Аналитическое сравнение российских систем SGRC (Security Governance, Risk and Compliance)

Один из ключевых вызовов современной российской кибербезопасности - дефицит кадров. Это ограничение сложно устранить даже в среднесрочной перспективе, оно препятствует и реализации проектов по импортозамещению, и эффективному реагированию на актуальные киберугрозы, и выполнению требований законодательства. Традиционным ответом является замещение ручного труда средствами автоматизации, которые вдобавок еще и помогают ускорить все процессы, систематизировать подходы к решению задач, устранить субъективность при принятии решений, повысить контролируемость и прозрачность операций. Кроме того, возможность автоматизации рутины привлекает не только с экономической точки зрения, но и с перспективы удержания специалистов, которых проще замотивировать творческими задачами нежели однотипными действия.

В кибербезопасности, несмотря на относительную молодость направления, есть немало процессов, которые хотя бы частично можно поручить системам автоматизации: учет и инвентаризация активов, сканирование на наличие уязвимостей и их оценка, учет и управление изменениями и конфигурациями, проведение аудитов и оценок соответствия, учет документов и их версий, анализ и декомпозиция требований законодательства и корпоративных регламентирующих норм, анализ киберрисков и т.д. Для автоматизации этих и многих других процессов ИБ используются системы класса GRC/SGRC - обзор их основных свойств и сценариев применения мы уже делали ранее. Настал черёд провести аналитическое сравнение отечественных продуктов данного класса, которые позволяют автоматизировать управление процессами ИБ, киберрисками, соответствием требованиям по защите информации.

На российском рынке до 2022 года встречались такие зарубежные GRC-решения, как Archer (бывший RSA Archer), IBM OpenPages, SAP GRC, SAS GRC, ServiceNow GRC и ряд других. По понятным причинам, мы не смогли включить их в обзор. Кроме того, есть и Open Source решение GRC Eramba, которое, однако, не поддерживает русский язык и не содержит базы российских законодательных требований, хотя может быть использовано для управления ИБ по международным стандартам и лучшим практикам. Для данного аналитического сравнения мы выбрали следующие российские on-prem (локальные) решения класса SGRC:

- АльфаДок
- R-Vision SGRC
- Securitm
- Security Vision SGRC

Методология оценки и сравнения функциональных возможностей продуктов включала в себя разработку перечня основных критериев, которые были сформированы авторами обзора анализа открытых источников с информацией о характеристиках продуктов, по результатам обратной связи от заказчиков указанных классов решений, а также руководствуясь экспертизой авторов. Вендорам рассылались опросники с перечнем основных критериев по их продуктам для заполнения, при этом формат некоторых вопросов предполагал развернутые ответы. Кроме ответов от вендоров, производился опрос выделенных вендорами экспертов по продуктам, проводилась оценка характеристик и функционала решений на live-демонстрациях решений, на основе предоставленных производителями доступов к демонстрационным стендам, на основе работы с референсными площадками (клиенты, интеграторы, эксперты-консультанты), которые предоставляли свои мнения и данные об используемых продуктах Производителям также предлагалось добавить свои расширенные критерии сравнения для включения их в обзор, с проведением второй итерации сравнения по уже расширенному перечню критериев. В перечень вопросов также был включен пункт о планах развития функционала продукта, куда вендоры могли включать пункты из своих "Дорожных карт развития продуктов", при этом в ответах на критерии не учитывался функционал, который на момент проведения опроса не был реализован, а был лишь запланирован.

Концепция SGRC-решений предполагает, что автоматизируются сразу несколько процессов кибербезопасности, поэтому в обзор были включены критерии, характеризующие работу рассматриваемых решений в более широких областях, таких как управление операционными рисками, защита КИИ, управление непрерывностью бизнеса, а также оценивались перспективные направления - использование методов обработки Big Data, машинного обучения, искусственного интеллекта.

В настоящем обзоре используются следующие термины и определения:

- Решение – SGRC-система для управления стратегией, документами и процессами ИБ (Governance), киберрисками (Risk Management), соответствием требованиям (Compliance).
- Модули решения – модуль управления стратегией, документами и процессами ИБ; модуль управления киберрисками; модуль управления соответствием требованиям.
- Объекты решения – активы, конфигурации, уязвимости, заявки, задачи, требования, аудиты, документы, инциденты ИБ, киберриски.
- Low-code – метод разработки программного обеспечения, при котором разработка упрощается за счет использования графического конструктора, при этом частичное написание кода требуется.

- No-code – метод разработки программного обеспечения, при котором разработка выполняется за счет использования графического конструктора, написание кода не требуется.

Основные критерии

Название продукта, производителя	АльфаДок ООО “НПЦ “КСБ”	R-Vision SGRC ООО “Р-Вижн” Демонстрируется версия 5.4, заявленный вендором срок выхода: Q1 2025	Securitm ООО “Секьюритм”	Security Vision SGRC ООО “Интеллектуальная безопасность”
1. Общие технические характеристики				
1.1. Технические требования к платформе и среде внедрения решения (системные требования к аппаратному и программному обеспечению, окружению);	ОС: Debian 11, Rocky 9, Альт 8, Redos-MUROM-7.3.2. Необходимые предустановленные пакеты: docker, docker-compose, xz, tz-data. Аппаратные требования (при количестве пользователей до 10): 4 ЦПУ, 8 Гб ОЗУ, 250 Гб дискового пространства.	ОС: CentOS 7.5 - 7.9; RHEL 7.7 - 8.8, 9.0 - 9.2; Debian 10.x - 12.5; Oracle Linux 8.6 - 8.8; Rocky Linux 8.6 - 8.8; Astra Linux SE 1.6 - 1.8; Astra Linux CE 2.12; RED OS 7.3; RED OS 7.3c; SberLinux 8.6-9.3; ALT Server 10 (p 10.x); ALT 8 SP Server (c 8.2); Ubuntu 18.04 - 22.04; Rosa 12.5.1. СУБД: PostgreSQL 14, Jatoba J4, Tantor 14. Для установки All-in-one (БД и коллектор на одном сервере): Минимальные требования: от 6vCPU 2 ГГц, 16 Гб ОЗУ, от 100 Гб дискового пространства.	CPU: 4-12 ядер; RAM: 8-16 ГБ; SSD: 100 ГБ; ОС: Astra Linux, РЕД ОС, МОС ОС, Ubuntu, CentOS и т.д., Docker; CPU: 4-12 ядер; RAM: 8-16 ГБ; SSD: 100 ГБ; СУБД: MySQL версии 8.	ОС: CentOS Stream 8 и выше, RHEL 8 и выше, Ubuntu 20.04/22.04/24.04, AlmaLinux 9, Debian 10/11/12, Oracle Linux 8/9, Astra Linux SE 1.7.3 и выше, Альт Сервер 10 и выше, Альт 8 СП, AlterOS 7.5, РЕД ОС 7/8, РОСА «ХРОМ» или Microsoft Windows Server 2016 R2 и выше. СУБД: Microsoft SQL Server версии 2016 или выше, PostgreSQL версии 11 или выше, Postgres Pro версии 11 или выше, Jatoba. Аппаратные требования: От 8 ЦПУ, 12 Гб ОЗУ, 100 Гб дисковой подсистемы.
1.2. Варианты поставки и инсталляции (аппаратный апплайнс, образ, контейнер, установка на “голое железо”, установка on-prem, установка в облаке, наличие графических инсталляторов, поддержка виртуализации);	Поддерживается работа из «облачной» веб-консоли и локальная (on-prem) установка. Поддерживается установка дистрибутива из командной строки.	Варианты: on-prem, виртуализация, контейнер. Поддержка виртуализации: VMware, MS Hyper-V, Xen, Parallels, VirtualBox	Варианты поставки: - Облачная версия; - Локальная версия (установка on-prem).	Поддержка установки в виде контейнера, на голое железо, из ISO образа, из RPM-пакетов, из графического инсталлятора и из командной строки. Поддержка систем виртуализации (VMware, VirtualBox, Hyper-V, Xen, Parallels, KVM). Поддерживается установка в облаке и on-prem.
1.3. Архитектурные особенности решения (стек технологий, возможность прямого доступа к внутренним структурам, возможность доступа покупателя к ОС/СУБД решения с правами администратора);	Поддерживается работа из «облака» и on-prem установка.	Распределенная архитектура: сервер управления (управление системой, инвентаризация, хранение информации), коллекторы (сканеры). Используются СУБД PostgreSQL 14, Jatoba J4.	Набор Docker контейнеров. Стек технологий: Nginx/Angie, MariaDB, PostgreSQL, REDIS, PHP, JS, node.js. Доступ к внутренним структурам ОС/СУБД решения.	Возможность отдельной установки выделенного сервера коннекторов (для взаимодействия с интегрируемыми системами), не требующего прямого соединения с основной базой данных решения. Взаимодействие всех компонент по защищенным протоколам сетевого доступа. Наличие административного доступа к компонентам решения. Используемые сторонние компоненты: Elasticsearch, RabbitMQ, IIS / NGINX, MSSQL / PostgreSQL / Postgres Pro / Jatoba.
1.4. Параметры масштабируемости, кластеризации, производительности;	Не поддерживается	Поддерживается установка дополнительных компонентов (коллекторов и серверов) в распределенной инфраструктуре. Поддерживается повышение производительности через увеличение доступных процессоров и оперативной памяти.	Для распределения нагрузки СУБД может быть вынесена на отдельный сервер. Реализуется за счет функционала ОС и СУБД.	Поддерживается балансировка нагрузки между компонентами, возможность установки неограниченного количества нод каждого компонента решения с целью горизонтального масштабирования, возможность установки каждого компонента решения на выделенный сервер.
1.5. Поддержка отказоустойчивости (реализация, требования вендора к инфраструктуре покупателя);	Не поддерживается	Реализуется за счет функционала ОС и СУБД Поддерживается Active-Passive кластер приложений на базе VRRP и кластер базы данных PostgreSQL.	Частично. Реализуется за счет функционала ОС и СУБД.	Поддерживается. Создание кластера высокой доступности с автоматическим переключением в случае сбоя, дублирование и резервирование всех элементов решения, возможность создания геокластера, поддержка отказоустойчивости для провайдеров MSS.
1.6. Поддержка распределенной установки компонентов, включая возможность размещения СУБД на отдельной ноде;	Не поддерживается, все компоненты устанавливаются на одном сервере.	Поддерживается установка БД на отдельном сервере, установка коллекторов на отдельных серверах.	Не поддерживается	Поддерживается возможность установки неограниченного количества нод каждого компонента.
1.7. Возможность работы решения в различных сетевых сегментах, включая частично изолированные, через отдельные ноды решения;	Не поддерживается	Поддерживается	Не поддерживается	Поддерживается возможность установки компонентов решения (сервисов) на выделенные серверы в удаленных и изолированных сетях, с дальнейшим импортом результатов сканирования на основной сервер.

