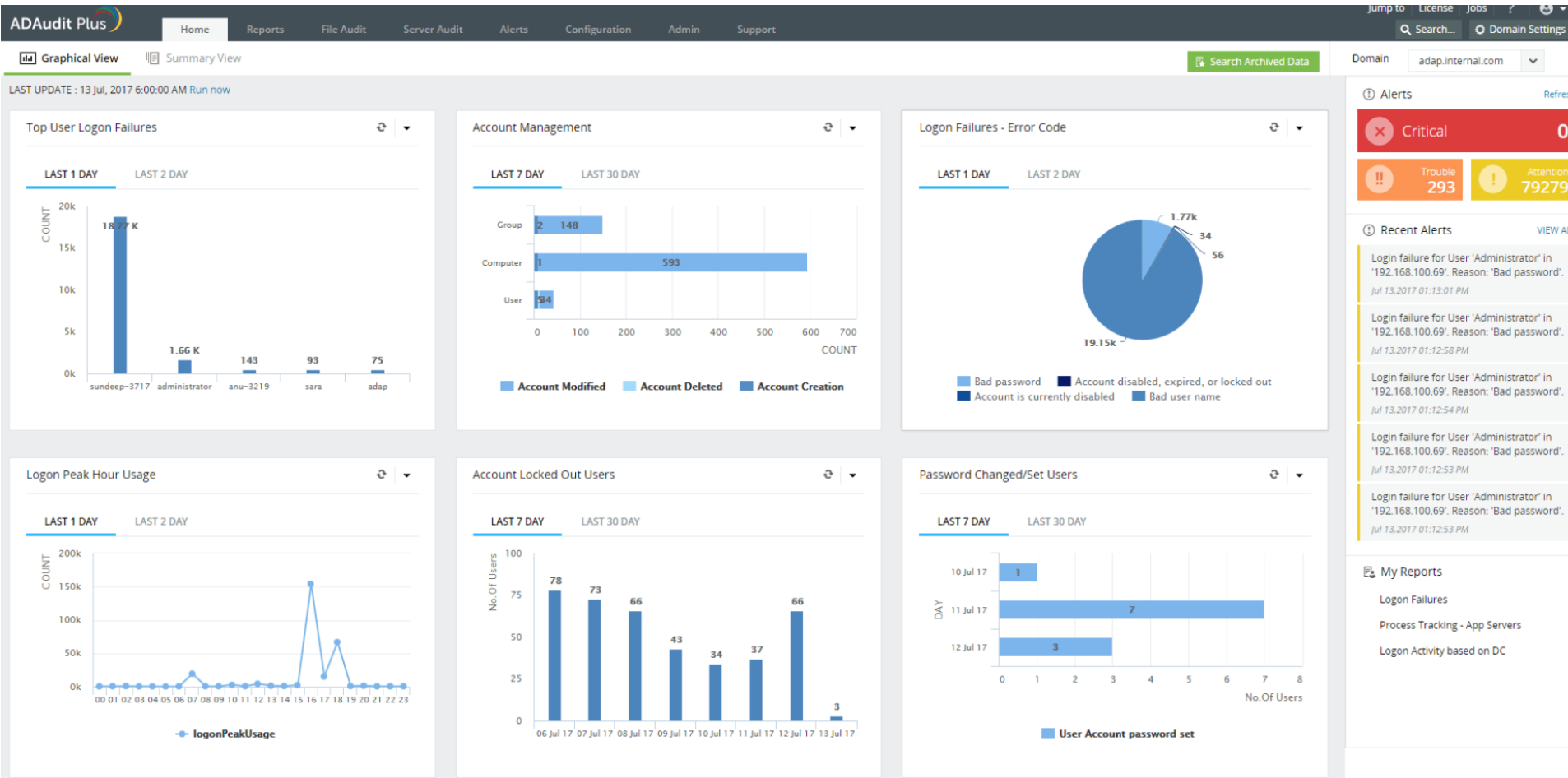
AD

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)

