CYBERPEAK

системы защиты данных

DCAP/DAG “СПЕКТР”

КОНТРОЛЬ И ЗАЩИТА КОРПОРАТИВНЫХ ДАННЫХ

cyberpeak.ru

«САЙБЕРПИК»

РОССИЙСКИЙ РАЗРАБОТЧИК РЕШЕНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

10 ЛЕТ

в разработке решений ИБ

Sk Resident

Резидент Фонда «Сколково»

Лицензия СЗКИ ФСТЭК России

ПАРТНЕР ТОП-25

компаний-интеграторов России

AXOFT · ITD GROUP · КРОК · Jet · Информзащита · softline We клон не сил · ANGARA SECURITY · Cross Technologies

Внедрения в компаниях уровня

ENTERPRISE

20 000 +
Численностью сотрудников

100 +
терабайтами данных

КЛИЕНТЫ

РОСАТОМ · Банк Национальный стандарт · ТРАНСНЕФТЬ · СБЕР ЛОГИСТИКА · FESCO · RT · SBER AUTOTECH · БАНК САНКТ-ПЕТЕРБУРГ · CMD ЦЕНТР МОЛЕКУЛЯРНОЙ ДИАГНОСТИКИ

DCAP/DAG «СПЕКТР»

РЕШЕНИЕ КЛАССА DATA-CENTRIC AUDIT AND PROTECTION/DATA ACCESS GOVERNANCE

ГЛАВНАЯ ЗАДАЧА «СПЕКТРА»

защита хранилищ неструктурированных данных и контроллеров домена.

Система осуществляет полный контроль доступа сотрудников компании к файлам, находящимся на хранилищах неструктурированных данных:

Windows Server, Active Directory, DELL EMC, NetApp, Synology, Exchange, SharePoint, Nextcloud, Confluence, JIRA, Bitbucket, Linux, ubuntu, debian, CentOS, Astra Linux, РЕДОС

СПЕКТР

DAG/DCAP-СИСТЕМА

СИСТЕМА ВЫПОЛНЯЕТ:

- аудит доступа,
- классификацию всех документов,
- анализ прав.

- **РОССИЙСКАЯ РАЗРАБОТКА**
- **ВКЛЮЧЕНА В ЕДИНЫЙ РЕЕСТР РОССИЙСКИХ ПРОГРАММ ДЛЯ ЭВМ И БД №7143**
- **НЕ ТРЕБУЕТ ЛИЦЕНЗИИ НА СТОРОННИЕ КОММЕРЧЕСКИЕ ПРОДУКТЫ**

НЕСТРУКТУРИРОВАННЫЕ ДАННЫЕ

КАКИЕ СИСТЕМЫ ХРАНЯТ НЕСТРУКТУРИРОВАННЫЕ ДАННЫЕ ?

ACTIVE DIRECTORY

Windows Server

LINUX

Nextcloud

SharePoint

Exchange

ПОЧЕМУ ВАЖНО КОНТРОЛИРОВАТЬ НЕСТРУКТУРИРОВАННЫЕ ДАННЫЕ?

80%

корпоративных данных являются неструктурированными, по оценке Gartner.

на 30%

ежегодно увеличивается объем данных.

65%

атак направлены на получение конфиденциальной информации из неструктурированных данных.

20%

информации не приносит никакой пользы бизнесу (копии документов, файлы без изменений и т.д.)

РИСКИ, КОТОРЫЕ НЕСУТ НЕСТРУКТУРИРОВАННЫЕ ДАННЫЕ:

- Несоблюдение требований регуляторов
- Утечка конфиденциальной информации
- Риски масштабных потерь от вредоносного ПО
- Репутационные риски
- Замедление и остановка бизнес-процессов

ЧТО ДЕЛАЕТ «СПЕКТР» С НЕСТРУКТУРИРОВАННОЙ ИНФОРМАЦИЕЙ?

Помогает контролировать доступ к важной конфиденциальной информации, защищает её.