Название продукта, производителя	АльфаДок ООО “НПЦ “КСБ”	R-Vision SGRC ООО “Р-Вижн” Демонстрируется версия 5.4, заявленный вендором срок выхода: Q1 2025	Securitm ООО “Секьюритм”	Security Vision SGRC ООО “Интеллектуальная безопасность”
1.8. Обеспечение безопасной работы решения (ограничение доступа, ролевая модель, ограничение используемых сетевых портов, защита канала связи, защита обрабатываемых данных, журналирование, способы аутентификации пользователей, контроль действий пользователей решения, шифрование критичных данных, контроль целостности исполняемых и вспомогательных файлов, возможность создания резервных копий, корректная обработка ошибок настройки решения);	Поддержка ролевой модели доступа с разграничением доступа на уровне организаций и назначением прав доступа к определенным разделам и выполнению шагов в них. Поддерживается ведение истории действий с учетными записями пользователей.	Шифрование трафика между компонентами решения с помощью TLS. Ролевая модель доступа, дискреционный доступ, аутентификация пользователей (локальная, SSO). Поддерживается логирование изменений, вносимых пользователями. Применяется шифрование учетных данных, сохраненных в системе.	Поддерживается: - Ограничение доступа к приложению по белым спискам IP адресов; - Ролевая модель; - Доступ по HTTPS; - Хеширование парольной информации в БД; - Журналирование операций в приложении с фиксацией прошлых и новых значений; - Использование локальных или доменных учетных записей (доменная аутентификация); - Двухфакторная аутентификация; - Возможность включения Captcha (облачная версия); - Настройка парольных политик; - Есть режим отладки; - Есть автоматическая отправка ошибок производителю.	Поддерживается ограничение доступа на основе IP-адресов, двухфакторная аутентификация, аутентификация по сертификатам для пользователей и компонентов решения (самоподписанные сертификаты, сертификатов от внутреннего центра сертификации), наличие SSO. Используется SSL/TLS для защиты доступа к веб-интерфейсу, поддерживается аудит попыток входа в систему, аудит действий пользователей и администраторов (включая факт просмотра карточек). Поддерживается контентно-ролевая модель управления доступом ко всем элементам решения (RBAC+ABAC). Поддерживается шифрование базы данных и отдельных критичных элементов (например, паролей для учетных записей). Система выполняет проверку целостности ПО и конфигурационных файлов во время функционирования и по команде пользователя. Система выполняет мониторинг состояния всех своих компонентов (сервисов) и выполняет оповещения пользователя при выявлении отклонений. Резервное копирование реализуется средствами ОС и СУБД. Ошибки решения доступны для просмотра в консоли решения с различным уровнем детализации.
1.9. Встроенная помощь в интерфейсе решения;	Поддерживаются подсказки и контекстная справка в интерфейсе решения.	Поддерживается	Поддерживается: - Встроенная Справка; - Подсказки в интерфейсе.	Поддерживается: - встроенные html руководства с видеозаписями; - контекстная помощь в веб-интерфейсе; - подсказки при заполнении различных форм (с возможностью кастомизации в рамках веб-интерфейсных настроек).
1.10. Локализация интерфейса, поддержка мультиязычности, возможность кастомизации интерфейса (включая темы, цветовые схемы), возможность сквозного поиска по всем обрабатываемым данным.	Поддерживается русский язык, сквозной поиск отсутствует, кастомизация интерфейса не поддерживается.	Частично поддерживается: сквозной поиск работает только в пределах определенного раздела решения, темы (темная, светлая) поддерживаются, кастомизация логотипа поддерживается.	Поддерживается только русский язык. Есть сквозной поиск по всем модулям системы.	Поддерживается мультиязычность, локализация интерфейса и всех элементов на русском и английском с возможностью добавления других языков. Поддерживаются темы (темная и светлая), кастомизация интерфейса (брендирование, логотип). Поддерживается сквозной поиск.
2. Общие организационные характеристики				
2.1. Дата первого релиза, текущая версия;	Дата первого релиза – 2014 год, текущая версия – 167.	Первый релиз – 2015 год. Демонстрируется версия 5.4, заявленный вендором срок выхода: Q1 2025.	Первый релиз 19.04.2021. Текущая версия: 2.3.1259.	Первый релиз – 2015, текущая версия – 5.
2.2. Наличие документации, наличие API;	Документация в виде PDF, взаимодействие с решением по API не поддерживается.	Документация поставляется с ПО, API документирован	Поддерживается встроенная справка. Есть API.	Документация в виде интерактивной справки в решении, в виде PDF-файлов, поддержка API. Предоставляется документация на API.
2.3. Наличие технической поддержки, режим работы, SLA-нормативы;	Пакеты технической поддержки «Лайт» и «Эксперт». Поддержка предоставляется по рабочим дням с 8 до 18 (по Московскому времени).	Варианты технической поддержки: Стандартная, Расширенная 24/7, Премиальная, Премиум Плюс (выделенный специалист).	Базовая техническая поддержка через портал ServiceDesk и электронную почту. Расширенная техническая поддержка через персональные чаты в мессенджерах, выделенный инженер. Режим работы 8x5. SLA от 4 часов до 3 дней в зависимости от формата поддержки и критичности запроса. Бесплатная поддержка через раздел «Отправить идею» на портале Community версии.	Техническая поддержка четырех уровней: Базовая, Стандартная, Расширенная, Премиальная. Премиальная - 24/7. Показатели SLA для тарифа «Премиальный»: время реакции: 4 часа, время предоставления решения: 24 часа. Поддерживается возможность согласования и подписания сжатых SLA-нормативов и условий предоставления услуг, индивидуальное ведение.
2.4. Наличие гарантии, срок предоставления гарантийного обслуживания, что включено в стандартное гарантийное обслуживание, возможность расширенной гарантии;	Поддерживается консультирование по функционалу, доступ к Базе знаний, участие в обучающих вебинарах по эксплуатации решения и по защите информации.	Предоставляется в соответствии с условиями гарантийного обслуживания на основании договора или сертификата на клиентскую (гарантийную) поддержку.	Гарантийная и техническая поддержка составляют 1 год и включены в стоимость продукта. Пролонгация со второго года при покупке технической поддержки. Возможно приобретение поддержки сразу на несколько лет. Есть базовая и расширенная поддержка.	Стандартное гарантийное обслуживание на 1 год: - личный кабинет с маркетплейсом экспертного контента, дистрибутивов платформы, окружения, ОС, модулями и обновлениями; - прием заявок через портал, телефон и эл. почта (кол-во обращений не ограничено); - предоставление консультаций по ВКС, телефону и email; - консультации по: настройке и администрированию программных продуктов, диагностике и сбора информации для определения неисправностей в работе программных продуктов, применению решений по устранению неисправностей и восстановлению работы программных продуктов.

Название продукта, производителя	АльфаДок ООО “НПЦ “КСБ”	R-Vision SGRC ООО “Р-Вижн” Демонстрируется версия 5.4, заявленный вендором срок выхода: Q1 2025	Securitm ООО “Секьюритм”	Security Vision SGRC ООО “Интеллектуальная безопасность”
2.5. Лицензионная политика: стоимость дополнительных интеграций (ИТ/ИБ-системы, СЗИ, внешние сервисы и т.д.), лицензирование API, правила расчета лицензии (по пользователям, активам, интеграциям и т.д.), отличие в стоимости при разных вариантах инсталляции, специальные условия для MSS-провайдеров.	Отдельно лицензируется on-prem установка, существуют отдельные тарифы.	Предоставляется по запросу.	Публичный прайс на сайте производителя.	Предусмотрены временные и бессрочные лицензии. Метрики лицензирования: 1) Количество конкурентных лицензий коннекторов для подключения к внешним системам; 2) Режим функционирования (количество дополнительных нод) – отказоустойчивость, режим мультинод; 3) Мультиарендность для MSSP провайдеров, холдингов, групп компаний. 4) Количество сканируемых IP-адресов (узлов) – применяется только для модулей: VS и SPC. 5) Количество обрабатываемых событий в секунду – применяется только для модулей NG SOAR, TIP, UEBA. Других ограничительных метрик не предусмотрено. Количество активов, пользователей, сценариев, отчетов и дашбордов – все входит в неограниченном количестве. API и конструкторы не лицензируются дополнительно, включены в любую поставку решения.
2.6. Опыт внедрений;	Множество внедрений в различных отраслях. Перечень заказчиков имеется на сайте разработчика.	Опыт внедрения во многих отраслях экономики.	Публичные кейсы: Евраз, Лента, Администрация Санкт-Петербурга, Банки.ру, Протек.	Опыт внедрения во многих отраслях экономики. Среди Заказчиков – Сбербанк России, Альфа-Банк, Тинькофф Банк, РосБанк, Норильский Никель, Северсталь, Уралхим, Евраз, ТГК-1, X5 Group, Магнит, ФСО России, Совет Федерации, ДомРФ, Мегафон MSSP, Центр киберустойчивости Angara SOC, РТ-Информационная безопасность (РОСТЕХ), МТС, Вымпелком, Первый Канал и другие.
2.7. Наличие в реестре российского ПО;	Зарегистрирован в Реестре российского ПО.	Зарегистрирован в Реестре российского ПО.	Зарегистрирован в Реестре российского ПО.	Зарегистрирован в Реестре российского ПО.
2.8. Наличие сертификатов регуляторов.	Отсутствует	Демонстрируется версия 5.4. Версия 5.3 сертифицирована ФСТЭК России по УД4.	Отсутствует	Заключение 8 Центра ФСБ России 149/3/6/908 от 01.10.2024; Сертификат соответствия ФСТЭК России № 4574 от 02.09.2022 (УД4); Сертификат соответствия ОАЦ при Президенте Республики Беларусь BY/112 02.02. ТР027 036.01 01673 от 6 декабря 2024 года (по требованиям технического регламента ТР 2013/027/BY).
3. Общий функционал				
3.1. Настройка правил и логики управления объектами решения;	Поддерживается только заложенная производителем логика и правила работы с объектами.	Поддерживается кастомизация правил и логики управления объектами решения.	Система состоит из модулей. Модули состоят из объектов. Объекты одного и различных модулей могут быть связаны друг с другом.	Поддерживается настройка правил и логики управления всеми объектами решения (включая произвольные пользовательские типы объектов) через графический low-code / no-code конструктор объектов.
3.2. Настройка и управление жизненным циклом объектов решения, возможность выполнять действия (автоматически, вручную) или диагностировать проблемы на каждом этапе жизненного цикла каждого объекта;	Не поддерживается перенастройка жизненного цикла объектов решения. Большинство действий выполняется после команд пользователя (формирование документов, отчетов, перерасчет оценок соответствия и т.д.).	Поддерживается	Частично. Создавать, изменять, архивировать/ удалять объекты можно вручную или автоматически.	Поддерживается настройка жизненного цикла объектов решения через графический low-code / no-code конструктор рабочих процессов. Поддерживаются автоматические и ручные действия. Настраивается расписание, частота, параметры действий. Поддерживается ведение истории выполненных действий по всем объектам с возможностью диагностики проблем.
3.3. Возможность создания пользовательских типов объектов с кастомизацией свойств;	Не поддерживается	Поддерживается	Частично. Поддерживается, в модуле активов.	Поддерживается создание произвольных типов объектов с любыми свойствами. Поддерживается создание произвольных типов объектов с любыми свойствами с применением подхода low-code / no-code. Созданные пользовательские типы объектов могут использовать во всех процессах, ролевой модели, дашбордах и т.д..
3.4. Поддержка ведения и отображения истории изменений объектов и их свойств;	Поддерживается ведение общей истории выполненных действий, сформированных документов.	Поддерживается	История изменений всех объектов журналируется, с сохранением прошлых и текущих значений. Доступ к журналам возможен как из карточек объектов или из общего журнала изменений.	Поддерживается, возможна настройка ведения истории изменений объектов с детализацией до каждого свойства. Наличие фильтра для поиска истории изменения свойств.
3.5. Дедупликация объектов решения с возможностью настройки механизма и правил дедупликации;	Не поддерживается	Частично поддерживается только для оборудования (активы). Настройка дедупликации выполняется только «под капотом», пользователь не может сам поменять логику дедупликации.	Частично. Механизм объединения активов с настройкой полей для сопоставления и типов активов, по которым проводится объединение.	Поддерживается дедупликация данных, тонкая настройка правил дедупликации на основании любых свойств объектов решения и их комбинаций. Определение условий применения правил дедупликации.
3.6. Поддержка выполнения автоматических и ручных действий с объектами: добавление, удаление, изменение, включая массовые операции;	Поддерживается выполнение ручных действий (добавление, удаление, изменение), включая массовые.	Поддерживается	Поддерживаются: - Ручные действия с объектами; - Массовые операции; - Автоматические действия с объектами через модуль RPA.	Поддерживаются автоматические действия и автоматические массовые операции. Поддерживаются ручные действий и ручные массовые операции. Поддерживается создание произвольных типовых массовых сценариев изменения объектов. Поддерживается разграничение доступа пользователей к выполнению тех или иных массовых типовых сценариев над объектами.
3.7. Импорт настроек, контента, документов, стандартов, требований НПА и ОРД (форматы csv, xlsx, json, xml, yaml и т.д.);	Поддержка импорта данных об активах в форматах: json из ПО «АРМ-сканер», Excel (xls, xlsx, csv), AIDA64 (xml).	Импорт настроек и контента в формате xlsx, импорт документов в любых форматах.	Поддерживается импорт реестров активов в xls, импорт уязвимостей в xls и xml, импорт документов в json и xls, импорт файлов (в качестве вложений) в любых форматах.	Поддерживается импорт данных любых типов объектов решения в форматах csv, json, xml, включая импорт документов в оригинальном формате. Поддерживается импорт настроек в формате json.