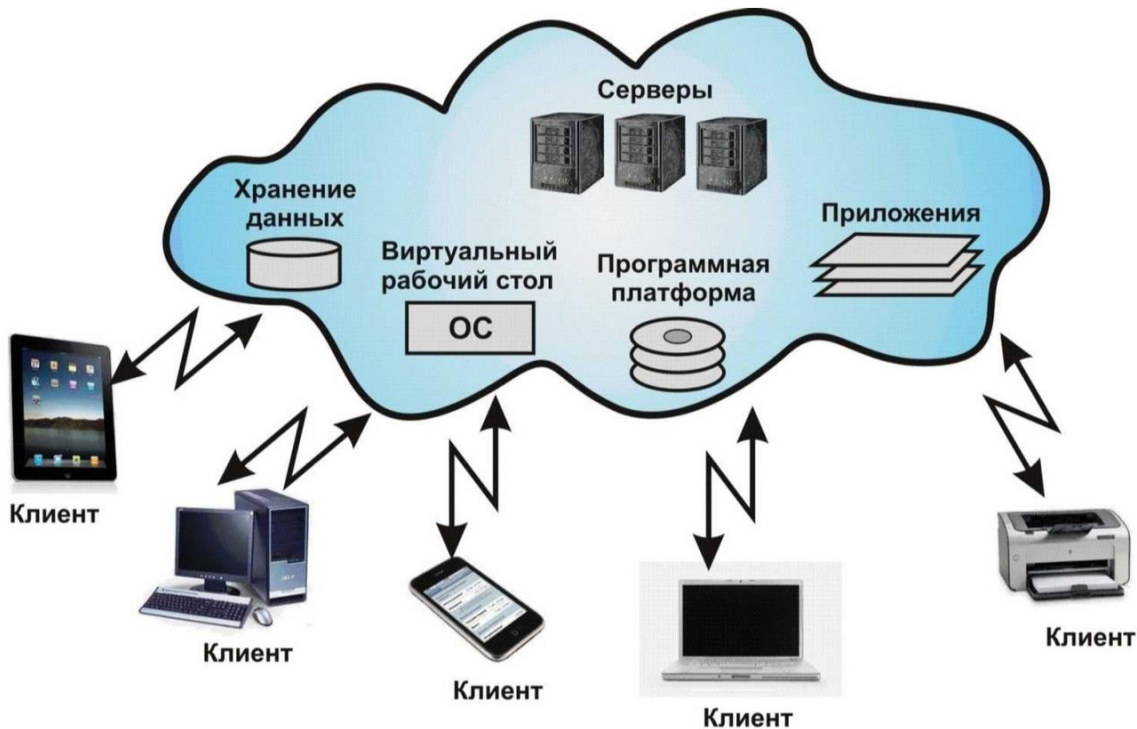


+

=



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				

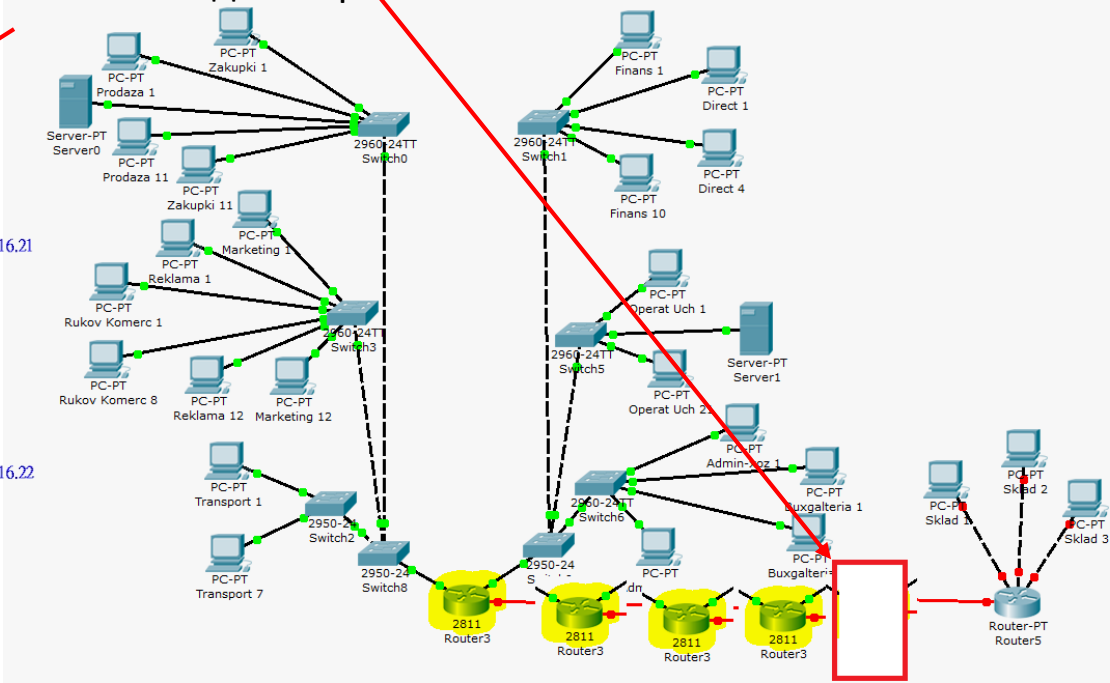
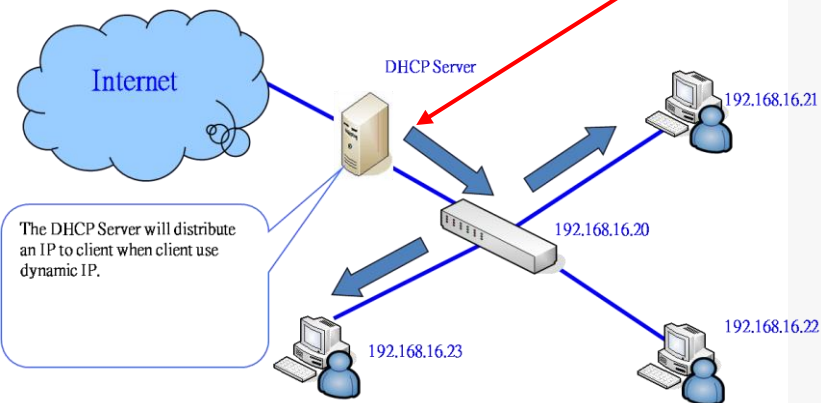
10.22.11.18	FLEET	
10.22.11.18	PORT	21/ftp/vsftpd/2.0.5/cpe:/a:vsftpd:vsftpd:2.0.5 21/
10.22.11.18	PORT	23/telnet/Linux telnetd//cpe:/o:linux:linux_kernel 23/
10.22.11.18	PORT	80/http/mini_httpd/1.19_19dec2003/cpe:/a:acme:mini_httpd:1.19_19dec2003 80/{"http-server-header": "mini_httpd/1.19_19dec2003", "http-title": "Site doesn't have a valid SSL certificate"}
10.22.11.18	PORT	427/svrlloc/// 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 http//cpe:/o:linux:linux_kernel 5988/{"http-title": "Site doesn't have a valid SSL certificate"}
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/sentinelism// 1947/{"fingerprint-strings": "\n FourOhFourRequest:\n HTTP/1.0 403 Forbidden\n Server: HASP LM/24.00\n Date: Sat, 02 Nov 2019 12:00:00 GMT\n Content-Type: text/html\n Content-Length: 131\n Connection: close\n Error: 403 Forbidden\n Error-Description: Access is denied."}
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\n"}
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

