ТЕХНИЧЕСКОЕ ЗАДАНИЕ

Система контроля и управления доступом к неструктурированным данным «Спектр»

Оглавление

1. ОБЩИЕ ТРЕБОВАНИЯ

1.1. ЦЕЛЬ ДОКУМЕНТА

В настоящем документе приведено описание требований к функциональным возможностям системы контроля и управления доступом к неструктурированным данным (далее – Система «Спектр»).

1.2. ТРЕБОВАНИЯ К ПРОИЗВОДИТЕЛЮ СИСТЕМЫ

1.2.1. Производителем Системы «Спектр» должна выступать организация, зарегистрированная на территории Российской Федерации.

1.2.2. Производитель Системы «Спектр» должен обладать действующей лицензией ФСТЭК России на деятельность по разработке и производству средств защиты конфиденциальной информации https://reestr.fstec.ru/reestr-litsenzij-szki.

1.2.3. Система «Спектр» должна быть включена в единый реестр российских программ для электронных вычислительных машин и баз данных https://reestr.digital.gov.ru/reestr/.

1.2.4. Система «Спектр» должна обладать действующим сертификатом ФСТЭК России на соответствие уровню доверия не ниже 4-го. Система «Спектр» должна быть включена в государственный реестр сертифицированных средств защиты информации https://reestr.fstec.ru/reg3

1.3. НАЗНАЧЕНИЕ СИСТЕМЫ

1.3.1. Система «Спектр» должна позволять осуществлять мониторинг операций пользователей с данными, расположенных на файловых серверах, СХД, облачных хранилищах, почтовых серверах, порталах совместного доступа, контроллерах домена (далее – защищаемые ресурсы), уведомлять об инцидентах аномального поведения и применять к ним активные реакции, включая блокировку доступа. Система «Спектр» также должна позволять сканировать и классифицировать защищаемые сервера, получать и отображать структуру и права доступа к объектам с неограниченным уровнем вложенности, осуществлять контекстный поиск по содержимому документов, и выявлять потенциальных владельцев данных.

1.3.2. Система «Спектр» предназначается для решения задач представителей отделов информационной безопасности и информационных технологий.

2. ТРЕБОВАНИЯ К АРХИТЕКТУРЕ СИСТЕМЫ

2.1. ТРЕБОВАНИЯ К СТРУКТУРЕ СИСТЕМЫ

2.1.1. Система «Спектр» должна состоять из следующих функциональных частей:

- **Модуль аудита и анализа прав доступа**
  Модуль должен осуществлять полное логирование всех операций с данными, происходящих на файловых серверах (Windows, Linux), СХД (DellEMC, NetApp, Synology, Huawei Dorado, Hitachi NAS, NFS, SFTP), облачных хранилищах (NextCloud), почтовых серверах Exchange, порталах SharePoint, системах Confluence и Jira, сканировать и отображать структуру находящихся на них объектов и права доступа к ним, а также формировать отчёты.
  В зависимости от типа защищаемого ресурса модуль дополнительно должен предоставлять возможность анализа прав доступа с помощью двунаправленной модели, их изменения непосредственно через интерфейс программы с опциональным предварительным моделированием и подсвечивать проблемные моменты в виде рисков-индикаторов.
- **Модуль аудита MS Active Directory**
  Модуль должен осуществлять фиксацию событий, связанных с функционированием службы каталогов: создание, изменение, удаление учётных записей и других объектов; факты успешной и неуспешной авторизации; блокировки, активации, отключения учетных записей; изменение доменных политик и др. Модуль должен анализировать структуру службы каталогов и права доступа к ним, формировать отчёты и подсвечивать проблемные моменты в виде рисков-индикаторов.
- **Модуль классификации**
  Модуль должен позволять получать информацию о наличии той или иной критичной информации в файлах, содержащихся на защищаемых серверах, включая номера кредитных карт, ПДн, финансовую информацию и др. Модуль также должен распознавать изображения на базе технологий OCR и шаблоны изображений на базе обучаемых нейронных сетей.
- **Модуль маркировки документов**
  Модуль должен позволять осуществлять маркировку документов сотрудниками для их последующего визуального отображения при работе с файлом, применением наложенных политик работы в зависимости от категории метки и сохранением аудита действий с промаркированными документами.
- **Модуль поведенческой аналитики, оповещений и отчётности**
  Модуль должен строить модели типичного поведения каждой учётной записи, выявлять отклонения от стандартного поведения и уведомлять об этом пользователей Системы «Спектр». Модуль должен позволять формировать политики безопасности на базе активных реакций на одно или несколько событий, уведомлять о потенциальных инцидентах, направлять события аудита во внешние системы и отправлять отчёты на E-mail по расписанию заинтересованным лицам.
- **Модуль поиска**

Модуль должен осуществлять поиск информации по содержимому любых документов, расположенных на защищаемых серверах, включая поиск по текстовому содержимому графических изображений. Модуль должен предоставлять возможность экспортировать результаты в файл, проставлять метки на найденные документы, а также осуществлять поиск бинарной копии выбранного пользователем файла вне зависимости от его наименования и расширения.

- **Модуль переноса/удаления данных**
  Модуль должен позволять настраивать правила автоматической обработки и перемещения данных, включая перенос или удаление неиспользуемых данных, дубликатов или файлов с заданными свойствами, такими как размер или категории классификации.
- **Портал запроса/выдачи прав и разрешений**
  Модуль должен позволять автоматизировать процесс запроса и выдачи разрешений пользователям на файловые ресурсы, включая возможность назначения или отзыва прав конкретным сотрудникам, ограничения срока действия выданных прав, настройки цепочки согласования к каждому ресурсу и автоматизации добавления сотрудников в необходимые группы безопасности.

2.2. ТРЕБОВАНИЯ К КОМПОНЕНТАМ СИСТЕМЫ

2.2.1. Серверные компоненты Системы «Спектр» должны работать на серверах или виртуальных машинах под управлением одной из следующих ОС:
- Ubuntu Server 18.04 или 20.04;
- CentOS 7.4–7.9;
- Red Hat Enterprise Linux 7.4–7.9, 8.9;
- Astra Linux 1.7.3;
- РЕД ОС 7.3.

2.2.2. Подсистема хранения данных Системы «Спектр» должна быть построена с использованием следующих базах данных:
- ClickHouse;
- ElasticSearch;
- PostgreSQL.

2.2.3. Сбор событий с файловых серверов Windows должен осуществляться либо с помощью агентского решения без использования встроенного аудита, либо без агента с использованием встроенного аудита на выбор администратора.