Название продукта, производителя	АльфаДок ООО “НПЦ “КСБ”	R-Vision SGRC ООО “Р-Вижн” Демонстрируется версия 5.4, заявленный вендором срок выхода: Q1 2025	Securitm ООО “Секьюритм”	Security Vision SGRC ООО “Интеллектуальная безопасность”
3.8. Экспорт настроек, контента, документов, стандартов, требований НПА и ОРД (форматы csv, xlsx, json, xml, yaml, docx, ods, odt, txt, pdf, html и т.д.);	Поддерживается экспорт документов в xls, xlsx, csv, pdf, doc, docx. Поддерживается экспорт изображения в формате SVG.	Поддерживается экспорт отчетов показан (docx, xlsx, pptx, odt, pdf). Для json, csv поддерживается выгрузка отчетов через API. Форматы xml, yaml не поддерживаются.	Поддерживается экспорт реестров в csv, xls, json, xml, экспорт карточек и отчетов в docx, экспорт схем в png.	Поддерживается экспорт в форматах pdf, docx, odt, xlsx, ods, csv, txt, json.
3.9. Поддержка протоколов и механизмов для доступа к внешним системам: API, HTTPS, IMAP / SMTP, LDAP, RPC, SMB, SOAP, SSH, WMI и т.д.;	Не поддерживается	Поддерживаются протоколы и механизмы: CMD, PowerShell, LDAP, MS SQL, MySQL, Oracle DB, PostgreSQL, Python, REST, SNMP, SOAP, SSH	API, HTTP/HTTPS, IMAP/SMTP, LDAP, SMB, ICMP, SSH, RPC.	Поддерживается подключение к Linux, Windows, сетевым устройствам с помощью протоколов и механизмов REST API, SOAP, HTTP / HTTPS, WinRM, RPC, SNMP, SSH, LDAP, WMI, IMAP/SMTP, подключения к СУБД (MSSQL, MySQL, Oracle, PostgreSQL), SMB.
3.10. Возможность интеграции, включая двухстороннюю, с системами класса CMDB / ITAM, IDM, ITSM / ServiceDesk / Ticketing, BPM / ERP, SIEM / SOAR / TIP, VM / EASM, DLP / DCAP / DAG, службами каталогов, другими системами (указать);	Не поддерживается	Поддерживаются интеграции с SIEM (двусторонние), NGFW, IDS/IPS, VM, SOAR, TIP, антивирусным ПО, системами ITSM, ITAM, Service Desk, базами данных и другими системами. По умолчанию доступно более 30 готовых интеграций. Возможно создание кастомных интеграций.	Прямые интеграции с Active Directory, Kaspersky Security Center, Dr.Web, Zabbix, NetBox, Solar Dozor, Scan Factory, Cloud Advisor, Kaspersky ASAP, Vulns.io, Meta Scan, Staffcop, MaxPatrol VM, Manage Engine, Jira, Telegram, Почтовые серверы. Импорт отчетов от сканеров уязвимостей Qualys, Nessus, RedCheck, Nmap, OpenVas, Kaspersky, XSpider, AppScreener, OWASP ZAP, MaxPatrol 8, Manage Engine. Настраиваемые интеграции по API.	Поддерживается интеграция с Security Vision BCP, Security Vision RM/ORM, Security Vision CM, Security Vision UEBA, Security Vision AD + ML. Поддерживается интеграция с Any.Run, Kaspersky KATA, PT Sandbox, PT NAD, Trend Micro Deep Discovery Analyzer (DDA), Cisco StealthWatch, Zabbix, Microsoft Exchange, Veeam Backup, Check Point, Cisco ASA, Cisco Firepower, Cisco Switch, Juniper, Fortigate, Kaspersky Security Center, Microsoft Defender, TrendMicro DDA, Kaspersky OpenTIP, FireEye, Symantec Endpoint Protection Manager, Palo Alto, TrendMicro IMSVA, CMDB iTop, MS SCCM, MS WSUS, Kaspersky Security Center (подключение к БД и OpenAPI), Infoblox (IPAM), Skybox, SearchInform, Lansweeper, MaxPatrol 8, MaxPatrol SIEM, Kaspersky KUMA, IBM QRadar, Pangeo RADAR, RuSIEM, NEURODAT SIEM, ArcSight SIEM, Splunk, Symantec CSP, VMware vCenter, VMware vROps, Proxmox, Hyper-V, HP OneView, Cisco UCS, Symantec Endpoint Protection Manager, Efros Config Inspector, Microsoft Endpoint Configuration Manager, Ovirt, NetBox, Active Directory, OpenLDAP, FreeIPA, Astra Linux Directory, ALD Pro, One Vision SD, Jira, Naumen Service Desk, MicroFocus Service Manager (HP Service Manager), BPM Online (Creatio), OTRS, Redmine и другими системами.
3.11. Поддержка совместной работы над документами и требованиями, коллективное внесение правок и замечаний с учетом организационно-штатной структуры (например, подчиненный не может изменять правки руководителя и т.д.);	Поддерживается ролевая модель доступа с разграничением прав при выполнении действий, заполнении документов, создании отчетов.	Поддержка совместной работы над контентом в системе.	Частично. В рамках одного документа (набора требований) разные пользователи могут одновременно обрабатывать разные требования.	Поддерживается совместная работа с любыми карточками объектов. Поддерживаются чаты по задачам (заявкам), уязвимостям, активам, несоответствиям. Поддерживается ведение организационно-штатной структуры организации и назначение полномочий пользователей решения в соответствии с ней.
3.12. Поддержка параллельного независимого выполнения действий с объектами решения;	Частично поддерживается. Действия, затрагивающие свойства нескольких объектов, рекомендовано выполнять последовательно (например, формирование или обновление портфеля документов).	Не поддерживается	Частично. К объектам можно параллельно добавлять заметки, задачи, устанавливать связи с объектом из других объектов. Редактировать основные параметры объекта параллельно нельзя.	Поддерживается, максимальное число параллельных задач ограничено вычислительной мощностью используемой аппаратной платформы.
3.13. Работа с карточкой объекта: кастомизация полей, добавление комментариев, вложений и тегов, настройка отображаемых полей, настройка внешнего вида карточки в зависимости от пользователя или группы, возможность скрытия полей и их значений для различных пользователей или групп;	Поддерживается кастомизация создаваемых документов: настройка шапки документов, внешнего вида и оформления заголовков, наличия или отсутствия дат и номеров документов, вариантов написания некоторых слов (приказ или распоряжение) и т.д.	Поддерживается кастомизация карточки объекта.	Частично. Можно создавать собственные поля различного типа (строка, число, флаг, список, дата, связь, файл, счетчик), задавать полям различные свойства и валидации, в том числе настраивать их отображение или скрытие.	Поддерживается произвольная кастомизация карточек объектов по требованиям пользователя (добавление полей, элементов, вкладок, элементов управления и т.д.). Поддерживается настройка прав доступа к объектам и их свойствам, скрытие конфиденциальной информации (например, определенных свойств активов).
3.14. Наличие, функционал, кастомизация средств отправки и получения оповещений (электронная почта, мессенджеры, встроенные в решение средства и т.д.);	Частично. Поддерживается отправка уведомлений в интерфейсе решения, через email.	Поддерживается оповещение по email, через встроенную панель уведомлений, через Telegram.	Каналы уведомлений: электронная почта, Telegram, уведомления внутри приложения. Есть компонент мониторинга и уведомления об ошибках в приложении (память, процессор, интеграции, очереди задач и т.п.) Есть возможность настройка кастомных уведомлений через модуль RPA.	Поддерживается отправка оповещений через веб-интерфейс решения (включая звуковое оповещение), мессенджеры (Telegram, eXpress), электронную почту, через API к любой системе.
3.15. Наличие базы шаблонов оповещений;	Поддерживается частично, заложены шаблоны уведомлений подведомственных организаций, шаблоны документов для отправки регуляторам (КИИ, ГИС, ПДн).	Поддерживается	Не поддерживается	Имеется база типовых оповещений по ключевым событиям. Поддерживается возможность расширения шаблонов оповещений.
3.16. Настройка правил отправки оповещений (например, при обнаружении уязвимости, изменении свойств актива, принятом решении по киберриску и т.д.);	Не поддерживается	Поддерживается	Настройка отправки оповещений по любым событиям и изменениям в системе, по расписанию и т.п. через модуль RPA.	Поддерживается через настройку рабочих процессов в графическом low-code / no-code конструкторе.
3.17. Поддержка сквозного поиска, фильтрации, сортировки по свойствам объектов решения, возможность сохранения созданных фильтров и поисковых запросов;	Не поддерживается. Есть фильтрация выводимых данных.	Частично поддерживается: сквозной поиск работает только в пределах определенного раздела решения	Сквозной глобальный поиск по всем модулям и объектам. Сохранение фильтров в глобальном поиске. Локальный поиск в рамках отдельных реестров. Сортировка по полям объектов в реестрах.	Поддерживается сквозной поиск, фильтрация с применением множества различных логических (И, ИЛИ) выражений и операторов (содержит, больше, входит и др.) и вложенности. Поддерживается возможность сохранять фильтры.
3.18. Поддержка выполнения действий с объектами по расписанию;	Не поддерживается	Поддерживается настройка расписаний выполнения скриптов, запуска сканирований и коннекторов.	Да, через модуль RPA или настройки интеграций.	Поддерживается, любые действия, реализованные с использованием механизмов коннекторов или рабочих процессов, а также рассылки отчётов. Возможность тонкой настройки расписания для каждого отдельного действия.
3.19. Задание временных интервалов и расписаний, в течение которых действия с объектами не выполняются (ставятся на паузу автоматически);	Не поддерживается	Частично поддерживается через статусы объектов для аудитов и рисков.	Не поддерживается	Поддерживается формирование расписаний, “запрещенных” временных интервалов. Дополнительно поддерживается возможность использования произвольных Стоп-выражений.