77.222.61.88

As of: Nov 06, 2024 6:58am UTC | Latest

Summary

History

WHOIS

Basic Information

Forward DNSwww.mpzmr.ru, xn--8c-vip42.web.ru, online.

Routing77.222.32.0/24 via SV

Services (1)3306/MYSQL

LabelsDATABASE

MYSQL 3306/TCP

DATABASE

Software

Oracle MySQL

Details

Error Code1130

Error IDER_HOST_NOT_PRIVILEGED

Error MessageHost '66.132.153.63' is not allowed to connect to this MySQL server

mysqlnickj

5/24

Results

Host Filters

Autonomous System:

Location:

Service Filters

Service Names:

Hosts

Results: 2 Time: 0.01s

178.159.43.197

(178-159-43-197.netherlands-2.vps.ac)

Ubuntu Linux

PODAON (211381)

North Holland, Netherlands

jQuery

click

default-landing-page

remote-access

:22/SSH

80/HTTP

443/HTTP

188.124.39.78

(188-124-39-78.st-petersburg-hosting.com)

Ubuntu Linux

SELECTEL (49505)

St.-Petersburg, Russia

remote-access

database

angularjs

:22/SSH

5432/POSTGRES

80/HTTP

7946/UNKNOWN

443/HTTP

8000/HTTP

2377/UNKNOWN

3334/HTTP

8080/HTTP

9000/HTTP

9443/HTTP

Pagination limited to 1.

Register or Log In

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 обновлений 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: Управ
нарушителю выполнить команды ОС на уязвимом узле, получить контроль над ресурсами и проникнуть во внут

Описание уязвимости

Уязвимость модуля landing системы управления содержимым сайтов (CMS) 1С-Битрикс: Управление сайтом вызвана
Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить команды ОС на уязви
внутреннюю сеть

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)
Критический уровень опасности (базовая оценка CVSS 3.0 составляет 10)

Дата выявления

13.09.2023

Идентификатор типа

CWE-362

Subject Name	
Country	RU
State/Province	Moscow Oblast
Locality	Odintsovo
Organization	ООО Мрз Мyasnitkiy 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



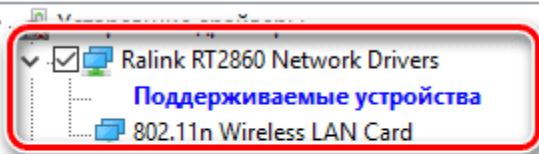
Virtual
Network
Computing



UltraVNC



Н



[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](#)