2.2.4. Агент для сбора событий на файловых серверах Windows должен иметь авторитетную цифровую подпись для предотвращения блокировки со стороны антивирусного ПО и другого специализированного ПО для защиты информации.

2.2.5. Сбор событий из службы каталогов Active Directory должен осуществляться с помощью агентского решения или удалённого получения событий аудита на выбор администратора.

2.3. ТРЕБОВАНИЯ К МАСШТАБИРОВАНИЮ

2.3.1. Модули Системы «Спектр» должны поддерживать горизонтальное масштабирование для решения следующих задач:

- увеличение производительности Системы «Спектр»;
- повышение отказоустойчивости конкретного модуля и Системы «Спектр»;
- возможность внедрения Системы «Спектр» на территориально распределенных площадках.

2.3.2. Модули мониторинга за защищаемыми ресурсами Системы «Спектр» должны поддерживать вертикальное масштабирование с целью увеличения общей производительности посредством увеличения количества экземпляров данных модулей.

2.3.3. Система «Спектр» должна позволять кластеризовать компоненты хранилища, распределяя тем самым нагрузку между узлами кластера.

2.4. ТРЕБОВАНИЯ К НАДЁЖНОСТИ И ОТКАЗОУСТОЙЧИВОСТИ

2.4.1. Система «Спектр» должна обладать возможностью выделения модулей-реплик для каждого модуля Системы «Спектр» в целях повышения отказоустойчивости.

2.4.2. Система «Спектр» должна обеспечивать следующие показатели надежности:

- круглосуточная работа 24/7 в необслуживаемом режиме;
- коэффициент готовности Системы «Спектр» – 99,9%.

2.4.3. В случае программных или аппаратных сбоев Система «Спектр» должна обладать возможностью предоставления администратору Системы «Спектр» отладочной информации.

2.5. ТРЕБОВАНИЯ К ПОДДЕРЖИВАЕМЫМ ТИПАМ СИСТЕМ

2.5.1. Система «Спектр» должна обладать возможностью осуществлять мониторинг следующих защищаемых ресурсов:

- файловые сервера под управлением ОС MS Windows Server 2008R2 и выше, включая поддержку DFS (Distributed File System) и технологию кластеризации серверов, без использования встроенного аудита Windows;
- системы хранения данных DellEMC, NetApp, Synology, Huawei Dorado, Hitachi NAS;
- файловые сервера под управлением ОС семейства Linux: Ubuntu, Debian, CentOS, RedHat, Fedora, Astra Linux, RedOS, без использования встроенного аудита;
- облачные хранилища NextCloud, VK WorkDisk;
- S3-совместимые объектные хранилища;
- сервера NFS;
- сервера SFTP;
- рабочие станции;
- почтовые сервера MS Exchange;
- сервера MS SharePoint;
- службы каталогов MS Active Directory, FreeIPA, ALD Pro;

- системы базы знаний Atlassian Confluence;
- системы контроля заявок Atlassian Jira;
- системы совместной разработки BitBucket.

2.6. ТРЕБОВАНИЯ К ХРАНЕНИЮ И ОБРАБОТКЕ ДАННЫХ

2.6.1. Время доступности в интерфейсе информации о совершенных событиях не должно превышать 200 секунд с момента совершения этого действия на защищаемом ресурсе.

2.6.2. Скорость отображения информации в графическом виде в интерфейсе Системы «Спектр» для 1 000 000 событий аудита не должна превышать 5 секунд.

2.6.3. Система «Спектр» должна обеспечивать обработку и сохранение всей получаемой информации, позволять делать интерактивную выборку и формировать отчёты с использованием фильтров, а также экспортировать данные во внешние системы.

2.6.4. Система «Спектр» должна обеспечивать возможность резервного копирование и ротации данных для каждого из защищаемых ресурсов и функциональных модулей Системы «Спектр» с указанием следующих режимов работы:

- резервное копирование;
- удаление;
- резервное копирование и удаление.

2.6.5. Резервное копирование должно осуществляться по заданному расписанию с указанием путей хранения.

2.6.6. Система «Спектр» должна позволять задавать глубину хранения данных.

2.7. ТРЕБОВАНИЯ К ИНТЕГРАЦИИ С ВНЕШНИМИ СИСТЕМАМИ

2.7.1. Система «Спектр» должна обладать возможностью отправки событий аудита с защищаемых ресурсов, аномалий, политик безопасности, внутреннего журнала действий пользователей и журнала системных событий во внешнюю систему посредством одного или нескольких методов:

- E-mail;
- Telegram;
- Syslog;
- HTTP;
- TCP/UDP;
- Splunk;
- ElasticSearch;
- Slack.

2.7.2. Система «Спектр» должна обладать возможностью настройки нескольких шаблонов для отправки событий во внешние системы с наложением фильтров.

2.7.3. Система «Спектр» должна интегрироваться со службой каталогов Active Directory, FreeIPA и ALD Pro посредством протокола LDAP и собирать информацию пользователях и группах с целью корректного отображения прав доступа на защищаемых ресурсах.
2.7.4. Система «Спектр» должна поддерживать несколько доменов, деревьев и лесов службы каталогов.
2.7.5. Сбор информации из службы каталогов должен осуществляться в автоматическом режиме с заданным расписанием.
2.7.6. Система «Спектр» должна обладать задокументированным интерфейсом REST API для взаимодействия с внешними системами.

2.8. ТРЕБОВАНИЯ К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.8.1. Система «Спектр» должна поддерживать и использовать защищенные протоколы и механизмы взаимодействия с внешними системами и между собственными внутренними модулями.
2.8.2. Доступ к интерфейсу системы должен осуществляться по зашифрованному протоколу HTTPS с авторизацией пользователей.
2.8.3. Система «Спектр» должна поддерживать установку в локальной инфраструктуре без доступа к сети Интернет.

3. ТРЕБОВАНИЯ К ФУНКЦИОНАЛЬНЫМ ВОЗМОЖНОСТЯМ

3.1. СБОР СОБЫТИЙ АУДИТА

3.1.1. Результаты аудита файловых серверов (Windows, Linux), СХД (DellEMC, NetApp, Synology, Huawei Dorado, Hitachi NAS, NFS, SFTP), облачных хранилищ (NextCloud), порталов SharePoint должны включать в себя следующую информацию:

- базовую информации о событии (дату, время и статус операции; информацию об объекте, субъекте и источнике события);
- тип действия (операции) над объектом, включая:
  - чтение / изменение / удаление / создание;
  - переименование (с отображением старых и новых имени объекта и месторасположения);
  - перемещение (с отображением старых и новых имени объекта и месторасположения);
  - изменение прав (с отображением прав до и после совершения операции, а также различий (изменений) между ними);
  - открытие / отключение сетевого доступа;
  - добавление / изменение / удаление квоты NTFS (Windows).
- способ совершения действия: локально или удаленно;
- имя процесса (в случае локального способа и для систем с агентом).