Название продукта, производителя	АльфаДок ООО “НПЦ “КСБ”	R-Vision SGRC ООО “Р-Визи” Демонстрируется версия 5.4, заявленный вендором срок выхода: Q1 2025	Securitm ООО “Секьюритм”	Security Vision SGRC ООО “Интеллектуальная безопасность”
3.20. Возможность приостановки или полной остановки действий с объектами по команде оператора или автоматически при выполнении определенных условий (например, при ошибках аутентификации);	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается выполнение ручной приостановки, остановки действий (по команде пользователя) и автоматической приостановки, остановки действий (через настройку рабочих процессов в графическом low-code / no-code конструкторе).
3.21. Возможность задания таймаута, после которого действия с объектом останавливаются с записью ошибки таймаута и отправкой оповещения оператору;	Не поддерживается	Частично поддерживается через статусы объектов для аудитов и рисков.	Не поддерживается	Поддерживается, с настройками таймаутов, а также количества повторений при получении ошибки. Оповещение отображается в консоли, отправляется через email или мессенджеры, по API в любую совместимую систему.
3.22. Поддержка выполнения ручных или автоматических действий при выполнении задаваемых пользователями условий (например, изменение свойства объекта, входящее email-сообщение с определенным текстом, наступление даты и т.д.).	Не поддерживается	Частично поддерживается через статусы объектов для аудитов и рисков.	Поддерживается через модуль RPA, реагирование на создание/изменение/архивирование/удаление различных объектов с расширенными параметрами для настройки условий сработки.	Поддерживается выполнение ручных и автоматических действий при наступлении заданных условий через настройку рабочих процессов в графическом low-code / no-code конструкторе.
3.23. Поддержка формирования документов (опросников, таблиц, карточек, формуляров и т.д.) для офлайн-заполнения (в сетях без доступа к интернет) с дальнейшим импортом в решение;	Поддерживается	Частично поддерживается: формирование документа (опросников, таблиц, карточек и т.д.), экспорт в формате xlsx.	Приоритетно механизмы коммуникации построены на Модуле опросов, который позволяет онлайн собирать любую информацию с участников процесса. Можно выгружать реестры в xls/csv, заполнять их и импортировать обратно в систему.	Поддерживается за счет импорта и экспорта данных в файл (в форматах csv, json, xml). Поддерживается офлайн-заполнение опросных листов, методик оценки, формирование стандартов, выполнение сбора информации.
3.24. Поддержка совместной работы ИБ / ИТ / бизнес-подразделений: чат, оповещения, возможность обработки email и приложенных файлов;	Частично, за счет встроенных информационных сообщений в интерфейсе решения.	Поддерживается чат, оповещения, возможность отправки и обработки электронной почты.	Частично, за счет модуля опросов, в котором можно коммуницировать с ИТ и бизнес-подразделениями, не пуская их в систему. В модуле задач есть возможность ставить задачи не пользователям системы, собирать с них статус и результаты выполнения задач.	Поддерживаются чаты по задачам (заявкам), уязвимостям, активам, несоответствиям. Поддерживается отправка оповещений через веб-интерфейс решения, электронную почту, мессенджеры (Telegram), через API к любой системе. Поддерживается парсинг входящих email с обработкой вложений.
3.25. Поддержка интеграции с АСОИ (ФинЦЕРТ), ГосСОПКА (НКЦКИ);	Не поддерживается	Встроенный сервис, обеспечивающий двухстороннюю интеграцию с ФинЦЕРТ и ГосСОПКА.	Не поддерживается	Поддерживается отправка уведомлений в ФинЦЕРТ (через АСОИ), в НКЦКИ (через ГосСОПКА). Поддерживается работа с сообщениями НКЦКИ, ФинЦЕРТ с получением и обработкой оповещений, бюллетеней.
3.26. Возможность управления объектами решения через API;	Не поддерживается	Да, public API для разделов системы.	Поддерживается, есть API, позволяющий создавать и изменять объекты в системе.	Поддерживается создание и изменение любых объектов, а также поддерживается вызов любых сценариев обработки объектов.
3.27. Возможность настройки прав доступа при взаимодействии с объектами решения через API.	Не поддерживается	Применяются права пользователя, который делает запрос через API.	Поддерживается ограничение доступа к API по белым спискам IP адресов. Поддерживается создание API токенов с разными правами (чтение, чтение и запись).	Поддерживается. Настройка прав доступа к объектам и действиям через API – базируется на аналогичных возможностях, которые используются для предоставления доступа пользователям.
4. Управление стратегией, документами и процессами ИБ (Governance)				
4.1. Поддержка автоматизации различных процессов ИБ: управление активами, конфигурациями, уязвимостями, инцидентами ИБ, киберрисками, аудитами ИБ, соответствием (НПА и ОРД), управление непрерывностью бизнеса, заявками, задачами, документами, поддержка формирования модели угроз, модели нарушителя и сценариев реализации угроз, отчетность, визуализация состояния ИБ, другие (указать);	Поддерживается автоматизация процессов управления активами, уязвимостями, инцидентами ИБ, аудитами ИБ, соответствием (НПА и ОРД), заявками, задачами, документами. Поддерживается формирование модели угроз, модели нарушителя и сценариев реализации угроз. Поддерживается формирование отчетности, визуализации состояния ИБ.	Поддержка управления активами, аудитами ИБ, управление свидетельствами аудита, киберрисками, соответствием (НПА и ОРД), планирование и контроль задач, управление документацией, защитными мерами, моделирование угроз, модель нарушителя, сценарии реализации угроз, бюджет и обоснование, отчетность, метрики состояния ИБ. Для решения смежных ИБ-задач (управление инцидентами, уязвимостями и т.д.) в экосистеме R-Vision представлены другие продукты.	Система состоит из модулей - Управление активами; - Управление рисками; - Контроль соответствия требованиям (Compliance); - Управление уязвимостями (VM); - Управление защитными мерами; - Управление задачами; - Опросы и заявки; - Автоматизация процессов (RPA); - Управление метриками. Управление аудитами реализуется через комбинацию модулей Соответствия, Активов и Опросов. Управление инцидентами ИБ реализуется через комбинацию модуля активов и RPA. Управление угрозами, модель нарушителя, сценарии реализации угроз являются частью модуля рисков. Отчетность и визуализация присутствуют в каждом модуле.	Поддерживаются «из коробки» процессы управления активами, уязвимостями, конфигурациями, изменениями, непрерывностью бизнес-процессов, киберрисками (включая операционные риски по 716-П), аудитами, соответствием международным и российским стандартам (в том числе 187-ФЗ), документами, задачами, заявками (тикетинг), инцидентами, моделирование угроз и нарушителей. Поддерживается формирование любых пользовательских процессов ИТ/ИБ через настройку рабочих процессов в графическом low-code / no-code конструкторе.
4.2. Поддержка выбора предпочтительного ИБ-фреймворка (ISO 27000 series, COBIT, NIST CSF, CIS Critical Security Controls и т.д.) с отображением декомпозированных требований и рекомендаций, с передачей данных в модуль управления соответствием требованиям (Compliance);	Поддерживаются стандарты, методики, документы: Методический документ «Методика оценки угроз безопасности информации» (утвержден ФСТЭК России 05.02.2021 г.).	Встроенная база фреймворков аудитов (ISO 27000 series, NIST, ГОСТ 57580.2-2018, PCI DSS, SWIFT, GDPR и др.), фреймворков рисков (COBIT, ISO 27000 series, FAIR, РС БР ИББС-2.2-2009 и др.), каталоги защитных мер (CIS Critical Security Controls, Приказы ФСТЭК №17, №21, №239, меры защиты из БДУ ФСТЭК 2024) Возможность добавлять собственные фреймворки и каталоги.	В базе Модуля управления соответствием множество российских и международных стандартов (нормативных документов), декомпозированных на требования. Требования всех стандартов скоррелированы между собой.	Поддерживаются стандарты, методики, документы (и их декомпозиции): Методический документ «Методика оценки угроз безопасности информации» (утвержден ФСТЭК России 05.02.2021 г.), ISO 27000, NIST Cybersecurity Framework 2.0, CIS Critical Security Controls v.8, ГОСТ Р 57580, PCI DSS 4.0. Поддерживается возможность добавлять собственные фреймворки и каталоги.

Название продукта, производителя	АльфаДок ООО “НПЦ “КСБ”	R-Vision SGRC ООО “Р-Вижн” Демонстрируется версия 5.4, заявленный вендором срок выхода: Q1 2025	Securitm ООО “Секьюритм”	Security Vision SGRC ООО “Интеллектуальная безопасность”
4.3. Поддержка выбора применимых высокоуровневых норм законодательства (152-ФЗ, 187-ФЗ, 98-ФЗ, 149-ФЗ и т.д.) с отображением декомпозированных требований и рекомендаций, с передачей данных в модуль управления соответствием требованиям (Compliance);	Поддерживаются документы: Федеральный закон №152-ФЗ, Федеральный закон №187-ФЗ, Приказ ФСТЭК России от 14 марта 2014 г. № 31, Приказ ФСТЭК России от 11 февраля 2013 г. № 17, Приказ ФСТЭК России от 18 февраля 2013 г. № 21, Приказ ФСТЭК России от 25 декабря 2017 г. № 235, Приказ ФСТЭК России от 21 декабря 2017 г. № 239.	Поддерживается, по умолчанию доступны нормативные документы различных уровней (152-ФЗ, 187-ФЗ, 149-ФЗ, Приказы ФСТЭК №17, №21, №31, №239, Приказ ФСБ № 378, ГОСТ 27001-2021, ГОСТ 57580, 716-П, 719-П, 802-П, 683-П, 821-П и др.).	Аналогично предыдущему пункту.	Поддерживаются документы: Федеральный закон № 98-ФЗ Федеральный Закон № 149-ФЗ Приказ ФАПСИ № 152 Федеральный Закон № 152-ФЗ Федеральный закон № 572-ФЗ Федеральный закон № 63-ФЗ Федеральный Закон № 161-ФЗ Федеральный закон № 126-ФЗ Федеральный Закон № 187-ФЗ Приказ ФСБ России № 367 Приказ ФСБ России № 378 Приказ ФСБ России № 796 Приказ ФСБ России № 368 Приказ ФСБ России № 282 Приказ ФСБ России № 196 Приказ ФСБ России № 77 Приказ ФСБ России № 281 Приказ ФСТЭК России № 31 Приказ ФСТЭК России № 17 Приказ ФСТЭК России № 76 Приказ ФСТЭК России № 239 Приказ ФСТЭК России № 75 Приказ ФСТЭК России № 235 Приказ ФСТЭК России № 21 ГОСТ Р 59547-2021 Приказ 66 ОАЦ Приказ Роскомнадзора № 179 Приказ Роскомнадзора № 996 Приказ Роскомнадзора № 178 Указ Президента РФ № 166 Постановление Правительства РФ № 211 Постановление Правительства РФ № 1272 Постановление Правительства РФ № 676 Указ Президента РФ № 250 Постановление Правительства РФ № 1912 Постановление Правительства РФ № 1478 Постановление Правительства РФ № 883 Постановление Правительства РФ № 1119 Постановление Правительства РФ № 687 Постановление Правительства РФ № 584 Постановление Правительства РФ № 127 Постановление Правительства РФ № 820 Приказ Минцифры № 453 Приказ Минздрава № 911н PCI SSF – PCI Secure Software Standard v1.2.1 PCI DSS 4.0 PCI SSF – PCI Secure SLC Standard v1.1 NIST Cybersecurity Framework 2.0 ГОСТ Р ИСО/МЭК 27001—2021 ГОСТ Р ИСО 22301—2021 ИСО/МЭК 27001-2022 E ИСО 22301:2019 E CIS Critical Security Controls v7.1 CIS Critical Security Controls Version 8 GDPR ГОСТ Р 57580_1-2017 ГОСТ Р 57580_3-2022 ГОСТ Р 57580_4-2022 Положение Банка России 683-П Положение Банка России 716-П Положение Банка России 719-П Положение Банка России 757-П Положение Банка России 779-П Положение Банка России 787-П Положение Банка России 802-П Положение Банка России 808-П Положение Банка России 821-П Положение Банка России 822-П Положение Банка России 833-П
4.4. Отчетность ИБ: разнообразные виды и форматы выгрузки отчетов (doc, pdf и т.д.), возможность создания стратегических, оперативных, тактических, аналитических отчетов для различных групп потребителей решения, возможность отправки отчетов автоматически и по запросу по электронной почте, через мессенджеры и т.д.;	Поддерживается формирование отчетов в форматах pdf, docx, xlsx. Поддерживается формирование следующих типов отчетов: эксплуатируемые объекты информатизации, специалисты по защите информации, сотрудники, полнота сбора согласий на обработку ПДн, принятые к учету ИСПДн, ГИС и объектах КИИ, используемое для обработки информации программное обеспечение, используемые средства защиты информации, назначенные ответственными лица, состояние разработки, утверждения и актуальности документации по защите информации, последнее отправленное уведомление в Роскомнадзор, планирование мероприятий по защите информации, реквизиты исходящих и входящих документов во ФСТЭК России с результатами категорирования объектов КИИ, степень готовности к проверкам регуляторов. Поддерживается формирование пользовательских отчетов по ответственным лицам, ИСПДн, ГИС и объектам КИИ, средствам защиты информации, техническим средствам.	Встроенная база официальных форм отчетности (PCI Council Prioritized Approach Report, положение о применимости контролей, отчёт по форме 0403202, отчётность по ГОСТ 57580 (лист сбора свидетельств, отчет по результатам оценки соответствия ЗИ), отчётность КИИ (акт проверки объекта КИИ, акт о категорировании объекта КИИ, сведения о присвоении категории объекту КИИ) и др.). Поддержка форматов pdf, xlsx, docx, pptx, odt, и др).	Поддерживаются отчеты в формате doc о соответствии требованиям выбранных документов (стандартов). Специализированные отчеты по ГОСТ 57580 и 8/12МР, положения о применимости. Выгрузка архивов со свидетельствами аудита. Отчеты о соответствии в разрезе различных областей (scopes), паспорта областей, паспорта активов. Реестры рисков, мер, активов, уязвимостей в xls, csv. Возможность автоматической выгрузки реестров активов на сетевые шары.	Поддерживается формирование отчетов в форматах pdf, docx, odt, xlsx, ods. Поддерживается отображение состояния объектов (активов, уязвимостей, несоответствий) в отчетах различного типа с элементами визуализации (таблицы, графики, диаграммы, географическая карта и т.д.).