[ОСПБ «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.jspsa?id=92004	Игорь Игоревич Игорев
90.90.48.39	G-0000-5202	https://ShowObject.jspsa?id=92699	Игорь Игоревич Игорев
90.86.4.2	G2800-SQ01	https://ShowObject.jspsa?id=99942	Иванов Иван Иванович
90.46.0.57	G6400-DP01	https://ShowObject.jspsa?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)

ZABBIX



Network and server infrastructure



Cloud deployments



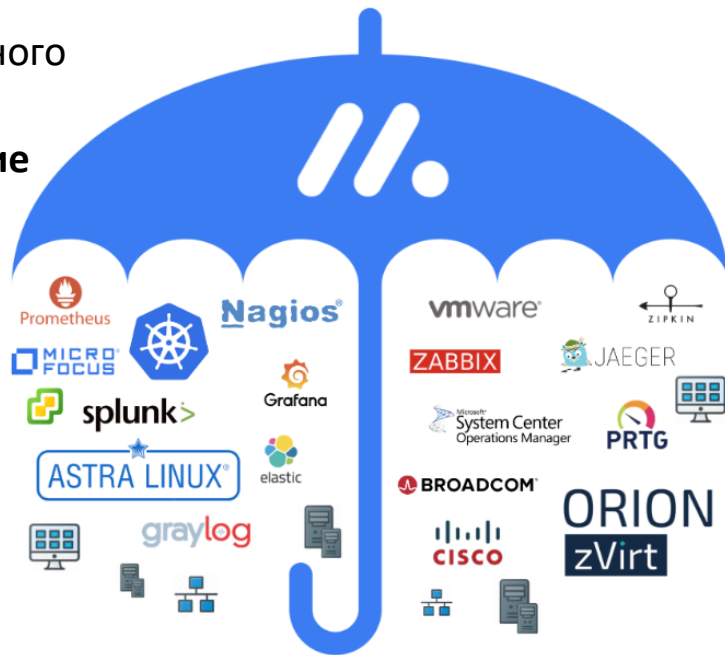
APIs and websites



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:

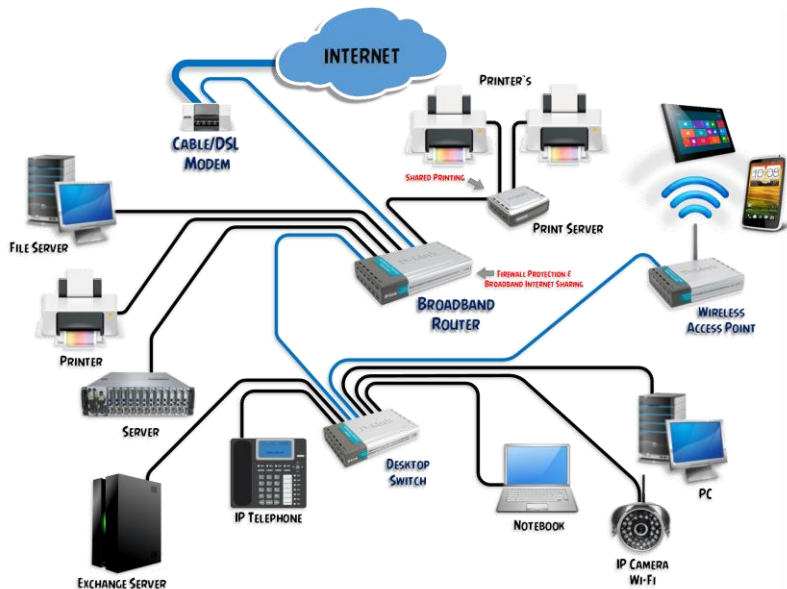
- **Ограничение физического доступа к инфраструктуре.**