Выявляет информацию, которая не приносит пользы бизнесу (копии, файлы, которые не используются).

Помогает оптимизировать пространство хранилищ.

Фиксирует все действия, которые сотрудники производят с информацией.

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

Аудит действий и прав доступа к данным файловых хранилищ

UEBA построение профилей поведения сотрудников

Классификация и поиск чувствительных данных по требованиям регуляторов РФ, GDRP и других стандартов

Аудит Active Directory обнаружение связанных с этим аномалий и инцидентов

Активная реакция на инцидент/аномалию остановит действия вируса-шифровальщика путем блокировки пользователя/хранилища

Детекитрование изображений, паспартов, ВУ, СНИЛС, кредитных карт и др. на основе нейронных сетей

Автоматическое выявление рисков, связанных с неоптимально выданными правами

Мгновенный поиск по информации, хранящейся на файловых серверах

Портал выдачи прав и разрешений помогает выстроить работу с заявками на предоставление прав доступа

ТРЕБОВАНИЯ И СТАНДАРТЫ

В «СПЕКТРЕ» ИМЕЕТСЯ БОЛЕЕ 300 ПРАВИЛ, ОТЧЕТОВ, КАТЕГОРИЙ, КОТОРЫЕ ПОМОГАЮТ ВЫПОЛНЯТЬ ТРЕБОВАНИЯ РЕГУЛЯТОРОВ:

- Приказ ФСТЭК №21 – Обеспечение безопасности обработки ПДН
- Приказ ФСТЭК №239 – Меры безопасности для значимых объектов КИИ
- Приказ ФСЭК № 17 – Требования к защите информации в ГИС
- 152 ФЗ – О персональных данных.
- 187 ФЗ – Безопасность объектов КИИ РФ
- Приказ МинКомСвязи РФ №104 – Обеспечение безопасности для информационных систем общего пользования
- ГОСТ Р 57580.1 – 2017 – Безопасность финансовых операций
- PCI DSS – Международный стандарт безопасности данных платежных систем СТО БР
- ИББС – Стандарт по обеспечению ИБ банков РФ
- GDPR – Европейский регламент по защите ПДн

ОСОБЕННОСТИ ПРОДУКТА

«СПЕКТР» ОБЛАДАЕТ РЯДОМ ПРЕИМУЩЕСТВ

- Система адаптирована для работы с большим объемом данных (100+ ТБ, более 10 000 сотрудников)
- Внедрение системы в виде кластерного решения для отказоустойчивости и территориально распределенных инсталляций
- «Спектр» - это поисковая система для корпоративных файловых хранилищ
- Единый Портал выдачи и отзыва прав доступа и разрешений позволяет оптимизировать связанные бизнес процессы

«СПЕКТР» ДЛЯ IT-ДЕПАРТАМЕНТОВ И ДЕПАРТАМЕНТОВ ИБ

ДЛЯ IT-ДЕПАРТАМЕНТА

- Обнаружение действий вирусов шифровальщиков
- Помощь в распределении нагрузок на ресурсы
- Контроль и прогноз заполняемости файловых хранилищ
- Помощь в оптимизации файловых хранилищ
- Формирование отчетности о неиспользуемых файлах
- Формирование отчетности о дублированных файлах

ДЛЯ ДЕПАРТАМЕНТОВ ИБ

- Определение бизнес-владельца любого объекта
- Выявление сотрудников, имеющих доступ к объекту
- Список объектов, к которым есть доступ у сотрудника
- Кто из сотрудников и как использует данные
- Построение модели поведения сотрудника
- Определение излишнего доступа у сотрудников к данным
- Все инструменты для информационных расследований

ТЕХНОЛОГИЧЕСКИЕ ПРЕИМУЩЕСТВА

Производительность

Выявление инцидентов на ранних этапах

Возможность активной реакции на инцидент/ аномалию

Более 300 отчетов, правил, категорий для стартовой работы

Может инсталлироваться на Astra Linux, RedOS

Распознавание сканов и фотографий в том числе и внутри документов паспортов, ВУ, кредиток, СНИЛС на основе нейронных сетей

«Спектр» полностью готов к работе IT-департамента и Департамента информационной безопасности после инсталляции.