3.1.2. Результаты аудита службы каталогов Active Directory должны включать в себя следующую информацию:

- базовую информации о событии (дату, время и статус операции; информацию об объекте, субъекте и источнике события);
- уровень важности события;
- тип действия (операции) над объектом, включая следующие Event ID: 4608, 4610, 4611, 4612, 4614, 4615, 4616, 4618, 4621, 4622, 4624, 4625, 4626, 4627, 4634, 4646, 4647, 4648, 4649, 4650, 4651, 4652, 4653, 4655, 4656, 4657, 4658, 4660, 4661, 4662, 4663, 4664, 4665, 4666, 4667, 4668, 4670, 4671, 4672, 4673, 4674, 4675, 4688, 4689, 4690, 4691, 4692, 4693, 4694, 4695, 4696, 4697, 4698, 4699, 4700, 4701, 4702, 4703, 4704, 4705, 4706, 4707, 4709, 4710, 4711, 4712, 4713, 4714, 4715, 4716, 4717, 4718, 4719, 4720, 4722, 4723, 4724, 4725, 4726, 4727, 4728, 4729, 4730, 4731, 4732, 4733, 4734, 4735, 4737, 4738, 4739, 4740, 4741, 4742, 4743, 4744, 4745, 4746, 4747, 4748, 4749, 4750, 4751, 4752, 4753, 4754, 4755, 4756, 4757, 4758, 4759, 4760, 4761, 4762, 4763, 4764, 4765, 4766, 4767, 4768, 4769, 4770, 4771, 4772, 4773, 4774, 4775, 4776, 4777, 4778, 4779, 4780, 4781, 4782, 4783, 4784, 4785, 4786, 4787, 4788, 4789, 4790, 4791, 4792, 4793, 4794, 4798, 4799, 4800, 4801, 4802, 4803, 4816, 4817, 4818, 4819, 4826, 4864, 4865, 4866, 4867, 4868, 4869, 4870, 4871, 4872, 4873, 4874, 4875, 4876, 4877, 4878, 4879, 4880, 4881, 4882, 4883, 4884, 4885, 4886, 4887, 4888, 4889, 4890, 4891, 4892, 4893, 4894, 4895, 4896, 4897, 4898, 4902, 4904, 4905, 4906, 4907, 4908, 4909, 4910, 4911, 4912, 4913, 4928, 4929, 4930, 4931, 4932, 4933, 4934, 4935, 4936, 4937, 4944, 4945, 4946, 4947, 4948, 4949, 4950, 4951, 4952, 4953, 4954, 4956, 4957, 4958, 4960,

4961, 4962, 4963, 4964, 4965, 4976, 4977, 4978, 4979, 4980, 4981, 4982, 4983, 4984, 4985, 5024, 5025, 5027, 5028, 5029, 5030, 5031, 5032, 5033, 5034, 5035, 5037, 5038, 5039, 5040, 5041, 5042, 5043, 5044, 5045, 5046, 5047, 5048, 5049, 5051, 5056, 5057, 5058, 5059, 5060, 5061, 5062, 5063, 5064, 5065, 5066, 5067, 5068, 5069, 5070, 5136, 5137, 5138, 5139, 5140, 5141, 5142, 5143, 5144, 5145, 5148, 5149, 5150, 5151, 5152, 5153, 5154, 5155, 5156, 5157, 5158, 5159, 5168, 5376, 5377, 5378, 5440, 5441, 5442, 5443, 5444, 5446, 5447, 5448, 5449, 5450, 5451, 5452, 5453, 5456, 5457, 5458, 5459, 5460, 5461, 5462, 5463, 5464, 5465, 5466, 5467, 5468, 5471, 5472, 5473, 5474, 5477, 5478, 5479, 5480, 5483, 5484, 5485, 5632, 5633, 5712, 5888, 5889, 5890, 6144, 6145, 6272, 6273, 6274, 6275, 6276, 6277, 6278, 6279, 6280, 6281, 6400, 6401, 6402, 6403, 6404, 6405, 6406, 6407, 6408, 6409, 6410, 6416, 6419, 6420, 6421, 6422, 6423, 6424;

- детальные текстовые изменения содержимого групповой политики для соответствующих событий изменения политик GPO.

3.1.3. Результаты аудита MS Exchange должны включать в себя следующую информацию:

- базовую информации о событии (дату, время и статус операции; информацию об объекте, субъекте и источнике события);
- список отправителей, получателей и скрытых получателей;
- тип действия (операции), включая:
  - создание, перемещение, удаление, отправка, отправка от другого лица, получение, экспорт письма;
  - выключение и отключение почтового пользователя, ящика, контакта;
  - создание и удаление почтового пользователя, ящика, контакта, внутренней папки, общей папки, почтового правила;
  - добавление, удаление и изменение разрешений на ящик, внутреннюю папку или общую папку.

3.1.4. Результаты аудита Atlassian Confluence должны включать в себя следующую информацию:

- базовую информации о событии (дату, время и статус операции; информацию об объекте, субъекте и источнике события);
- тип действия (операции) над объектом, включая:
  - пользователь создан, удален, переименован, обновлен, выполнил запрос сброса пароля, успешно авторизовался, добавлен в группу, удалён из группы;
  - каталог пользователя создан, удалён, обновлён;
  - группа создана, удалена;
  - вложение скачано, загружено, удалено, отправлено в корзину;
  - комментарий добавлен или удалён;
  - добавлено, удалено или обновлено глобальное разрешение, изменены глобальные настройки, добавлена или обновлена лицензия;
  - создание, удаление, импорт, экспорт, добавление разрешения, удаление разрешения, обновление конфигурации пространства;
  - создание, изменение, удаление, восстановление страницы, добавлено или удалено ограничение на просмотр или редактирование страницы.

3.1.5. Результаты аудита Atlassian Jira должны включать в себя следующую информацию:

- базовую информации о событии (дату, время и статус операции; информацию об объекте, субъекте и источнике события);

- тип действия (операции) над объектом, включая:
  - пользователь создан, удален, переименован, обновлен, выполнил запрос сброса пароля, успешно авторизовался, добавлен в группу, удалён из группы;
  - каталог пользователя создан, удалён, обновлён;
  - группа создана, удалена;
  - вложение скачано, загружено, удалено, отправлено в корзину;
  - комментарий добавлен или удалён;
  - добавлено, удалено или обновлено глобальное разрешение, изменены глобальные настройки, добавлена или обновлена лицензия;
  - создание или удаление фильтра, доски, задачи или ссылки;
  - создание, удаление, обновление проекта или роли проекта;
  - создание или обновление рабочего процесса или пользовательского поля, создание и добавление в проект схемы рабочего процесса;
  - схема прав доступа добавлена, удалена, создана или обновлена;
  - создана новая резолюция, создан тип задачи, выполнен поиск JQL, выполнена синхронизация по расписанию.