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**

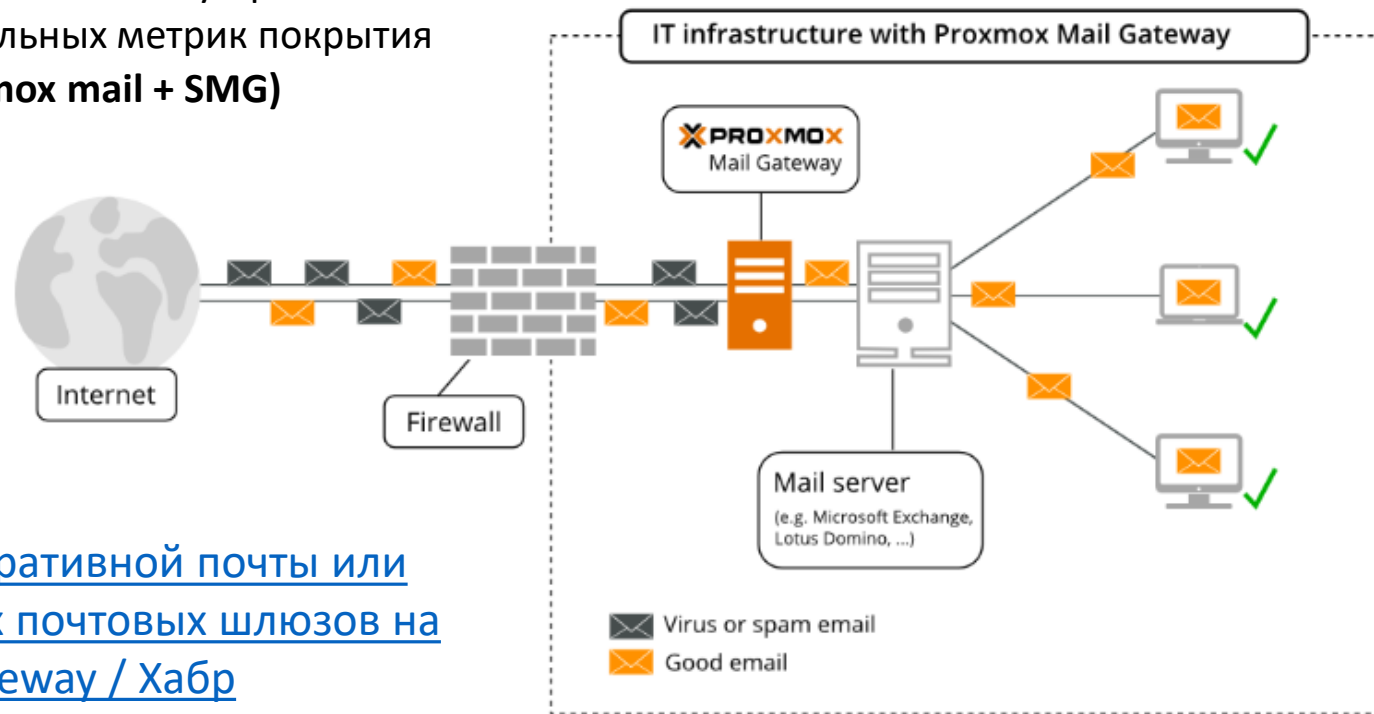
AB3 EDR SOC IDS DLP ...

	Кол-во	AB3	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)**

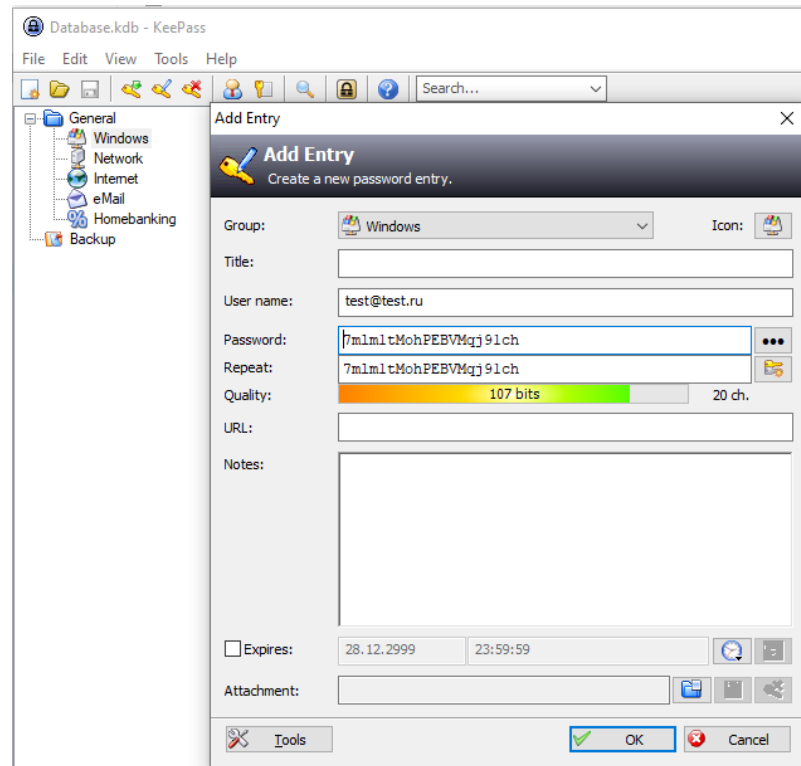


[ЧудЕСА защиты корпоративной почты или внедрение свободных почтовых шлюзов на базе Proxmox Mail Gateway / Хабр](#)