Confluence, Jira, NextCloud, Bitbucket

«Спектр» включает полностью описанный Rest API, позволяющий интегрироваться с: DLP, IDM, IRP и др.

Мгновенный поиск по всем хранилищам, в том числе и в содержимом на основе сохраненных индексов

ЧТО ЗАЩИЩАЕТ «СПЕКТР»

«СПЕКТР» ОСУЩЕСТВЛЯЕТ АУДИТ, КЛАССИФИКАЦИЮ И АНАЛИЗ ПРАВ ДОСТУПА ДЛЯ БОЛЬШОГО ЧИСЛА РАЗЛИЧНЫХ ХРАНИЛИЩ НЕСТРУКТУРИРОВАННЫХ ДАННЫХ, В Т. Ч. УНИКАЛЬНЫХ ДЛЯ РЕШЕНИЙ КЛАССА DCAP/DAG. СРЕДИ НИХ ПРИСУТСТВУЮТ:

- файловые серверы под управлением ОС Microsoft Windows Server, включая DFS;
- почтовые серверы Microsoft Exchange, включая Exchange 365;
- серверы контроллера домена Microsoft Active Directory, включая Azure AD, Novell eDirectory;
- порталы Microsoft SharePoint, включая SharePoint 365;
- файловые хранилища DELL EMC, NetApp, Synology;
- облачные файловые хранилища Nextcloud;
- файловые хранилища на основе ОС семейства Linux: Ubuntu, Debian, CentOS, RedHat, Fedora и их производных, а также Astra Linux и РЕД ОС;
- внутренние системы базы знаний Atlassian Confluence;
- система отслеживания ошибок Atlassian Jira;
- системы хостинга проектов и совместной разработки BitBucket.

МОДУЛИ «СПЕКТРА»

«СПЕКТР» ЛИЦЕНЗИРУЕТСЯ ПО МОДУЛЬНОМУ ПРИНЦИПУ, В ЗАВИСИМОСТИ ОТ КОЛИЧЕСТВА УЧЁТНЫХ ЗАПИСЕЙ И ТИПОВ ЗАЩИЩАЕМЫХ ХРАНИЛИЩ.

МОДУЛЬ	ТИП КОМПЛЕКТАЦИИ
Модуль аудита и анализа прав доступа	**БАЗОВАЯ**
Модуль аудита Microsoft Active Directory Модуль классификации данных защищаемых серверов Модуль поведенческой аналитики, оповещений и отчётности Модуль поиска по содержимому файлов Модуль переноса/удаления данных Портал выдачи/отзыва прав доступа и разрешения	**ДОПОЛНИТЕЛЬНАЯ**

МОДУЛЬ АУДИТА И АНАЛИЗА ПРАВ ДОСТУПА

ЯДРО СИСТЕМЫ «СПЕКТР», НА ЕГО ОСНОВЕ БАЗИРУЮТСЯ ОСТАЛЬНЫЕ МОДУЛИ.

- Собирает информацию о структуре каждого защищаемого хранилища и контроллеров домена, входящих в инфраструктуру организации.
- Анализирует структуру каталогов/ файлов защищаемых серверов, структуру организации, полученную посредством интеграции с контроллером домена, и прав доступа, полученных из ACL.
- Фиксирует все операции с данными на защищаемых серверах.
- Формирует двунаправленную матрицу доступа к данным.

МОДУЛЬ АУДИТА MICROSOFT ACTIVE DIRECTORY

ФИКСИРУЕТ СОБЫТИЯ ACTIVE DIRECTORY:

- создание / изменение / удаление учетных записей и других объектов,
- факты успешной и неуспешной авторизации, блокировки, активации, отключения учетных записей и др.