3.2. ОБРАБОТКА И ОТОБРАЖЕНИЕ СОБЫТИЙ АУДИТА

3.2.1. Система «Спектр» должна обеспечивать обработку и сохранение событий аудита и позволять вести выборочный анализ данных с возможностью фильтрации по любым свойствам событий в любых комбинациях.

3.2.2. Система «Спектр» должна обладать возможностью отображения событий аудита в табличном виде со встроенной системой фильтрации с поиском по точному совпадению, по точному совпадению с отрицанием, по части строки, по части строки с отрицанием, по заданному регулярному выражению или режиму отрицания регулярного выражения.

3.2.3. Для всех колонок таблицы должны быть доступны сортировка и группировка данных.

3.2.4. Должна быть возможность экспорта всех или отфильтрованных событий аудита в формате PDF, XLSX, CSV или HTML.

3.2.5. Для каждого события аудита должна быть возможность просмотра детальной информации с возможностью её сохранения в файл формата PDF.

3.3. АНАЛИЗ И РАБОТА СО СТРУКТУРОЙ РЕСУРСОВ

3.3.1. Система «Спектр» должна с заданной периодичностью синхронизировать структуру защищаемых ресурсов и отображать её в виде дерева с указанием названия объектов, владельцев, даты последнего изменения и прав доступа к объектам.

3.3.2. Система «Спектр» должна позволять по запросу пользователя производить динамическую синхронизацию структуры конкретного каталога защищаемого ресурса для обновления его данных вне расписания синхронизации.

3.3.3. Система «Спектр» должна сохранять нескольких последних результатов сканирования защищаемых ресурсов (не менее 10) с возможностью последующего просмотра любого из них.

3.3.4. Система «Спектр» должна поддерживать и корректно отображать права доступа для каждого защищаемого ресурса.

3.3.5. Система «Спектр» должна предоставлять возможность фильтрации структуры защищаемых ресурсов по субъекту, объекту, правам доступа и другим дополнительным свойствам в зависимости от типа ресурса.

3.3.6. Система «Спектр» должна обладать возможностью построения двунаправленной модели прав доступа в виде «объект-субъекты» (список пользователей и групп и их права на объекты защищаемых ресурсов) или «субъект-объекты» (список объектов защищаемых ресурсов с правами у заданного пользователя или группы) с отображением результирующих прав для следующих защищаемых ресурсов:

- файловые сервера Windows, Linux;
- СХД DellEMC, NetApp, Synology, Huawei Dorado, Hitachi NAS;
- рабочие станции.

3.3.7. Система «Спектр» должна отображать права доступа на общих папках (Shared Permissions) с целью полного анализа результирующих привилегий для следующих защищаемых ресурсов:

- файловые сервера Windows, Linux;
- СХД DellEMC, NetApp, Synology, Huawei Dorado, Hitachi NAS;
- рабочие станции.

3.3.8. Система «Спектр» должна предоставлять возможность прямого изменения прав доступа из веб-интерфейса Системы «Спектр» для следующих защищаемых ресурсов:

- файловые сервера Windows, Linux;
- СХД DellEMC, NetApp, Synology, Huawei Dorado, Hitachi NAS.

3.3.9. Система «Спектр» должна предоставлять возможность виртуального моделирования последствий изменений в списки контроля доступа с учётом накопленной статистики по активности пользователей (кто и куда потерял бы доступ) и членства групп безопасности службы каталогов для следующих защищаемых ресурсов:

- файловые сервера Windows, Linux;
- СХД DellEMC, NetApp, Synology, Huawei Dorado, Hitachi NAS.

3.4. ВЫЯВЛЕНИЕ РИСКОВ

3.4.1. Система «Спектр» должна в автоматическом режиме выявлять и отображать риски для объектов файловых серверов (Windows, Linux), СХД (DellEMC, NetApp, Synology, Huawei Dorado, Hitachi NAS) и рабочих станций, связанные с настроенными правами доступа к данным, включая:

- неуправляемые папки/файлы;
- общедоступные папки/файлы;
- общедоступные папки/файлы для доменных пользователей;
- папки/файлы с выключенным наследованием;
- папки/файлы с неизвестными SID’ами;
- папки/файлы со сломанными ACL;
- папки/файлы с прямыми разрешениями;
- папки/файлы разрешениями из других доменов;
- папки/файлы с уникальными правами;
- скрытые папки/файлы.

3.4.2. Система «Спектр» должна предоставлять возможность кастомизации указанных рисков с целью добавления различных исключений и правил корреляции в зависимости от особенностей инфраструктуры, включая возможность фильтрации по:

- путям и названиям файла/папки;
- уровню вложенности;
- типу, размеру и владельцу;
- учётным записям;
- учётной записи владельца.

3.4.3. Система «Спектр» должна в автоматическом режиме выявлять и отображать риски для объектов MS Active Directory, связанные с особенностями настройки службы каталогов, включая:

- УЗ без пре-аутентификации Kerberos;
- УЗ не требующие пароля для входа;
- административные УЗ с включенным SPN;
- заблокированные УЗ;
- пустые группы;
- УЗ администраторов вне групп администрирования;
- нарушения целостности основной группы;
- группы с отключёнными учётными записями;
- УЗ с паролем без срока действия;
- УЗ с исходным при создании паролем;
- пустые организационные единицы.

3.4.4. Система «Спектр» должна предоставлять графическую репрезентацию следующих рисков и отчётов в виде связей между объектами службы каталогов:

- администраторы домена;
- доверительные отношения с доменом;
- компьютеры с неподдерживаемой операционной системой;
- объекты с правами DCSync;
- группы, содержащие объекты из другого домена;
- важные вершины.

3.4.5. Система «Спектр» должна в автоматическом режиме выявлять и отображать риски для объектов MS Exchange, связанные с настроенными правами доступа к почте, включая:

- уникальные права;
- общедоступные ящики/папки;
- права уровня «полный доступ»;
- права уровня «отправить как»;
- права уровня «отправить от имени».

3.4.6. Система «Спектр» должна в автоматическом режиме выявлять и отображать риски для объектов Confluence и Jira, связанные с настроенными правами доступа к пространствам, включая:

- анонимный доступ к пространствам.