Начальные телодвижения

Установка, настройка, доработка:

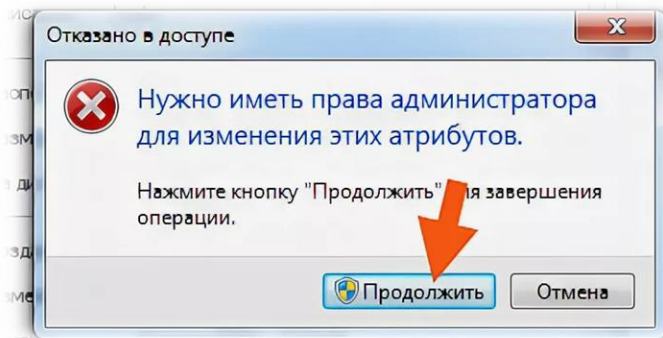
- Ограничение физического доступа к инфраструктуре.
- Покрытие СЗИ всех возможных устройств
- Выстраивание правильных метрик покрытия
- Защита почты (Proxmox mail + SMG)
- **Менеджеры паролей**



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)**

A screenshot of the LAPS UI window. The title bar says "LAPS UI". Inside the window, there are several fields: "Computer name:" with a text box containing "SRV01" and a "Search" button; "Password:" with a text box containing "oGYV+dRZ ([} 47-"; "Password expires:" with a text box containing "8/7/2021 10:54:21 PM"; and "New expiration time (leave as is for immediate expiration):" with a text box containing "Thursday , July 8, 2021 10:54:50 PM". There are "Set" and "Exit" buttons at the bottom right.

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

Начальные телодвижения

Установка, настройка, доработка:

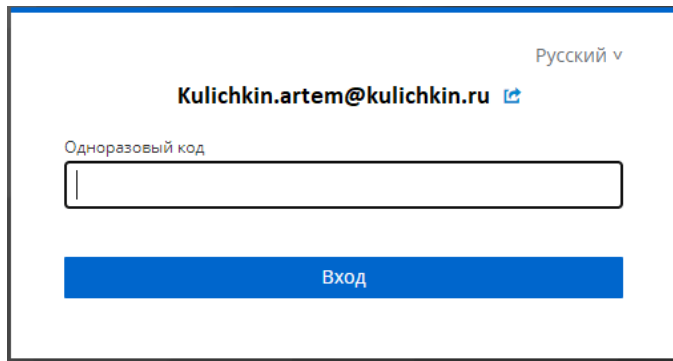
- Ограничение физического доступа к инфраструктуре.
- Покрытие СЗИ всех возможных устройств
- Выстраивание правильных метрик покрытия
- Защита почты (Proxmox mail + SMG)
- Менеджеры паролей
- Минимальные права у юзера
- Запрет работать из под администратора администраторам
- Внедрение Local Administrator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



The screenshot shows a web-based login interface for Two-Factor Authentication (2FA). At the top right, there is a language selector labeled "Русский" with a dropdown arrow. Below it, the email address "Kulichkin.artem@kulichkin.ru" is displayed next to a small blue icon. The main part of the interface features a label "Одноразовый код" (One-time code) above a text input field. At the bottom, there is a prominent blue button labeled "Вход" (Login).

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.
- Бэкап и восстановление + проверка.
- Запретить вход через рут по ssh