АНАЛИЗИРУЕТ НАСТРОЙКИ ACTIVE DIRECTORY:

- список УЗ с постоянным паролем,
- отключенные УЗ,
- членство в группах безопасности,
- и др.

Microsoft Active Directory

ВОЗМОЖНОСТЬ ГИБКОЙ НАСТРОЙКИ ОПОВЕЩЕНИЙ, ОТЧЕТОВ, СЦЕНАРИЕВ РЕАГИРОВАНИЯ.

МОДУЛЬ КЛАССИФИКАЦИИ ДАННЫХ ЗАЩИЩАЕМЫХ СЕРВЕРОВ

МОДУЛЬ ПОЗВОЛЯЕТ ОПРЕДЕЛИТЬ МЕСТОПОЛОЖЕНИЕ КРИТИЧНОЙ ИНФОРМАЦИИ И ПРАВА ДОСТУПА К НЕЙ:

- классифицирует всю информацию на защищаемых серверах;
- определяет наличие критичной информации в файлах, такой как: кредитные карты, ПДН, финансовая информация и другое (более 230 категорий);
- распознает изображения на базе технологий OCR и шаблоны изображений на базе пред обученных нейронных сетей.

ПОДДЕРЖИВАЕТ РАСПОЗНАВАНИЕ

БОЛЕЕ

70 ФОРМАТОВ

ДОКУМЕНТОВ, ВКЛЮЧАЯ НЕОГРАНИЧЕННЫЙ УРОВЕНЬ ВЛОЖЕННОСТИ.

МОДУЛЬ ПОВЕДЕНЧЕСКОЙ АНАЛИТИКИ, ОПОВЕЩЕНИЙ И ОТЧЁТНОСТИ

ПОВЕДЕНЧЕСКАЯ АНАЛИТИКА

Поведенческая аналитика выстраивается на основе данных:

- о работе всего хранилища;
- о работе каждого сотрудника;
- об активности доступа к определенной категории данных.

Модуль функционирует на основе обучаемых нейронных сетей, что дает:

- Высокую производительность
- Выявление отклонений в режиме, приближенном к реальному времени
- Минимизация количества ложноположительных срабатываний

МОДУЛЬ ПОВЕДЕНЧЕСКОЙ АНАЛИТИКИ, ОПОВЕЩЕНИЙ И ОТЧЁТНОСТИ

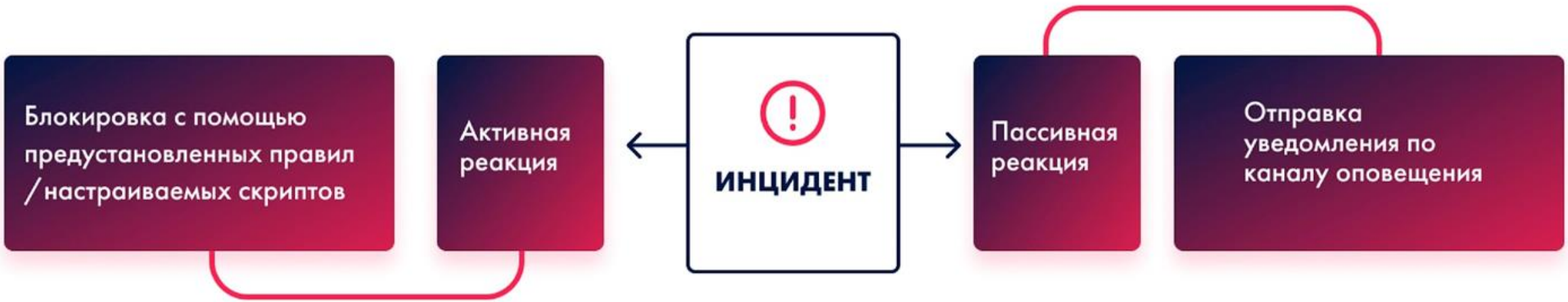
РАБОТА С ИНЦИДЕНТАМИ

Модуль выявляет нарушение пред настроенных политик безопасности, а также настроек, созданных при помощи конструктора «Спектра».