Название продукта, производителя	АльфаДок ООО “НПЦ “КСБ”	R-Vision SGRC ООО “Р-Вижн” Демонстрируется версия 5.4, заявленный вендором срок выхода: Q1 2025	Securitm ООО “Секьюритм”	Security Vision SGRC ООО “Интеллектуальная безопасность”
4.5. Визуализация состояния ИБ: дашборды (стратегические, оперативные, тактические, аналитические), диаграммы (лепестковые, гистограммы, круговые и т.д.), виджеты («светофоры», «спидометры» и т.д.), функционал «drill down»;	Поддерживается отображение состояния ИБ на виджетах (дашборды, таблицы). Функционал “drill down” не поддерживается.	Дашборды в различных разрезах. Карта мира, планы помещений, схемы взаимосвязей. Конструктор отчетов. Функциональность “drill down”. Графики типа “Топ-... объектов”.	Поддерживаются встроенные дашборды в каждом модуле системы. Отдельный Модуль метрик, позволяющий конструировать дашборды по любой логике на базе данных, имеющихся в системе, с функцией drill down. Возможность собирать данные для метрик через модуль опросов. Возможность создавать отдельные группы дашбордов и публиковать их по ссылке (например, для размещения на мониторе). Встроенные в модули дашборды выполняют функцию фильтров (BI).	Поддерживается отображение состояния ИБ на виджетах (линейный график, столбчатая диаграмма, круговая диаграмма, спидометр, таблица, географическая карта), на графах связей, на дашбордах, в отчетах. Во всех графических элементах поддерживается функционал «drill down» для непосредственного перехода от визуальных элементов к данным, на основании которых было построено графическое отображение.
4.6. Возможность пользовательской настройки элементов визуализации (дашборды, виджеты) с настройкой отображения под каждого пользователя или группы, поддержка сохранения пользовательской настройки отображения, поддержка брендирования (фирменные логотипы, шрифты, цветовая гамма компании).	Поддерживается добавление виджетов из списка предустановленных.	Поддерживается пользовательская настройка элементов визуализации, настройка по каждому разделу системы для групп пользователей, возможность брендировать интерфейс.	На странице “Мои дела” каждый пользователь может создать персональный набор дашбордов и виджетов. Дашборды можно привязать и отображать в реестрах активов. У дашбордов настраивается стиль. Поддерживается брендирование системы – можно задать свой логотип, иконку, шрифты и цвета.	Поддерживается настройка произвольных графических элементов индивидуально под каждого пользователя и сохранение настроек.
5. Управление киберрисками (Risk Management)				
5.1. Формирование моделей угроз и нарушителя по методологиям ФСТЭК России, PASTA, DREAD, VERIS, STRIDE, MITRE ATT&CK, другие (указать);	Поддерживается формирование моделей угроз и нарушителя по методологии ФСТЭК России («Методика оценки угроз безопасности информации»).	Поддерживается. Встроенные: МУ ФСТЭК 2015, МУ ФСТЭК 2021.	Поддерживается построение модели угроз и нарушителя по методике ФСТЭК. Реестр актуальных угроз с оценкой величины рисков по каждой угрозе.	Поддерживается формирование моделей угроз и нарушителя по методологиям ФСТЭК России, MITRE ATT&CK.
5.2. Формирование моделей угроз и нарушителя по методологиям вендора (кратко описать), поддержка кастомизации предустановленных методологий, поддержка создания пользовательской методологии;	Частично. Поддерживается ограниченная перенастройка встроенной методологии оценки угроз ФСТЭК России.	Модель угроз формируется путем автоматического отбора актуальных угроз на основе заполнения экспертами опросников по источникам и предпосылкам.	Настраиваемая качественная методика оценки рисков, баллы или проценты, с учетом ущерба, вероятности, приоритета актива.	Поддерживается изменение предустановленных и создание пользовательских методологий моделирования угроз и нарушителей.
5.3. Построение сценариев реализации угроз ИБ;	Поддерживается частично	Не поддерживается	Поддерживается частично	Поддерживается, по методологиям ФСТЭК России, MITRE ATT&CK.
5.4. Использование каталогов БДУ ФСТЭК России, MITRE ATT&CK, OWASP, другие (указать);	Поддерживается использование каталогов БДУ ФСТЭК России.	Поддерживается частично.	Поддерживается частично. Встроенные каталоги MITRE ATT&CK, БДУ ФСТЭК).	Поддерживаются каталоги БДУ ФСТЭК России, MITRE ATT&CK.
5.5. Использование вендорских (кратко описать) и пользовательских каталогов угроз;	Поддерживается добавление пользовательских значений в справочники негативных последствий, объектов воздействий, видов воздействия, возможных нарушителей, техногенных источников, возможных способов реализации угроз.	Каталог на базе собственной экспертизы R-Vision, поддержка пользовательских каталогов.	Встроенный каталог рисков, угроз, уязвимостей, типов активов. Возможность использовать готовые объекты или создавать собственные.	Поддерживается создание пользовательских каталогов угроз.
5.6. Связь моделирования угроз и нарушителя с процессом управления киберрисками;	Не поддерживается	Частично. Поддерживается связь угроз и нарушителей, но не процессов.	Оценка актуальных угроз является следствием процесса оценки рисков.	Поддерживается. Функционал оценки рисков базируется на результатах моделирования угроз по методике ФСТЭК России.
5.7. Поддержка управления киберрисками по методологиям ГОСТ/ISO 27005, ГОСТ/ISO 31000, NIST RMF, FAIR, OCTAVE, TARA, другие (указать);	Не поддерживается	Поддерживается ГОСТ/ISO 27005, ГОСТ/ISO 31000, NIST, FAIR, OCTAVE, ALE, методология оценки угроз ФСТЭК Россиию	Поддерживается частично. Наиболее близкий подход - ISO 27005.	Поддерживаются стандарты, методики, документы: Методический документ «Методика оценки угроз безопасности информации» (утвержден ФСТЭК России 05.02.2021 г.), ГОСТ Р ИСО 31000-2019, ГОСТ Р ИСО/МЭК 27005-2010, ISO 27005:2022, методика FAIR (Factor Analysis of Information Risk). Поддерживается проведение качественной, количественной оценки рисков кибербезопасности по методике вендора. Поддерживается моделирование рисков методом Монте-Карло.