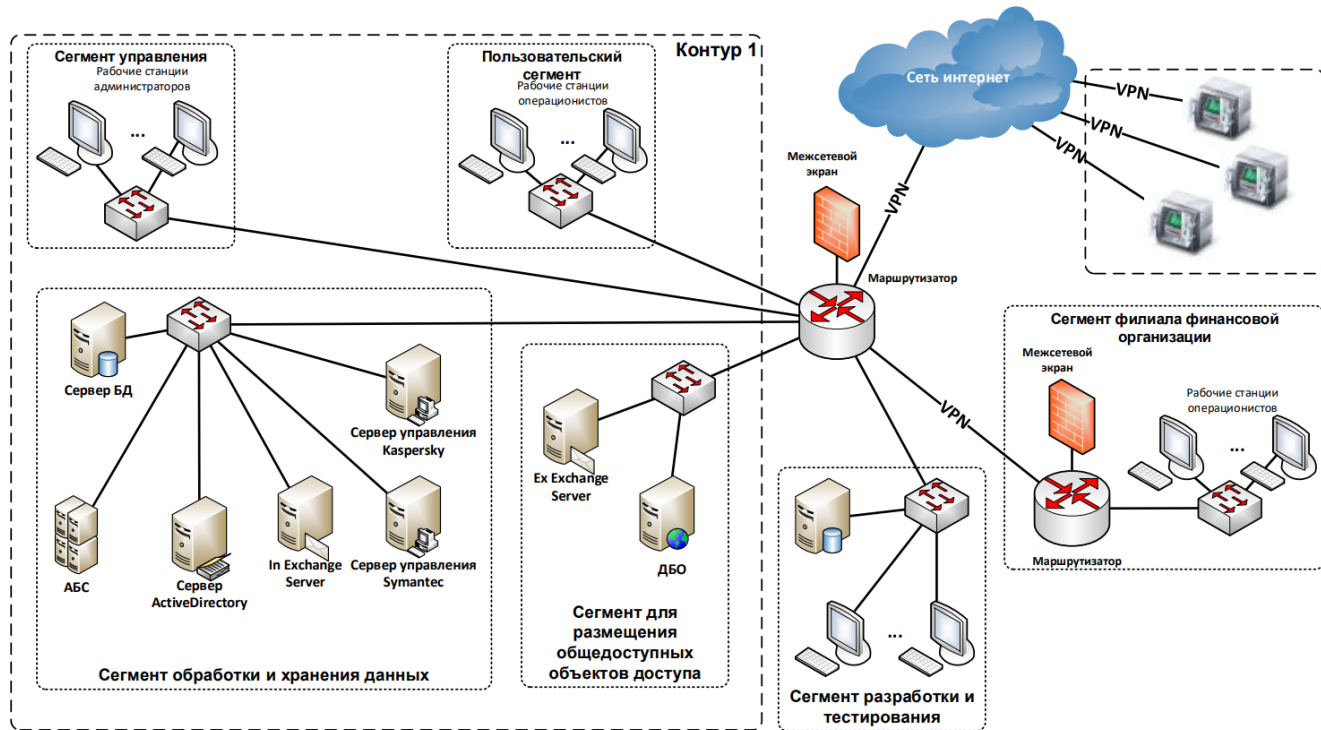
Прописать в ОРД спина болеть не будет

Администрирование

Установка, настройка, доработка:

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

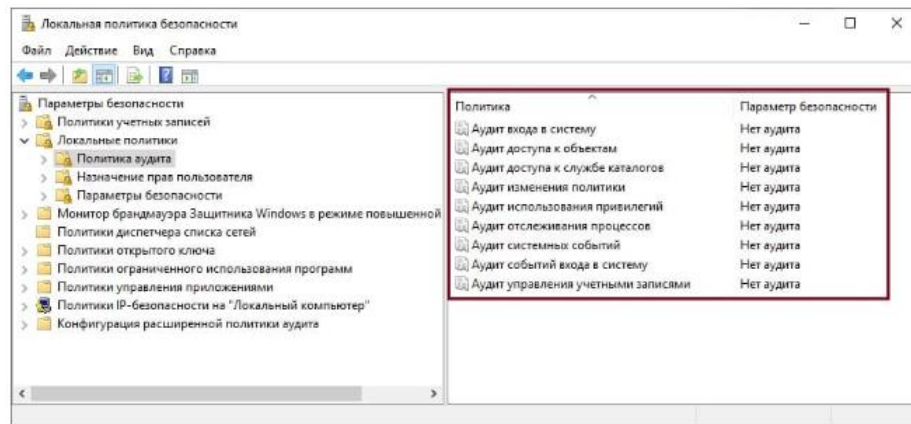
- ✓ Сегментирование сети
- ✓ Разделять прод, тест, деф.
- ✓ Запретить выход в интернет из серверного сегмента
- ✓ Выход в интернет через единый прокси с авторизацией