SIEM

отправляет результаты аудита в SIEM-системы

уведомляет по электронной почте сотрудников о потенциальных инцидентах



МОДУЛЬ ПОВЕДЕНЧЕСКОЙ АНАЛИТИКИ, ОПОВЕЩЕНИЙ И ОТЧЁТНОСТИ

ОТЧЕТЫ

БОЛЕЕ 50

предустановленных отчетов, решающие самые частные задачи ИТ-департаментов и Департаментов ИБ. Модуль позволяет изучить информацию по всем выявленным рискам в просканированных хранилищах.

ВЫ МОЖЕТЕ СОЗДАВАТЬ СВОИ ОТЧЕТЫ НА ОСНОВАНИИ ДАННЫХ АУДИТА ДОСТУПА К ХРАНИЛИЩАМ.

Модуль выявляет нарушение пред настроенных политик безопасности, а также настроек, созданных при помощи конструктора «Спектра»

Модуль отчетов помогает оптимизировать ваши корпоративные файловые хранилища, выявив:

- дубликаты файлов
- файлы, к которым не было обращений
- неиспользуемые ресурсы (без изменений)
- наиболее быстрорастущие папки
- динамику заполнения свободного места хранилищ

Отчеты строятся по заданному расписанию в автоматическом режиме с возможностью отправки на e-mail и сохранением на публичной папке.

ВЫЯВЛЕНИЕ И БЛОКИРОВКА ДЕЙСТВИЙ ВИРУСОВ-ШИФРОВАЛЬЩИКОВ

«СПЕКТР» ВЫЯВЛЯЕТ НАЛИЧИЕ И АКТИВНОСТЬ ВРЕДОНОСНОГО ПО В СИСТЕМЕ (НАПРИМЕР, ВИРУСОВ-ШИФРОВАЛЬЩИКОВ).

АНТИВИРУС

Совместная работа более эффективна

Сигнатурный анализ всех загружаемых исполняемых файлов

- ⊕ файлы, не прошедшие проверку, не загружаются
- ⊖ пропускает уязвимости 0-day

СПЕКТР
DAG/DCAP-СИСТЕМА

Сигнатурный анализ всех загружаемых исполняемых файлов →

Анализ действий с файлами от любого процесса/пользователя /приложения

анализирует все выполняемые операции вредоносного по, независимо от того, как оно попало в систему. →

Если операции носят аномальный характер, «Спектр»:

1. фиксирует и уведомляет
2. блокирует все операции вредоносного ПО/ все операции на системе.

МОДУЛЬ ПОИСКА ПО СОДЕРЖИМОМУ ФАЙЛОВ

Модуль обеспечивает возможность быстрого контентного поиска по содержимому всех документов. «Спектр» производит полную индексацию данных, анализируя содержимое документов защищаемых хранилищ на этапе сканирования. Индексация включает все поддерживаемые системой форматы файлов.

ВЫПОЛНЯЕТ ПОИСК ПО СЛОВАМ И СЛОВОСОЧЕТАНИЯМ ПО ГРАФИЧЕСКИМ ФАЙЛАМ

МОДУЛЬ ПОЛЕЗЕН:

- рядовым сотрудникам для поиска информации
- IT-департаменту
- департаменту информационной безопасности.

ПОРТАЛ ВЫДАЧИ/ОТЗЫВА ПРАВ ДОСТУПА И РАЗРЕШЕНИЯ

ПОЗВОЛЯЕТ ВЫСТРОИТЬ КОМПЛЕКСНЫЙ ПРОЦЕСС РАБОТЫ С ЗАЯВКАМИ НА УПРАВЛЕНИЕ ПРАВАМИ ДОСТУПА СОТРУДНИКОВ К ФАЙЛОВЫМ РЕСУРСАМ КОМПАНИИ.