Название продукта, производителя	АльфаДок ООО “НПЦ “КСБ”	R-Vision SGRC ООО “Р-Вижн” Демонстрируется версия 5.4, заявленный вендором срок выхода: Q1 2025	Securitm ООО “Секьюритм”	Security Vision SGRC ООО “Интеллектуальная безопасность”
5.8. Поддержка выполнения этапов оценки и анализа киберрисков: идентификация активов, уязвимостей, угроз и последствий их реализации, формирование и согласование плана обработки киберрисков, контроль выполнения плана;	Не поддерживается	Поддерживается	Поддерживается: 1. Формирование реестра рисков. Вручную или путем заполнения мастера, с учетом имеющихся в организации типов активов. 2. Формирование реестра защитных мер, которые уже снижают риски или будут это делать после внедрения. 3. Из связи мер с рисками формируется План обработки рисков. 4. Защитные меры внедряются, процесс сопровождается использованием модуля задач. В результате риски пересчитываются.	Поддерживается весь жизненный цикл процесса управления рисками: - Этап определения среды с использованием ресурсно-сервисной модели, система позволяет детально описать бизнес и ИТ-компоненты инфраструктуры. - Этап идентификации рисков с помощи методологии ФСТЭК России с моделированием угроз и с применением обширной базы данных уязвимостей. - Этап анализа и оценки рисков с использованием качественного и количественного методов оценки (самостоятельно или с помощью заполнения опросных листов). - Этап обработки рисков с моделированием различных конфигураций мер защиты с целью выбора оптимального набора по соотношению затрат и эффективности, с создаванием и управлением задачами обработки рисков. - Этап мониторинга и пересмотра рисков с использованием механизма ключевых индикаторов риска и функционалом переоценки рисков.
5.9. Реализация плана обработки киберрисков: формирование заявок, задач, документов в решении, экспорт во внешние системы ITSM / ServiceDesk / Ticketing, отправка и получение уведомлений;	Не поддерживается	Частично поддерживается: поддерживается формирование плана обработки рисков, заявок, задач.	План обработки основывается на модуле защитных мер, в котором идет учет уже внедренных и планируемых к внедрению активностей. Вокруг защитных мер формируются задачи (модуль задач), автоматизации (модуль RPA), метрики. Задачи могут направляться во внешние системы, через прямую интеграцию с Jira или кастомные интеграции по API (модуль RPA).	Поддерживается формирование заявок, задач, документов на обработку рисков с работой через веб-интерфейс решения, мессенджеры (Telegram), электронную почту, через API к любой системе, включая One Vision SD, Jira, Naumen Service Desk, MicroFocus Service Manager (HP Service Manager), BPM Online (Creatio), OTRS, Redmine.
5.10. Поддержка выбора способов обработки рисков (принять, избежать, минимизировать, передать), учет уровней остаточного риска, риск-аппетита, толерантности к риску;	Не поддерживается	Поддерживается	Поддерживается частично. Поддерживается механизм принятия рисков. Все остальные способы реализуются через связку рисков с защитными мерами, которые влияют на величину ущерба или вероятности риска. Оценивается первичный, текущий и остаточный уровни риска. Есть уровень риск аппетита, который можно настраивать.	Поддерживаются стандартные варианты обработки рисков, поддерживается создание пользовательских способов и методов обработки. Поддерживается возможность создания кастомизированных формул расчета уровней остаточного риска, риск-аппетита, толерантности к риску.
5.11. Интеграция процесса управления киберрисками с другими процессами ИБ (управление активами, уязвимостями, соответствием, обновлениями, конфигурациями, инцидентами ИБ и т.д.);	Не поддерживается	Поддерживается интеграция процесса управления киберрисками с активами.	Риски отображаются в карточках активов, которые являются источником рисков. Процесс управления уязвимостями (VM) является источником для процесса управления рисками. С управлением соответствием риски пересекаются через защитные меры, которые используются в обоих модулях.	Поддерживается интеграция киберрисков со всеми процессами, настроенными в решении, с учетом взаимосвязей и взаимных зависимостей объектов решения.
5.12. Связь киберрисков с защитными мерами, с моделированием их применения и оценкой эффективности снижения уровня киберрисков;	Не поддерживается	Поддерживается	Частично. Защитные меры являются базовым механизмом снижения рисков. Одна мера может снижать несколько рисков и выполнять ряд требований (комплаенса). Один риск может снижаться несколькими мерами. Мера может по-разному влиять на снижение ущерба и вероятности разных рисков.	Поддерживается моделирование эффекта от внедрения мер защиты, сопоставление их стоимости со степенью снижения риска при внедрении для выбора экономически эффективных мер.
5.13. Поддержка качественных и количественных методов оценки (перечислить методы);	Не поддерживается	Поддерживается задание пороговых значений рисков и возможность их настройки.	Частично. Поддерживается качественная оценка, в баллах или процентах.	Поддерживается количественная оценка по методике FAIR. Поддерживается проведение качественной, количественной оценки рисков кибербезопасности по методике вендора. Поддерживается моделирование рисков методом Монте-Карло.
5.14. Кастомизация методов, формул для проведения качественной, количественной оценки рисков;	Не поддерживается	Частично. Поддерживается кастомизация формул для расчета риско.в	Формула задается в настройках методики оценки и выбирается из готового списка.	Поддерживается изменение встроенных методов и формул. Поддерживается создание пользовательских методов и формул расчета.
5.15. Возможность приведения качественной оценки к количественной (с настройкой пороговых значений);	Не поддерживается	Поддерживается	Поддерживается через критерии оценки рисков.	Поддерживается за счет переведения качественных оценок в балльную систему. Качественная и количественная оценка могут быть рассчитаны по единым формулам.
5.16. Поддержка оценки и анализа киберрисков автоматически (по настраиваемому процессу), вручную (с помощью заполнения опросных листов, экспертным методом, методом Дельфи и т.д.);	Не поддерживается	Частично, с помощью заполнения опросных листов.	Частично.	Поддерживается ручной и автоматический способ оценки и анализа рисков. Автоматический способ оценки реализуется как по расписанию, так и по факту изменения исходных данных. Поддерживаются опросные листы, метод Монте-Карло, экспертный метод с разделением полномочий, метод Дельфи. Поддерживается автоматическая оценка и анализ рисков с настройкой рабочих процессов в графическом low-code / no-code конструкторе.
5.17. Управление задачами, заявками на обработку киберрисков (внедрение мер защиты, устранение уязвимостей, приведение конфигураций в соответствие и т.д.) с поддержкой отправки и получения оповещений, с поддержкой настройки жизненного цикла задач, заявок;	Не поддерживается	Поддерживается формирование плана обработки рисков, отправка задач в интегрированные системы.	Используется Модуль задач. Задачи привязываются к рискам, мерам, техническим уязвимостям. В задачах сроки, ответственные, критичность, можно прикладывать файлы, комментарии, чеклисты (подзадачи), откладывать задачи. Есть двухсторонняя интеграция с Jira..	Поддерживается управление заявками, задачами на обработку рисков с работой через веб-интерфейс решения, мессенджеры (Telegram), электронную почту, через API к любой системе.

Название продукта, производителя	АльфаДок ООО “НПЦ “КСБ”	R-Vision SGRC ООО “Р-Вижн” Демонстрируется версия 5.4, заявленный вендором срок выхода: Q1 2025	Securitm ООО “Секьюритм”	Security Vision SGRC ООО “Интеллектуальная безопасность”
5.18. Возможность интеграции, включая двухстороннюю, с системами класса CMDB / ITAM, ITSM / ServiceDesk / Ticketing, BPM / ERP, SIEM / SOAR / TIP, VM / EASM и другими для управления киберрисками;	Не поддерживается	Поддерживаются интеграции с SIEM (двусторонние), NGFW, IDS/IPS, VM, SOAR, антивирусным ПО, системами ITSM, ITAM, Service Desk, базами данных и другими системами. По умолчанию доступно более 30 готовых интеграций. Возможно создание кастомных интеграций.	Прямые интеграции с Active Directory, Kaspersky Security Center, Dr.Web, Zabbix, NetBox, Solar Dozor, Scan Factory (двухсторонняя), Cloud Advisor, Kaspersky ASAP, Vulns.io, Meta Scan, Staffcop, MaxPatrol VM, Manage Engine, Jira (двухсторонняя). Импорт отчетов от сканеров уязвимостей Qualys, Nessus, RedCheck, Nmap, OpenVas, Kaspersky, XSpider, AppScreener, OWASP ZAP, MaxPatrol 8, Manage Engine. Настраиваемые интеграции по API.	Поддерживается интеграция с Security Vision BCP, Security Vision RM/ORM, Security Vision CM, Security Vision UEBA, Security Vision AD + ML. Поддерживается интеграция с Any.Run, Kaspersky KATA, PT Sandbox, PT NAD, Trend Micro Deep Discovery Analyzer (DDA), Cisco StealthWatch, Zabbix, Microsoft Exchange, Veeam Backup, Check Point, Cisco ASA, Cisco Firepower, Cisco Switch, Juniper, Fortigate, Kaspersky Security Center, Microsoft Defender, TrendMicro DDA, Kaspersky OpenTIP, FireEye, Symantec Endpoint Protection Manager, Palo Alto, TrendMicro IMSVA, CMDB iTop, MS SCCM, MS WSUS, Kaspersky Security Center (подключение к БД и OpenAPI), Infoblox (IPAM), Skybox, SearchInform, Lansweeper, MaxPatrol 8, MaxPatrol SIEM, Kaspersky KUMA, IBM QRadar, Pangeo RADAR, RuSIEM, NEURODAT SIEM, ArcSight SIEM, Splunk, Symantec CSP, VMware vCenter, VMware vROps, Proxmox, Hyper-V, HP OneView, Cisco UCS, Symantec Endpoint Protection Manager, Efros Config Inspector, Microsoft Endpoint Configuration Manager, Ovirt, NetBox, Active Directory, OpenLDAP, FreeIPA, Astra Linux Directory, ALD Pro, One Vision SD, Jira, Naumen Service Desk, MicroFocus Service Manager (HP Service Manager), BPM Online (Creatio), OTRS, Redmine и другими системами.
5.19. Отчетность по киберрисками: предустановленные шаблоны отчетов по уровням и статусам обработки киберрисков, сводные отчеты по киберрискам, разнообразные виды и форматы выгрузки отчетов (doc, pdf и т.д.), возможность создания стратегических, оперативных, тактических, аналитических отчетов для различных групп потребителей решения, возможность отправки отчетов автоматически и по запросу по электронной почте, через мессенджеры и т.д.;	Не поддерживается	Частично. Встроенная база типовых отчетов. Возможность создать отчеты по рискам в различных разрезах. Поддержка форматов pdf, xlsx, docx, pptx, odt, и др). Отправка отчетов по электронной почте.	Частично. Выгрузка реестров и планов обработки рисков в CSV, XLS, JSON, XML.	Поддерживается формирование отчетов в форматах pdf, docx, odt, xlsx, ods. Поддерживается отображение состояния уровней и статусов киберрисков в отчетах различного типа с элементами визуализации (таблицы, графики, диаграммы, географическая карта и т.д.). Возможна отправка отчётов по электронной почте (вручную или по расписанию).
5.20. Визуализация состояния киберрисков: предустановленные дашборды по уровням и статусам обработки киберрисков, возможность создания дашбордов (стратегические, оперативные, тактические, аналитические), диаграмм (лепестковые, гистограммы, круговые и т.д.), виджетов (“светофоры”, “спидометры” и т.д.), функционал drill down”.	Не поддерживается	Встроенная база типовых дашбордов по рискам. Возможность создать дашборды по рискам в различных разрезах. Поддерживается функциональность «drill down». Поддерживается возможность создавать графики типа “Топ-... объектов”.	Поддерживаются предустановленные дашборды в модуле рисков, являющиеся фильтрами для реестра и плана обработки рисков.	Поддерживается отображение состояния киберрисков на виджетах (линейный график, столбчатая диаграмма, круговая диаграмма, спидометр, таблица, географическая карта), на графах связей, на дашбордах, в отчетах. Во всех графических элементах поддерживается функционал «drill down» для непосредственного перехода от визуальных элементов к данным, на основании которых было построено графическое отображение.
6. Управление соответствием требованиям (Compliance)				