3.5. КЛАССИФИКАЦИЯ ДАННЫХ

3.5.1. Система «Спектр» должна обладать возможностью классификации данных, распознавания изображений и выявления отсканированных документов без установки дополнительного ПО на следующих защищаемых ресурсах неструктурированных данных:

- файловые сервера Windows, Linux;
- СХД DellEMC, NetApp, Synology, Huawei Dorado, Hitachi NAS, NFS, SFTP;
- облачные хранилища NextCloud, VK WorkDisk;
- S3-совместимые объектные хранилища;
- рабочие станции;
- порталы SharePoint и SharePoint 365;
- системы базы знаний Atlassian Confluence;
- системы контроля заявок Atlassian Jira;
- системы совместной разработки BitBucket.

3.5.2. Классификация должна поддерживать анализ по словам, фразам, регулярным выражениям и словарям.

3.5.3. По результатам работы классификации файлы, попавшие под одну или несколько категорий, должны тегироваться без ограничений на количество категорий.

3.5.4. Система «Спектр» должна позволять просматривать результаты классификации с отображением расположения внутри древовидной структуры защищаемых ресурсов и возможностью их фильтрации по категориям.

3.5.5. Система «Спектр» должна обладать возможность предпросмотра текстовых форматов файлов (CSV, TXT, HTML и других), картинок (JPG, JPEG, GIF, BMP), офисных документов (XLSX, DOCX), PDF-файлов, а также аудио (MP3) и видео (WEBM, MP4) непосредственно из веб-интерфейса.

3.5.6. Система «Спектр» должна обладать возможность анализа результатов классификации с подсветкой места совпадения по правилам классификации в тексте файла (за исключением детектирования изображений на базе нейронных сетей).

3.5.7. Система «Спектр» должна обладать возможностью задания расписания классификации с возможностью указать максимальную длительность сканирования.

3.5.8. Повторно должны классифицироваться только те данные, которые были изменены или добавлены после предыдущего цикла классификации.

3.5.9. Система «Спектр» должна обладать возможностью настройки различных шаблонов и расписаний сканирования для разных защищаемых хранилищ.

3.5.10. Система «Спектр» должна включать следующие предустановленные категории информации для классификации:

- ИНН;
- паспорт;
- заграничный паспорт;
- СНИЛС;
- полис ОМС;
- номер телефона;
- кредитная карта;

- кредитная карта из 16 цифр;
- ОГРН;
- ОГРНИП;
- ОКВЭД;
- ОКПО;
- БИК;
- корреспондентский счет;
- расчетный счет;
- категории GDPR.

3.5.11. Система «Спектр» должна автоматически обнаруживать по словам, словосочетаниям, регулярным выражениям и энтропийным методам поиска как минимум следующие типы авторизационной информации:

- Amazon MWS Auth Token;
- AWS Access Key ID;
- AWS Account ID;
- AWS CLI credentials file;
- Contains a private key;
- Docker configuration file;
- Facebook access token;
- Facebook Secret Key;
- Github Key;
- Google Cloud API Key;
- Google OAuth Key;
- Linkedin Client ID;
- MailChimp API Key;
- netrc with SMTP credentials;
- NuGet API Key;
- Password Safe database file;
- PostgreSQL password file;
- Potential cryptographic private key;
- Potential Linux passwd file;
- Private SSH key;
- SSH Password;
- Username and password in URI.

3.5.12. Система «Спектр» должна обладать возможностью выделения текстовой информации из графических изображений (скан/фото документа).

3.5.13. Должно поддерживаться выделение текстовой информации из графических документов следующих форматов: BMP, JPEG, PNG, TIFF, включая анализ изображений данных форматов внутри документов MS Office и архивов с неограниченным уровнем вложенности.

3.5.14. Система «Спектр» должна обладать возможностью автоматической классификации (детектирования) на основе нейронных сетей для документов следующих типов:

- скан водительского удостоверения;

- скан кредитной карты;
- скан паспорта РФ;
- скан СНИЛС;
- скан паспорта Германии;
- скан паспорта Франции;
- скан паспорта Италии;
- скан паспорта США.

3.5.15. Система «Спектр» должна обладать возможностью добавления новых категорий документов для поиска шаблонов изображений.

3.5.16. Система «Спектр» должна обладать возможностью добавления новых категорий информации с помощью специального конструктора с использованием следующих параметров:

- слово/фраза с указанием минимального количества вхождений, близости, полного или частичного анализа и учёта регистра;
- словарь ключевых слов/фраз с возможностью их загрузки из файлов;
- путь, файл или расширение файла в виде точного поиска или регулярного выражения;
- регулярное выражение с указанием минимального количества вхождений, алгоритма валидации и возможностью проверки корректности выражения с помощью проверочного текста.

3.5.17. Конструктор правил должен позволять использовать любую комбинацию параметров с возможностью их логического объединения по «И» или «ИЛИ».

3.5.18. Система «Спектр» должна позволять классифицировать (проводить контентный анализ текстовой и графической информации на основании предустановленных и создаваемых пользователей категорий) документы следующих типов:

- Форматы документов MS Office:
  - OLE 2 Compound Document (MS Office 97);
  - Office Open XML (OOXML) (MS Office 2007 и выше).
- OpenDocument;
- PDF;
- RTF;
- XML и производные от него;
- HTML;
- EPUB;
- iWorks;
- форматы файлов с исходными кодами языков программирования:
  - C;
  - C++;
  - Java;
  - Groovy.
- форматы CAD-систем:
  - DWG.
- форматы архивов:
  - TAR;

- RAR;
- AR;
- CPIO;
- ZIP;
- 7ZIP;
- GZIP;
- BZIP2;
- XZ;
- Pack200.

3.5.19. Система «Спектр» должна обладать возможностью обработки документов и архивов, защищенных паролями, посредством автоматического подбора паролей по запросу пользователя с использованием предустановленных или загружаемых словарей паролей.

3.6. ПОЛЬЗОВАТЕЛЬСКИЕ МЕТКИ НА ОБЪЕКТЫ

3.6.1. Система «Спектр» должна обладать возможностью создания пользовательских меток через интерфейс.

3.6.2. Система «Спектр» должна обладать возможностью проставлять пользовательские метки на следующие типы защищаемых Системой объектов:

- пользователи;
- группы безопасности;
- каталоги (контейнеры) защищаемых ресурсов;
- файлы (конечные объекты) защищаемых ресурсов.

3.6.3. Факт наследования меток на нижерасположенные объекты должно задаваться пользователем на его усмотрение.

3.6.4. Система «Спектр» должна обладать возможностью автоматизированной загрузки меток через API к Системе.