ВОЗМОЖНОСТИ ПОРТАЛА:

- Назначение или отзыв прав конкретным сотрудникам
- Ограничение срока действия выданных прав доступа
- Указание ответственных за согласования выдачи прав доступа к каждому ресурсу
- Проведение инвентаризации и пересмотра текущих прав

Автоматизированное добавления сотрудников в группы безопасности, соответствующие правам доступа на заданный ресурс.
Портал позволяет вести анализ всех активных заявок с возможностью их отзыва и пересмотра.

МОДУЛЬ ПЕРЕНОСА/УДАЛЕНИЯ ДАННЫХ

ПРЕДЛАГАЕТ ФУНКЦИОНАЛ ДЛЯ ОРГАНИЗАЦИИ ПРОЦЕССА ОПТИМАЛЬНОГО ИСПОЛЬЗОВАНИЯ ФАЙЛОВЫХ ХРАНИЛИЩ С ТОЧКИ ЗРЕНИЯ РАСПОЛОЖЕННЫХ ТАМ ДОКУМЕНТОВ.

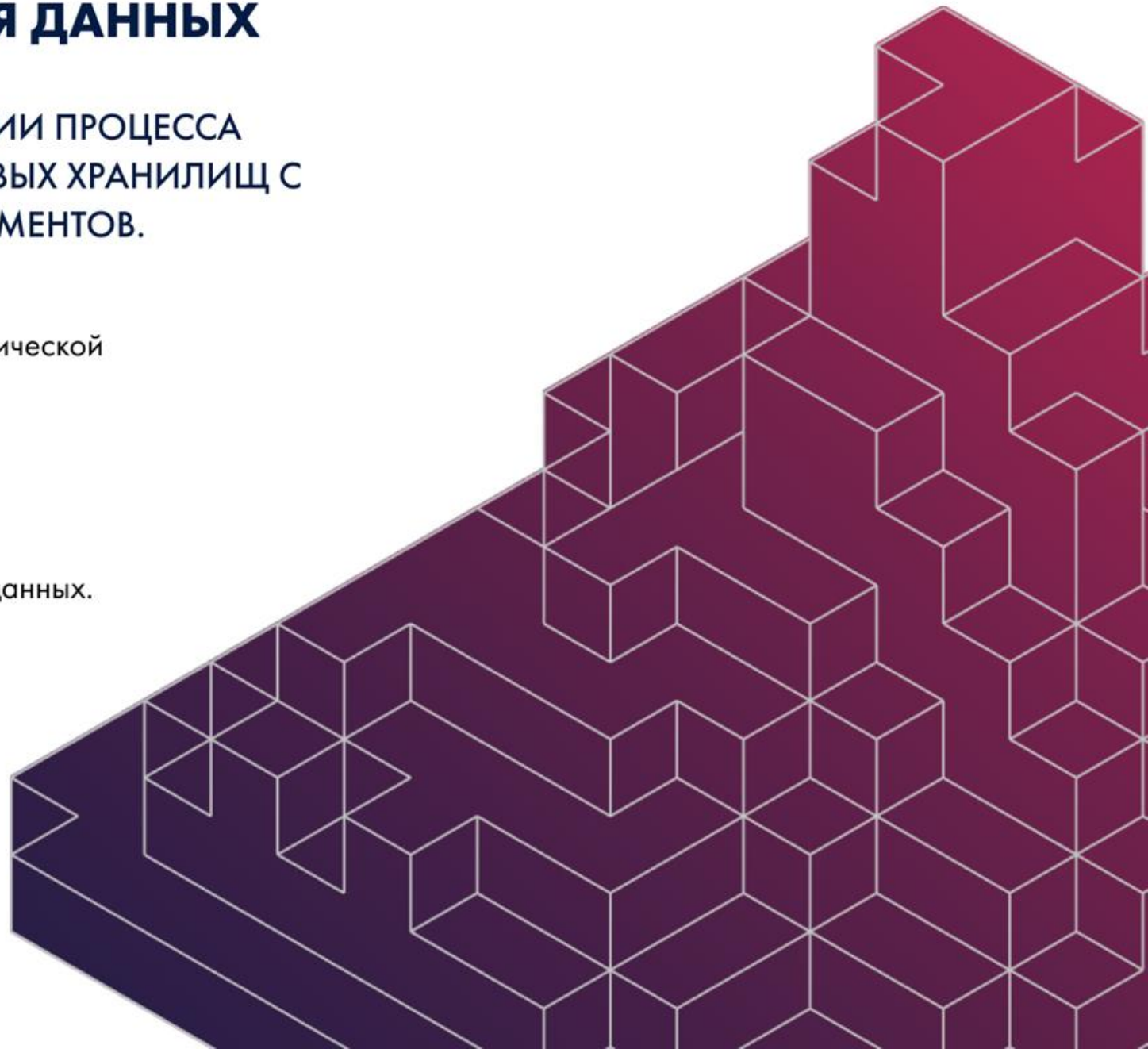
МОДУЛЬ ПОЗВОЛЯЕТ настраивать правила автоматической обработки и перемещения данных, учитывающие:

- месторасположение данных,
- дубликаты данных,
- статистику использования,
- настраиваемые пользователем правила обработки данных.

Выполнение требований регуляторов.

Инструмент для решения задач ИТ-департамента по оптимизации файловых хранилищ.

Автоматизация процесса преноса/удаления данных из нецелевых мест хранения.



ЭТАПЫ ИНТЕГРАЦИИ СИСТЕМЫ

30 ДНЕЙ БЕСПЛАТНО

1. **Аудит** существующей инфраструктуры (файловые сервера, контроллеры домена)
2. **Подготовка** инфраструктуры клиента к установке DAG «Спектр» (выделение ресурсов, открытие сетевых портов).
3. **Инсталляция** DAG «Спектр», установка агентов на защищаемые сервера
4. **Демонстрация** возможностей системы и обучение работе с основным функционалом
5. **Тестирование** системы с полным функционалом
6. **Отчет** по результатам аудита рисков
7. **Готовность** перейти в promo за 1 час

АРХИТЕКТУРА «СПЕКТРА»

ЦЕНТР УПРАВЛЕНИЯ СИСТЕМЫ «СПЕКТР»

СПЕКТР
DAG/DCAP-СИСТЕМА

Аудит доступа выполняется с помощью агентов. Классификация, получение структуры хранилищ и прав доступа происходит удаленно.

КОЛЛЕКТОРЫ

КОЛЛЕКТОРЫ

- Файловые хранилища MS Windows
- MS Exchange
- Серверы Sharepoint
- Dell EMC
- NetApp
- Active Directory
- Файловые хранилища Unix/Linux

СОТРУДНИЧЕСТВО

СПЕКТР
DAG/DCAP-СИСТЕМА

РАСЧЕТ СТОИМОСТИ

КОЛИЧЕСТВО МОДУЛЕЙ × КОЛИЧЕСТВО УЧЕТНЫХ ЗАПИСЕЙ

ТИПЫ ЛИЦЕНЗИРОВАНИЯ:

БЕССРОЧНАЯ ЛИЦЕНЗИЯ

ЛИЦЕНЗИЯ НА ОПРЕДЕЛЕННЫЙ СРОК (ПОДПИСКА)

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА:

8/5 **24/7**

CYBERPEAK
системы защиты данных

УЗНАЙТЕ ВСЕ О ВАШИХ ДАННЫХ И ЗАЩИТИТЕ ИХ

CYBERPEAK.RU

INFO@CYBERPEAK.RU

+7 (831) 228-01-82

Москва, ул. Донской 5-й проезд, 21Б, помещение 1

Нижний Новгород, ул. Академика Сахарова, 4, офис 628