Название продукта, производителя	АльфаДок ООО “НПЦ “КСБ”	R-Vision SGRC ООО “Р-Вижн” Демонстрируется версия 5.4, заявленный вендором срок выхода: Q1 2025	Securitm ООО “Секьюритм”	Security Vision SGRC ООО “Интеллектуальная безопасность”
6.1. Проведение оценок соответствия требованиям российских / СНГ / международных / отраслевых НПА и стандартов, включая 152-ФЗ, 187-ФЗ, 98-ФЗ, 149-ФЗ, ГОСТ 57580, ГОСТ/ISO 27001, документы ФСТЭК России (Приказы 17, 21, 31, 235, 239), документы ФСБ РФ (Приказы 378, 367, 196), Положения ЦБ РФ (683-П, 716-П, 719-П, 757-П, 779-П, 802-П), методические рекомендации ЦБ РФ (№ 8/12/18-МР), PCI DSS v.4 и т.д. (указать);	Поддерживаются документы: Федеральный закон №152-ФЗ, Федеральный закон №187-ФЗ, Приказ ФСТЭК России от 14 марта 2014 г. № 31, Приказ ФСТЭК России от 11 февраля 2013 г. № 17, Приказ ФСТЭК России от 18 февраля 2013 г. № 21, Приказ ФСТЭК России от 25 декабря 2017 г. № 235, Приказ ФСТЭК России от 21 декабря 2017 г. № 239.	Поддерживаются 152-ФЗ, 187-ФЗ, 98-ФЗ, 149-ФЗ. Приказы ФСТЭК №17, 21, 31, 239. Приказы ФСБ РФ №378, 367, 196. Положения Банка РФ №716-П, 719-П, 802-П, 683-П, 821-П ГОСТ 57580.1-2017, ISO 27001, PCI DSS v.4 и другие.	Поддерживаются документы: ПДн: Федеральный Закон № 152-ФЗ, GDPR (ru), Постановление Правительства РФ № 1119, Постановление Правительства РФ № 211, Постановление Правительства РФ № 687, Постановление Правительства РФ № 883, Приказ МЦРИАП РК от 12.06.23 № 179/НК, Приказ Минцифры N 453 от 12 мая 2023 г., Приказ Роскомнадзора № 178, Приказ Роскомнадзора № 179, Приказ Роскомнадзора №180 от 28.10.2022, Приказ Роскомнадзора № 996 от 05.09.2013, Приказ ФСБ № 378, Приказ ФСТЭК № 21, Рекомендации Роскомнадзора по обезличиванию ПДн. КИИ: Федеральный Закон № 187-ФЗ, Указ Президента РФ № 166, Указ Президента РФ № 250, Постановление Правительства РФ № 127, Постановление Правительства РФ № 1478, Приказ ФСТЭК № 235, Приказ ФСТЭК № 239, Приказ ФСБ № 196, Приказ ФСБ № 282, Приказ ФСБ № 367, Приказ ФСБ № 77, Методика оценки показателя состояния ТЗИ. СМИБ: ГОСТ Р ИСО/МЭК 27001-2021, ГОСТ Р № ИСО/МЭК 27002-2021, ISO/IEC 27001:2022 (En), ISO/IEC 27001:2022 (Ru), ГОСТР ИСО 22301-2021. Финансы: Федеральный закон №161, PCI DSS 4.0, SWIFT CSCF, ГОСТ Р 57580.1, ГОСТ Р 57580.3, ГОСТ Р 57580.4, 12-МР для 802-П, 12-МР для 719-П, 12-МР для 683-П, 18-МР 8-МР для 757-П, Положение Банка России 683-П, Положение Банка России 716-П, Положение Банка России 719-П, Положение Банка России 757-П, Положение Банка России 779-П, Положение Банка России 787-П, Положение Банка России 802-П, Положение Банка России 808-П, Положение Банка России № 821-П, Положение Банка России № 822-П, Постановление Правительства РФ № 584, Постановление Республики Казахстан №89, Постановление Республики Казахстан №90, Постановление Республики Казахстан № 110, Постановление Республики Казахстан №47, Приказ Минцифры N 453 от 12 мая 2023 г., РС БР ИББС-2.5-2014 РС БР ИББС-2.9-2016, СТО БР БФБО-1.8-2024, СТО БР ИББС-1.0-2014, СТО БР ИББС-1.3-2016, СТО БР ИББС-1.4-2018. Общее: Методика оценки угроз ФСТЭК 2021, Постановление Правительства РФ № 1385, Постановление Правительства РФ № 1441, Постановление Правительства РФ № 258, Постановление Правительства Республики Казахстан № 832, Приказ Минцифры РФ №646, Приказ Минцифры N935, Приказ ФСТЭК № 77, Федеральный закон № 126-ФЗ, Федеральный закон № 149-ФЗ. Здравоохранение: FDA 21 CFR part 11, Приказ Минздрава № 911н, GMP Annex 11: Computerised Systems. АСУ ТП: Приказ ФСТЭК № 31. СКЗИ: Приказ ФАПСИ № 152, Приказ ФСБ № 378, Федеральный Закон № 63-ФЗ. ГИС: Постановление Правительства РФ № 676, Приказ ФСТЭК № 17.	Поддерживаются стандарты, методики, документы: Федеральный закон № 98-ФЗ Федеральный Закон № 149-ФЗ Приказ ФАПСИ № 152 Федеральный Закон № 152-ФЗ Федеральный закон № 572-ФЗ Федеральный закон № 63-ФЗ Федеральный Закон № 161-ФЗ Федеральный закон № 126-ФЗ Федеральный Закон № 187-ФЗ Приказ ФСБ России № 367 Приказ ФСБ России № 378 Приказ ФСБ России № 796 Приказ ФСБ России № 368 Приказ ФСБ России № 282 Приказ ФСБ России № 196 Приказ ФСБ России № 77 Приказ ФСБ России № 281 Приказ ФСТЭК России № 31 Приказ ФСТЭК России № 17 Приказ ФСТЭК России № 76 Приказ ФСТЭК России № 239 Приказ ФСТЭК России № 75 Приказ ФСТЭК России № 235 Приказ ФСТЭК России № 21 ГОСТ Р 59547-2021 Приказ 66 ОАЦ Приказ Роскомнадзора № 179 Приказ Роскомнадзора № 996 Приказ Роскомнадзора № 178 Указ Президента РФ № 166 Постановление Правительства РФ № 211 Постановление Правительства РФ № 1272 Постановление Правительства РФ № 676 Указ Президента РФ № 250 Постановление Правительства РФ № 1912 Постановление Правительства РФ № 1478 Постановление Правительства РФ № 883 Постановление Правительства РФ № 1119 Постановление Правительства РФ № 687 Постановление Правительства РФ № 584 Постановление Правительства РФ № 127 Постановление Правительства РФ № 820 Приказ Минцифры № 453 Приказ Минздрава № 911н PCI SSF – PCI Secure Software Standard v1.2.1 PCI DSS 4.0 PCI SSF – PCI Secure SLC Standard v1.1 NIST Cybersecurity Framework 2.0 ГОСТ Р ИСО/МЭК 27001—2021 ГОСТ Р ИСО 22301—2021 ИСО/МЭК 27001-2022 E ИСО 22301:2019 E CIS Critical Security Controls v7.1 CIS Critical Security Controls Version 8 GDPR ГОСТ Р 57580_1-2017 ГОСТ Р 57580_3-2022 ГОСТ Р 57580_4-2022 Положение Банка России 683-П Положение Банка России 716-П Положение Банка России 719-П Положение Банка России 757-П Положение Банка России 779-П Положение Банка России 787-П Положение Банка России 802-П Положение Банка России 808-П Положение Банка России 821-П Положение Банка России 822-П Положение Банка России 833-П

Название продукта, производителя	АльфаДок ООО “НПЦ “КСБ”	R-Vision SGRC ООО “Р-Вижн” Демонстрируется версия 5.4, заявленный вендором срок выхода: Q1 2025	Securitm ООО “Секьюритм”	Security Vision SGRC ООО “Интеллектуальная безопасность”
			Коммерческая тайна: Федеральный закон № 98-ФЗ.	
6.2. Проведение оценок соответствия рекомендациям NIST CSF, NIST SP 800-171, NIST SP 800-53, NIST Privacy Framework, CIS Critical Security Controls, CIS Benchmarks, Microsoft ("Recommended security configuration baselines" из пакета "Microsoft Security Compliance Toolkit"), "Security Technical Implementation Guides" (STIGs), частным рекомендациям производителей (ОС, ПО, оборудования, сетевых устройств), лучшим практикам;	Не поддерживается	Не поддерживается. Для осуществления технического аудита в экосистеме R-Vision предусмотрены другие программные продукты.	Поддерживаются частично	Поддерживаются CIS Critical Security Controls v.8, CIS Benchmarks, NIST Cybersecurity Framework, рекомендации Microsoft, рекомендации вендоров, собственная экспертиза вендора. Автоматическая проверка корректности конфигурации узлов в сети в соответствии с принятыми политиками безопасности с помощью Security Vision SPC.
6.3. Проведение оценок соответствия рекомендациям и лучшим практикам из собственной экспертизы вендора;	Не поддерживается	Поддерживается	Поддерживаются частично	Поддерживается
6.4. Регулярность обновления базы НПА, стандартов, лучших практик, пакетов экспертизы вендора и т.д.;	Поддерживается ведение и обновление вендором базы НПА по мере выхода новых документов несколько раз в год.	База обновляется в ближайшем релизе после обновления НПА, возможно более раннее обновление по запросу заказчика	Регулярно производится обновление существующей базы и добавление новых документов.	Поддерживается ведение и обновление вендором базы НПА, стандартов, лучших практик, пакетов экспертизы по мере выхода новых документов, но не реже 1 раз в месяц.
6.5. Проведение оценок соответствия требованиям ОРД, возможность загрузки и декомпозиции ОРД и требований договоров, материнских организаций, отраслевых ассоциаций и т.д.;	Поддерживается загрузка уникальных документов организации в форматах jpg, jpeg, png, pdf, doc, docx, rtf, odt, ods, xlsx, pptx, vsd, rar, zip, 7z, tar.	Не поддерживается	Поддерживается	Поддерживается загрузка любых произвольных стандартов посредством импорта файла csv определенной структуры, с последующей автоматической декомпозицией на требования и домены (создание соответствующих карточек объектов и их группировка по доменам).
6.6. Формирование общей базы требований ОРД в решении;	Поддерживается	Поддерживается	Поддерживается	Поддерживается
6.7. Поддержка статусной модели и учет версионности для различных НПА и ОРД с указанием, для какой версии документа выполнялась оценка соответствия;	Поддерживается	Частично. Поддерживаются только статусы документов.	Поддерживается частично	Поддерживается
6.8. Возможность проведения ручного (заполнение опросных листов, форм, таблиц) и автоматического (на основе данных решения и данных от внешних ИТ/ИБ-систем) процесса оценки соответствия требованиям;	Поддерживается частично. Ручной процесс оценки соответствия с помощью заполнения опросных листов и форм.	Частично. Поддерживается только ручная оценка.	Поддерживаются 3 способа оценки соответствия: - Вручную (выполнено, не выполнено, частично, неприменимо) с указанием обоснования и файлов свидетельств; - Автоматически через статус связанных с требованием защитных мер (основной механизм); - Автоматически через метрики (модуль Метрик) – технические и организационные показатели, данные для которых собираются через интеграции с ИТ/ИБ-системами или опросы работников.	Поддерживается ручной и автоматический процесс оценки соответствия требованиям. Ручной режим – возможно заполнение как в интерфейсе решения, так и посредством экспорта опросного листа в виде файла, с последующем импортом результатов его заполнения. Автоматический режим: 1. На основании статуса реализации мер защиты 2. На основании данных решения (активы, уязвимости, инциденты и т.д.) 3. Посредством интеграции с СЗИ и ИТ-системами.
6.9. Применяемые встроенные методики оценки соответствия (вендорские, на базе лучших практик), возможность кастомизации встроенных методик, возможность создания пользовательской методики;	Поддерживается частично	Вендорская методика, возможность кастомизации встроенных методик, возможность создания пользовательской методики.	Методика по умолчанию для всех стандартов – процентная оценка уровня соответствия.	Поддерживаются встроенные методики оценки соответствия на базе лучших практик и законодательных требований. Поддерживается создание пользовательских методик.
6.10. Декомпозиция, дедупликация, корреляция требований (НПА, ОРД), группирование требований по направлениям (доменам);	Не поддерживается	Поддерживается. В системе предусмотрены контрольные проверки, объединение требований в группы.	Поддерживается частично. В базе более 100 стандартов и НПА (наборов требований), в которых требования скоррелированы между собой. На страницах требований видно все аналогичные требования из других наборов. Можно самостоятельно создавать связи между требованиями. НПА группируются по направлениям. Можно создавать области и группы областей для наборов требований.	Поддерживается, НПА и ОРД декомпозируются до отдельных требований. Устанавливается взаимосвязь требований между различными документами. Требования группируются по доменам, в соответствии с принятой в НПА и ОРД логикой.
6.11. Управление жизненным циклом проведения оценки соответствия: импорт / декомпозиция / создание требований, ручное и автоматическое заполнение, обработка ответов и исключений, расчет уровня соответствия, формирование и согласование плана обработки несоответствий, контроль выполнения плана;	Не поддерживается	Поддерживается	Поддерживается частично	Поддерживается проведение оценки соответствия по встроенной и пользовательской методикам.
6.12. Реализация плана обработки несоответствий: формирование заявок, задач, документов в решении, экспорт во внешние системы ITSM / ServiceDesk / Ticketing, отправка и получение уведомлений;	Поддерживается формирование задач с произвольным текстом, датой исполнения, напоминанием, статусом.	Поддерживается через функционал “Замечаний”.	Несоответствия в системе оформляются как проекты защитных мер (в статусе потребность) или как задачи, привязанные к требованиям. Используется модуль защитных мер, модуль задач. Задачи могут привязываться к мерам и требованиям. Модуль задач позволяет учитывать сроки, ответственных, критичность, прикладывать файлы, комментарии, чеклисты (подзадачи), откладывать задачи. Есть двухсторонняя интеграция с Jira.	Поддерживается формирование заявок, задач, документов на обработку несоответствий с работой через веб-интерфейс решения, мессенджеры (Telegram), электронную почту, через API к любой системе, включая One Vision SD, Jira, Naumen Service Desk, MicroFocus Service Manager (HP Service Manager), BPM Online (Creatio), OTRS, Redmine.