3.6.5. Система «Спектр» должна обладать возможностью отображения и фильтрации по пользовательским меткам для:

- аудита доступа к данным;
- построения отчётов;
- настройки инцидентов (политик безопасности).

3.7. ТРЕБОВАНИЯ К МАРКИРОВКЕ ДОКУМЕНТОВ

3.7.1. Система «Спектр» должна предоставлять возможность маркировки документов сотрудниками, визуальному отображению этих меток при работе с файлом, наложения политики работы с файлами в зависимости от категории метки и аудита действий с промаркированными документами.

3.7.2. Система «Спектр» должна предоставлять возможность форсировать обязательную маркировку документов пользователями при их создании.

3.7.3. Маркировка должна осуществляться для любых типов файлов через контекстное меню проводника Windows, для офисных документов - с помощью надстройки MS Office, для писем - с помощью надстройки MS Outlook.

3.7.4. При работе с документами должны обеспечиваться настраиваемые политики ограничения действий сотрудников с файлами, письмами и метками, включая реакцию на:

- отправку письма без метки;
- отправку письма с заданной меткой;
- отправку письма с вложением без метки;
- отправку письма с уровнем метки ниже, чем вложения;
- сохранение документа без метки в приложении;
- попытку изменения заданной метки документа.

3.7.5. В качестве действий при срабатывании политики должны быть предусмотрены следующие реакции:

- разрешить;
- предупредить;
- запретить.

3.7.6. Система «Спектр» должна предоставлять возможность создания базовых меток и меток второго уровня, а также настраиваемые приоритеты между ними.

3.7.7. Сохранение меток должно осуществляться через запись в альтернативные потоки данных, а для офисных документов – дополнительно дублироваться в метаданные файла.

3.7.8. Метки должны сохраняться при копировании или перемещении документа.

3.7.9. Система «Спектр» должна обеспечивать отслеживание всех действий с метками в документах и письмах.

3.8. ПОВЕДЕНЧЕСКАЯ АНАЛИТИКА

3.8.1. Система «Спектр» должна обладать возможностью автоматического построения следующих типов статистических профилей:

- активность каждого сотрудника на защищаемых файловых хранилищах с учётом типов операций;
- активность на защищаемых файловых хранилищах целиком;
- активность каждого сотрудника на защищаемых файловых хранилищах с учётом категории информации.

3.8.2. На основании собранной информации Система «Спектр» должна обладать возможностью выявления аномальной активности сотрудников, на файловых хранилищах в целом и по отношению к данным определенных категорий.

3.8.3. Информация о зафиксированной аномалии должна включать в себя:

- дату и время обнаружения;
- УЗ сотрудника (для активностей сотрудников);
- имя файлового хранилища;
- количество аномальных операций;
- количество произведённых операций, их среднее и медианное значения;
- графическое представление обнаруженной аномалии.

3.8.4. Система «Спектр» должна обладать возможностью отправки уведомлений при выявлении аномальных активностей пользователей по следующим каналам: E-mail, Telegram, Syslog, HTTP, TCP/UDP, Splunk, ElasticSearch, Slack.

3.8.5. Система «Спектр» должна обладать возможностью запуска произвольного скрипта при выявлении аномальных активностей с автоматической передачей туда следующих параметров:

- уникальный идентификатор инцидента;
- тип инцидента;
- идентификатор файлового хранилища;
- файловые операции;
- количество файловых операций;
- медианное значение файловых операций;
- среднее значение файловых операций.

3.9. ОБЕСПЕЧЕНИЕ ПОЛИТИК БЕЗОПАСНОСТИ

3.9.1. Система «Спектр» должна обладать возможностью создания политик безопасности с целью оперативного реагирования на инциденты на основе следующих данных:

- событий аудита файловых хранилищ;
- событий аудита MS Active Directory;
- событий аудита MS Exchange;
- обнаруженных аномалий;
- информации о структуре папок и файлов защищаемых файловых хранилищ;
- информации о правах доступа к данным защищаемых файловых хранилищ.

3.9.2. Политика безопасности должна обладать возможностью настройки правил фильтрации, на основе которых будут выявляться отклонения от политик.

3.9.3. Политика безопасности должна обладать возможностью выявления цепочек событий с агрегацией по следующим параметрам:

- название защищаемого файлового хранилища;
- УЗ сотрудника;
- тип операции;
- статус операции;
- путь до объекта;
- название объекта;
- размер объекта (если доступно).

3.9.4. Для каждой цепочки событий в рамках политики безопасности должна быть возможность указания минимального количества событий и интервала времени, за который они происходят.

3.9.5. Для каждой политики безопасности должна быть возможность отправки уведомлений о срабатываниях политики по каналам E-mail, Telegram, Syslog, HTTP, TCP/UDP, Splunk, ElasticSearch, Slack, а также запуск произвольного скрипта.

3.9.6. Дополнительно на каждую политику для файловых хранилищ с установленным агентским ПО должна быть возможность настройки следующих активных реакций на выявленный инцидент:

- временный режим на чтение для папки/файла для всех пользователей;
- временный режим на чтение для папки/файла для данного пользователя;

- временный запрет доступа на папку/файл для всех пользователей;
- временный запрет доступа на папку/файл для данного пользователя.

3.10. СИСТЕМА ОТЧЁТНОСТИ

3.10.1. Система «Спектр» должна обладать встроенной подсистемой отчётности и включать в себя как предустановленные шаблоны, так и возможность настройки пользовательских отчётов.

3.10.2. Предустановленные отчёты должны содержать в себе следующие типы:

- Отчёты на основании аудита доступа к файлам и структуры хранилищ:
  - Файлы и папки, к которым не было обращений
  - Неиспользуемые ресурсы
  - Данные, определенного формата, кол-во файлов
  - Данные, определенного формата, объем файлов
  - Данные, нарушающие принятые правила
  - Топ файлов/почтовых сообщений
  - Топ дубликатов
  - Таймлайн активности с файлом
  - Рекомендации по сокращению прав
  - Статистика директорий по их размерам
  - Наиболее быстрорастущие папки
  - Время нахождения файлов в папке
  - Контроль уровня вложенности
  - Список файлов, с заданными условиями
  - Сводный отчёт по директории
  - Распределение файлов по расширениям
  - Распределение файлов по расширениям в графическом виде
  - Список файлов, у которых расширение не соответствует содержимому
- Отчёты по хранилищам:
  - Динамика заполнения свободного места хранилищ
  - Распределение событий по хранилищам
  - Список ресурсов, имеющих в ACL неизвестные SID’ы
  - Изменения в структуре хранилища за выбранный период
- Эксплуатационные:
  - Общая статистика системы
  - Список файлов/папок, информацию о которых не удалось прочитать
  - История сканирований хранилищ
  - Список хранилищ
  - Состояние агентов
  - Перенос данных
  - Распределение фоновых задач по времени
  - Схема комплекса
- Отчёты по рискам:
  - Папки/файлы с выключенным наследованием
  - Общедоступные папки/файлы