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**



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

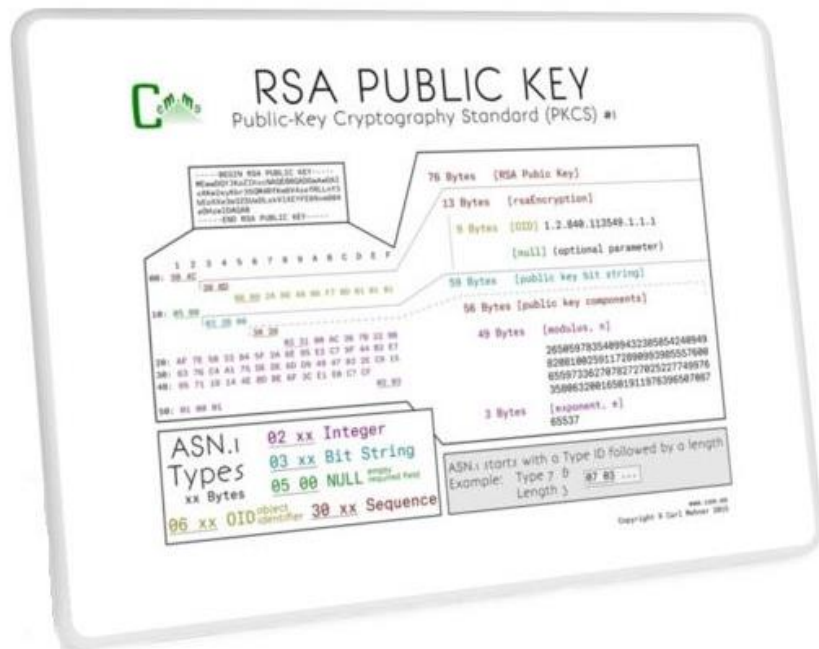


[Многоуровневая модель
среды PAM | Microsoft
Learn](#)

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 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

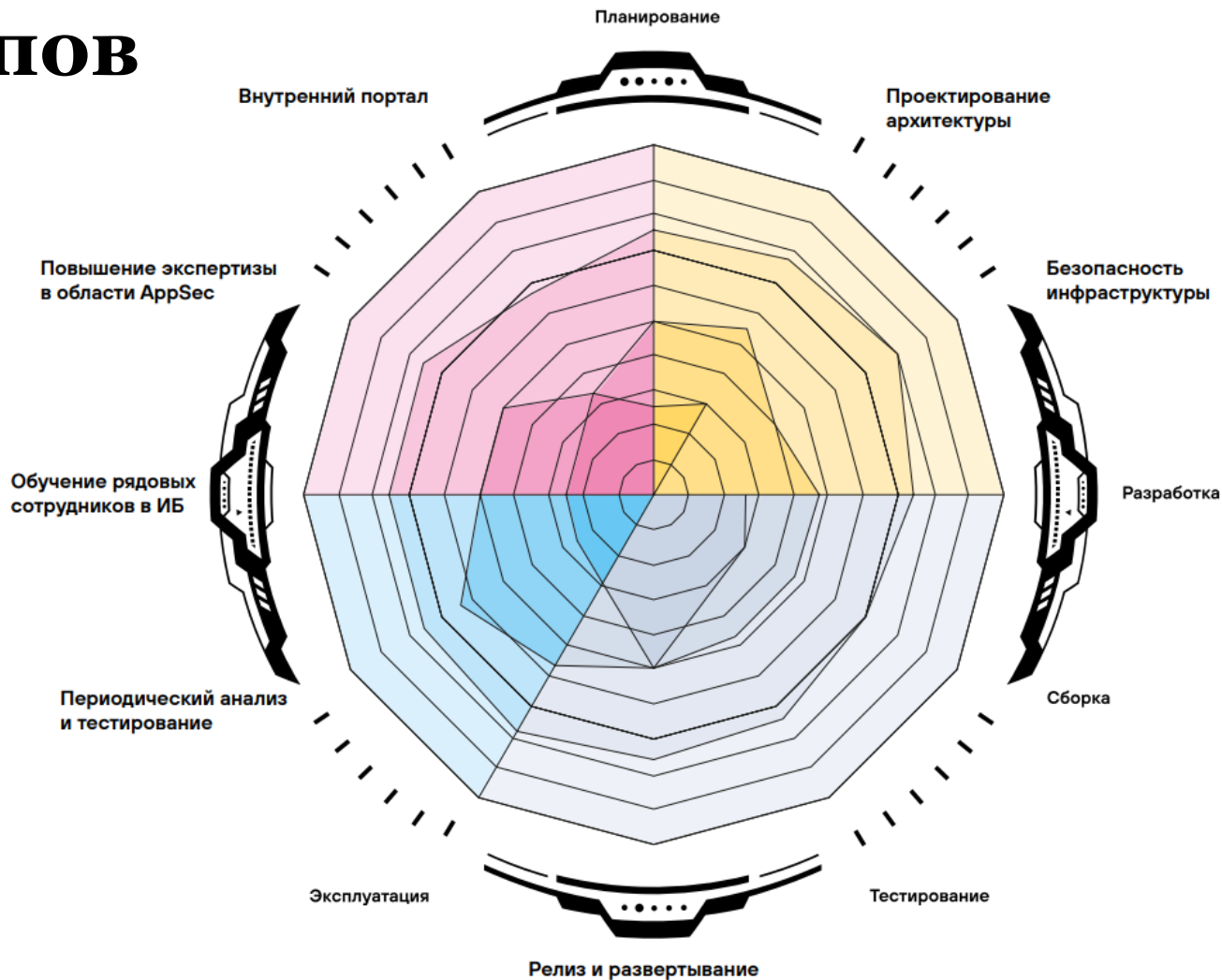
Установка, настройка, доработка:

- 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.