    - Папки/файлы с прямыми разрешениями
    - Папки/файлы со сломанным ACL
    - Уникальные права
    - Неуправляемые папки и файлы
    - Неизвестные SID'ы
    - Разрешения из других доменов
    - Скрытые директории и файлы
    - Доступ всем пользователям домена
    - Сводный отчёт по всем рискам и всем хранилищам
    - Динамика уровня информационной безопасности неструктурированных данных
    - Папки/файлы, доступ к которым имеет не только владелец файла
    - Пользовательские риски
- Отчёты на основании анализа Active Directory:
    - Отключенные учетные записи
    - Заблокированные учетные записи
    - Список сотрудников с постоянным паролем
    - Список неактивных учетных записей
    - Пустые организационные единицы (OU)
    - Пустые группы безопасности
    - Компьютеры
    - Членство пользователей в группах безопасности
    - Состав групп безопасности
    - Список сотрудников с истекающим паролем
    - Список групп в определенной OU
    - Элементы доменов с заданными условиями
    - Компьютеры с неподдерживаемой операционной системой
    - Пользователи, у которых пароль не менялся более N дней
- Отчёты по сотрудникам:
    - Определение "бизнес"-владельца файла
    - Кластеризация сотрудников по их действиям
    - Топ сотрудников
    - Бизнес-владелец ресурса
    - Назначенные бизнес-владельцы
- Отчёты по категориям:
    - Распределение файлов по категориям
    - Распределение файлов по категориям и хранилищам
    - Список файлов определенных категорий
- Отчёты по правам и разрешениям:
    - Параметры безопасности папок/файлов
    - Права доступа сотрудника
    - Права доступа группы
    - Список сотрудников, которые могут изменять права
    - Разрешения на папки или файлы

- Несоответствие фактических прав доступа, декларируемых по правилам именования групп
- Разница в параметрах безопасности за выбранный период

- Отчёты по квотам:
  - Квоты по томам (NTFS квоты)
  - Квоты для пользователей (NTFS квоты)
  - Квоты на директории (FSRM квоты)
- Отчёты по почтовым ящикам:
  - Список почтовых ящиков
  - Топ почтовых ящиков по размеру
  - Почтовые ящики, близкие к порогу квот

3.10.3. Должна быть возможность строить отчёты по любым срезам информации за любые временные промежутки.

3.10.4. Должна быть возможность экспорта табличных отчётов в форматы CSV, Excel, PDF, HTML.

3.10.5. Должна быть возможность автоматизированного построения отчётов по расписанию и отправки их на E-mail.

3.10.6. Должна быть возможность сохранения построенных отчётов на внешнюю сетевую папку с указанием авторизационной информации (логин/пароль).

3.11. СОГЛАСОВАНИЕ И ПРЕДОСТАВЛЕНИЕ ПРАВ ДОСТУПА К РЕСУРСАМ

3.11.1. В Системе должен быть предусмотрен веб-портал самообслуживания по запросу / отзыву прав доступа с автоматическим исполнением заявок.

3.11.2. Система «Спектр» должна поддерживать роли, необходимые для автоматизации процесса назначения и согласования прав: Администратор, Владелец данных, Авторизатор (согласующее лицо) и Пользователь.

3.11.3. Администраторы должны иметь возможность назначить Владельца данных на любой каталог файловых серверов с неструктурированным данным.

3.11.4. Система «Спектр» должна предоставлять интерфейс Владельцам данных для периодической проверки корректности текущих прав доступа к ресурсам с возможностью добавления или удаления сотрудников в интерактивном режиме.

3.11.5. Система «Спектр» должна предоставлять возможность администраторам назначать на ресурс цепочку согласующих лиц (Авторизаторов) с указанием уровня согласования, включая возможность назначить нескольких согласующих на один и тот же уровень.

3.11.6. Авторизаторы должны иметь возможность работы с заявкой на доступ, представленной в наглядном виде, для принятия решения по этой заявке (одобрить, отклонить, изменить).

3.11.7. Система «Спектр» должна предоставлять возможность администраторам назначать одного или нескольких заместителей для каждого сотрудника-авторизатора, а Авторизаторам – самостоятельно активировать и деактивировать данный список заместителей на время своего отсутствия.

3.11.8. Пользователи Системы «Спектр» (все сотрудники компании) должны иметь возможность подать заявку на предоставление доступа через Web-интерфейс Системы «Спектр» с возможностью отслеживания статуса своих заявок.

3.11.9. Система «Спектр» должна поддерживать режим работы как с существующими группами безопасности, указанными в правах доступа к каталогам, так и возможность создавать и добавлять в права доступа новые группы безопасности непосредственно через интерфейс Системы «Спектр».

3.11.10. Система «Спектр» должна предоставлять возможность назначения прав доступа начиная с конкретной даты и с указанием срока действия выдачи привилегий. По истечении указанного срока Система «Спектр» должна автоматически аннулировать права доступа и отправить соответствующие уведомления по электронной почте.

3.11.11. Система «Спектр» должна поддерживать автоматическую генерацию уведомлений по электронной почте: при создании заявки – Авторизатору, при любом изменении статуса заявки – Пользователю, подавшему эту заявку.

3.11.12. После прохождения последнего этапа авторизации необходимые изменения в службе каталогов должны вноситься автоматически без необходимости выполнения ручных операций.

3.11.13. Система «Спектр» должна позволять создавать новые каталоги в структуре файловых серверов прямо из интерфейса Системы «Спектр» и назначать на неё группы безопасности для последующего управления доступом.

3.11.14. Все заявки на доступ, поступившие в Систему «Спектр», и результаты рассмотрения заявок должны сохраняться в электронном журнале с возможностью поиска по фильтрам.

3.12. ПЕРЕНОС И УДАЛЕНИЕ ДАННЫХ ХРАНИЛИЩ

3.12.1. Система «Спектр» должна обладать возможностью создания автоматизированных правил по удалению или переносу данных на файловых серверах (Windows, Linux), СХД (DellEMC, NetApp, Synology, Huawei Dorado, Hitachi NAS), рабочих станциях, порталах SharePoint.

3.12.2. Переносу или удалению данных должны подвергаться файлы, подпадающие под одну из категорий:

- Произвольные файлы, с возможностью указания следующих фильтров:
  - хранилище данных;
  - путь до файла;
  - имя файла;
  - категории;
  - риски;
  - размер;
  - владелец;
  - временной промежуток (дней), в который не было изменений файла;
  - форматы файлов;
  - пользовательские метки;
  - максимальный уровень вложенности.
- Дубликаты файлов, с возможностью указания следующих фильтров:
  - хранилище данных;

- путь до файла;
- имя файла;
- категории;
- размер;
- форматы файлов.

- Неиспользуемые ресурсы, с возможностью указания следующих фильтров:
  - характеристика, по которой определяется отсутствие использования файла (аудит событий или дата модификации файла);
  - хранилище данных;
  - путь до файла;
  - имя файла;
  - размер;
  - временной промежуток в днях, за который не было изменений или обращений к файлу.

3.12.3. Процесс переноса или удаления данных должен происходить в автоматическом режиме разово или по указанному расписанию.

3.12.4. Должна быть возможность просмотра состояния, редактирования или удаления правил переноса или удаления данных.

3.12.5. При переносе данных должна быть возможность указания следующих опций:

- целевой путь, куда будет осуществляться перенос;
- сохранение относительного пути;
- сохранение изначальных ACL;
- создание «Readme» файла на месте перемещаемого файла с указанием информации о том, куда осуществляется перенос;
- перемещение групп доступа к неиспользуемому ресурсу в отдельный OU.

3.12.6. Система «Спектр» должна осуществлять журналирование всех событий удаления или переноса данных и предоставлять статистическую информацию о количестве и размеру обработанных файлов.

3.13. ПОИСК ПО СОДЕРЖИМОМУ ФАЙЛОВ

3.13.1. Система «Спектр» должна предоставлять функционал поиска по содержимому файлов, расположенных на файловых серверах (Windows, Linux), СХД (DellEMC, NetApp, Synology, Huawei Dorado, Hitachi NAS, NFS, SFTP), облачных хранилищах (NextCloud, VK WorkDisk), S3-совместимых объектных хранилищах, рабочих станциях, порталах SharePoint и SharePoint 365, системах Confluence, Jira и BitBucket.

3.13.2. Процесс выделения текстового содержимого из файлов различных форматов должен осуществляться Системой согласно заданному расписанию.

3.13.3. Поиск должен поддерживаться по всем форматам документов, описанных в разделе 3.5.18.

3.13.4. По выделенной текстовой информации должны быть доступны следующие виды поиска:

- поиск по слову;
- поиск по нескольким словам:
- поиск по фразе;
- поиск по фразе с учётом расстояния между словами;

- поиск с использованием подстановочных знаков (учёт морфологии);
- поиск с использованием логических операторов и группировки.

3.13.5. Система «Спектр» должна предоставлять возможность фильтрации поисковых запросов по следующим параметрам:

- хранилище данных;
- полный путь, имя и расширение файла;
- категории;
- размер;
- автор.

3.13.6. Результатом любого из видов поиска должен быть набор файлов, удовлетворяющих условиям поиска, с указанием их названия, места нахождения (хранилище, полный путь) и другой вспомогательной информации.

3.13.7. Отображаемые результаты должны учитывать реальные разрешения пользователя к данным и показывать только те файлы, к которым у него есть права доступа.

3.13.8. Система «Спектр» должна предоставлять возможность экспорта результатов в формате PDF, XLSX, CSV или HTML.

3.13.9. Система «Спектр» должна предоставлять возможность назначения пользовательских меток на результаты поиска.

3.13.10. Система «Спектр» должна предоставлять возможность быстрого перехода к анализу структуры прав доступа и просмотру событий с каждым конкретным файлом из результатов поиска.

4. ТРЕБОВАНИЯ К АДМИНИСТРИРОВАНИЮ СИСТЕМЫ

4.1. ИНТЕРФЕЙС ПОЛЬЗОВАТЕЛЯ

4.1.1. Графический интерфейс оператора Системы «Спектр» должен быть выполнен в виде веб-приложения.

4.1.2. Доступ к интерфейсу должен осуществляться с использованием одного из следующих веб-браузеров:

- Google Chrome версии 60.0.3112 и выше;
- Mozilla Firefox версии 52 и выше;
- Microsoft Edge;
- Яндекс.Браузер версии 17.6.1 и выше.

4.2. ТРЕБОВАНИЯ К УПРАВЛЕНИЮ ДОСТУПОМ

4.2.1. Доступ к графическому интерфейсу Системы «Спектр» должны иметь только авторизованные пользователи с настроенными ролями.

4.2.2. Каждому пользователю должна назначаться одна роль.

4.2.3. Каждая роль должна настраиваться гранулярно с помощью следующих параметров:

- функциональные возможности (страницы интерфейса продукта);
- уровень доступа к каждой странице (просмотр или управление);
- доступные хранилища;
- доступные домены;
- возможность предпросмотра содержимого документов.

4.2.4. Система «Спектр» должна поддерживать как внутреннюю базу пользователей, так и интегрироваться со службой каталогов.

4.2.5. Система «Спектр» должна позволять производить настройки безопасности входа, включая:

- время неактивности в интерфейсе до автоматического выхода;
- время действия пароля;
- количество попыток ввода пароля до блокировки;
- длительности блокировки;
- количество анализируемых последних паролей при его смене;
- минимальная длина пароля;
- использование в пароле символов в верхнем и нижнем регистрах, цифр и спец символов;
- принудительная смена пароля при первом входе.

4.2.6. Система «Спектр» должна поддерживать технологию Single Sign-On (SSO) для авторизации.

4.3. ТРЕБОВАНИЯ К МОНИТОРИНГУ И ОПЕРАЦИОННОМУ КОНТРОЛЮ

4.3.1. Система «Спектр» должна предоставлять следующую диагностическую информацию:

- суммарная загрузка Системы «Спектр»;
- загрузка процессора;
- использованной оперативной памяти;
- занимаемое место на жестком диске.

4.3.2. Система «Спектр» должна обладать возможностью сбора диагностической информации с защищаемых ресурсов через интерфейс Системы «Спектр».

4.3.3. Система «Спектр» должна обладать возможностью сбора диагностической информации и предоставления данных о состоянии каждого компонента и статуса каждой задачи, запускающийся по расписанию.

4.3.4. Все действия пользователей внутри Системы «Спектр» и все системные события должны заноситься в соответствующие журналы с возможностью автоматизированной отправки через Telegram, Syslog, HTTP, TCP/UDP, Splunk, ElasticSearch и Slack.

4.3.5. Данные в журналах не должны автоматически удаляться по истечении срока давности в целях избежания потерь важной для администратора Системы «Спектр» информации.