Название продукта, производителя	АльфаДок ООО “НПЦ “КСБ”	R-Vision SGRC ООО “Р-Вижн” Демонстрируется версия 5.4, заявленный вендором срок выхода: Q1 2025	Securitm ООО “Секьюритм”	Security Vision SGRC ООО “Интеллектуальная безопасность”
6.13. Возможность проведения скоринга соответствия: расчет оценки соответствия выбранным требованиям для всей организации / отдельных процессов / инфраструктуры / отдельных информационных систем и активов, возможность кастомизации формулы для расчета, непрерывный автоматический расчет оценки соответствия, перерасчет оценки соответствия для уже оцененных объектов при изменении формулы расчета;	Поддерживается оценка соответствия для отдельных информационных систем и организаций. Кастомизация формулы оценки не поддерживается. Поддерживается автоматический расчет оценки соответствия.	Поддерживается скоринг через “индекс соответствия”.	Поддерживается оценка для всей организации, ее отдельных областей (юр.лиц, систем, сегментов и т.п.) или отдельных активов. Настройка бальной оценки. Непрерывная автоматическая оценка и переоценка в зависимости от имеющихся данных в модулях активов, защитных мер и метрик.	Поддерживается скоринг-оценка соответствия по встроенной и пользовательской методикам для всех применимых объектов решения. Поддерживается автоматический перерасчет скоринг-балла. Расчёт и визуализация общей оценки и по доменам.
6.14. Поддержка ведения и отображения истории оценки соответствия, использование собранных данных для проактивной оценки соответствия новым требованиям;	Поддерживается частично за счет уведомлений (без указания подробностей о выполненных действия), проактивная оценка не поддерживается.	Частично поддерживается только история оценки соответствия	Поддерживается частично за счет учета и отображения уровня соответствия по месяцам в разрезе документов. Рекомендательная модель при проведении оценки по новым наборам требований, взятым на контроль через результаты уже проведенных оценок (только если оценка была проведена через связь с защитными мерами).	Поддерживается ведение и визуализация динамики оценки соответствия. Наличие таймлайна процесса проведения оценки соответствия. Поддерживается автоматическая оценка требований на основании статуса реализации мер защиты.
6.15. Поддержка ведения и отображения истории выполненных действий (ручных, автоматических) по приведению в соответствие;	Поддерживается частично за счет уведомлений (без указания подробностей о выполненных действия).	Частично поддерживается (отображение истории)	Частично. Журналируются изменения по связям защитных мер с требованиями, по изменению статуса защитных мер, по изменению метрик.	Поддерживается история выполненных действий с детализацией до каждого свойства. Визуализация пройденных этапов жизненного цикла задачи по устранению несоответствия.
6.16. Возможность интеграции процесса управления соответствием требованиям с другими процессами ИБ (управление активами, уязвимостями, обновлениями, конфигурациями, инцидентами ИБ, киберрисками и т.д.);	Частично	Частично	В карточке актива отображается оценка по набору требований если оценка проводится в отношении этого актива. В карточке актива отображается сводная оценка соответствия по областям, в которые он входит. Данные из модуля активов формируют результаты в модуле метрик, которые влияют на оценку соответствия. Управление задачами проводится в привязке к требованиям. Защитные меры исполняют требования.	Поддерживается интеграция процесса управления соответствием со всеми процессами, настроенными в решении, с учетом взаимосвязей и взаимных зависимостей объектов решения.
6.17. Возможность интеграции, включая двухстороннюю, с системами класса CMDB / ITAM, ITSM / ServiceDesk / Ticketing, SIEM / SOAR / TIP, VM / EASM и другими для управления соответствием требованиям;	Не поддерживается	Поддерживаются интеграции с SIEM (двусторонние), NGFW, IDS/IPS, VM, SOAR антивирусным ПО, системами ITSM, ITAM, Service Desk, базами данных и другими системами. По умолчанию доступно более 30 готовых интеграций. Возможно создание кастомных интеграций.	Прямые интеграции с Active Directory, Kaspersky Security Center, Dr.Web, Zabbix, NetBox, Solar Dozor, Scan Factory (двухсторонняя), Cloud Advisor, Kaspersky ASAP, Vulns.io, Meta Scan, Staffcop, MaxPatrol VM, Manage Engine, Jira (двухсторонняя). Импорт отчетов от сканеров уязвимостей Qualys, Nessus, RedCheck, Nmap, OpenVas, Kaspersky, XSpider, AppScreener, OWASP ZAP, MaxPatrol 8, Manage Engine Настраиваемые интеграции по API.	Поддерживается интеграция с Security Vision BCP, Security Vision RM/ORM, Security Vision CM, Security Vision UEBA, Security Vision AD + ML. Поддерживается интеграция с Any.Run, Kaspersky KATA, PT Sandbox, PT NAD, Trend Micro Deep Discovery Analyzer (DDA), Cisco StealthWatch, Zabbix, Microsoft Exchange, Veeam Backup, Check Point, Cisco ASA, Cisco Firepower, Cisco Switch, Juniper, Fortigate, Kaspersky Security Center, Microsoft Defender, TrendMicro DDA, Kaspersky OpenTIP, FireEye, Symantec Endpoint Protection Manager, Palo Alto, TrendMicro IMSVA, CMDB iTop, MS SCCM, MS WSUS, Kaspersky Security Center (подключение к БД и OpenAPI), Infoblox (IPAM), Skybox, SearchInform, Lansweeper, MaxPatrol 8, MaxPatrol SIEM, Kaspersky KUMA, IBM QRadar, Pangeo RADAR, RuSIEM, NEURODAT SIEM, ArcSight SIEM, Splunk, Symantec CSP, VMware vCenter, VMware vROps, Proxmox, Hyper-V, HP OneView, Cisco UCS, Symantec Endpoint Protection Manager, Efros Config Inspector, Microsoft Endpoint Configuration Manager, Ovirt, NetBox, Active Directory, OpenLDAP, FreeIPA, Astra Linux Directory, ALD Pro, One Vision SD, Jira, Naumen Service Desk, MicroFocus Service Manager (HP Service Manager), BPM Online (Creatio), OTRS, Redmine и другими системами.
6.18. Возможность связать процесс управления соответствием требованиям с процессами управления уязвимостями и конфигурациями, интеграция с системами управления уязвимостями и конфигурациями;	Не поддерживается	Не поддерживается. Для решения задачи управления уязвимостями в экосистеме R-Vision представлены другие продукты, с которыми возможна интеграция.	Частично. Результаты работы модуля управления уязвимостями (VM) могут косвенно влиять на соответствие требованиям.	Поддерживается интеграция процесса управления соответствием с процессами управления уязвимостями и конфигурациями, с интеграцией через API со сторонними системами. Управление уязвимостями и конфигурациями реализуется отдельными продуктам: Security Vision VM и Security Vision SPC.
6.19. Связь процесса управления соответствием требованиям с реализованными защитными мерами, оценка фактически реализуемого уровня ИБ, учет требований НПА и ОРД при оценке конфигураций СЗИ;	Частично. Поддерживается только за счет ручного указания перечня выполненных мер.	Частично	Поддерживается как основной метод оценки соответствия – через связь с защитными мерами (модуль мер) и их статус.	Поддерживается анализ реализованных мер с помощью интеграций с СЗИ и ИТ-системами, с получением данных об их состоянии и настройках конфигураций.
6.20. Отчетность по соответствию требованиям: предустановленные шаблоны отчетов по уровням и статусам обработки требований, сводные отчеты по соответствию требованиям, включая отчетность по готовности к проверкам регуляторов (ФСТЭК, РКН, ФСБ, ЦБ РФ и т.д.) и отчетность с разбивкой по направлениям (доменам) и отдельным требованиям, разнообразные виды и форматы выгрузки отчетов (doc, pdf и т.д.), возможность создания стратегических, оперативных, тактических, аналитических отчетов для различных групп потребителей решения, возможность отправки отчетов автоматически и по запросу по электронной почте, через мессенджеры и т.д.;	Поддерживается формирование отчетов в форматах pdf, docx, xlsx. Перечень формируемых отчетных документов по защите ПДн, ГИС, КИИ: cloud.alfa-doc.ru	Частично поддерживается, есть база шаблонов оповещений	Универсальный отчет по соответствию требованиям. Отчет по соответствию требованиям в рамках конкретной области оценки. Специализированные отчеты по ГОСТ 57580 и 8/12-МР. Выгрузка вручную, в формат doc.	Поддерживается формирование отчетов в форматах pdf, docx, odt, xlsx, ods. Поддерживается отображение состояния уровней и статусов киберрисков в отчетах различного типа с элементами визуализации (таблицы, графики, диаграммы, географическая карта и т.д.). Поддерживается формирование отчетности по состоянию соответствия требованиям ФСТЭК, РКН, ФСБ, ЦБ РФ.

Название продукта, производителя	АльфаДок ООО “НПЦ “КСБ”	R-Vision SGRC ООО “Р-Вижн” Демонстрируется версия 5.4, заявленный вендором срок выхода: Q1 2025	Securitm ООО “Секьюритм”	Security Vision SGRC ООО “Интеллектуальная безопасность”
6.21. Визуализация состояния соответствия требованиям: предустановленные дашборды по уровням и статусам обработки требований, включая визуализацию состояния готовности к проверкам регуляторов (ФСТЭК, РКН, ФСБ, ЦБ РФ и т.д.) и визуализацию с разбивкой по направлениям (доменам) и отдельным требованиям, возможность создания дашбордов (стратегические, оперативные, тактические, аналитические), диаграмм (лепестковые, гистограммы, круговые и т.д.), виджетов (“светофоры”, “спидометры” и т.д.), функционал “drill down”.	Поддерживается отображение состояния соответствия требованиям на виджетах (дашборды, таблицы). Функционал “drill down” не поддерживается.	Встроенная база типовых дашбордов по аудитам. Возможность создать дашборды по аудитам в различных разрезах. Поддерживается функциональность “drill down”. Поддерживается возможность создавать графики типа “Топ-... объектов”.	Предустановленные дашборды по оценке соответствия, показывающие общий уровень соответствия, соответствие по отдельным доменам, по отдельным группам областей и областям (например, организациям, системам) с возможностью фильтрации по доменам и отдельным наборам требований. В рамках отдельных наборов требований дашборды показывающие историю изменений уровня соответствия, текущий, планируемый и целевой уровни соответствия, соответствие по отдельным блокам (направлениям) стандарта. Светофоры, спидометры, барчарты, лепестковые диаграммы. В дашбордах по разделам стандартов «drill down» до разделов.	Поддерживается отображение состояния соответствия требованиям на виджетах (линейный график, столбчатая диаграмма, круговая диаграмма, спидометр, таблица, географическая карта), на графах связей, на дашбордах, в отчетах. Во всех графических элементах поддерживается функционал «drill down» для непосредственного перехода от визуальных элементов к данным, на основании которых было построено графическое отображение. Поддерживается формирование визуализации состояния соответствия требованиям ФСТЭК, РКН, ФСБ, ЦБ РФ.

Расширенные критерии

Название продукта, производителя	АльфаДок ООО “НПЦ “КСБ”	R-Vision SGRC ООО “Р-Вижн” Демонстрируется версия 5.4, заявленный вендором срок выхода: Q1 2025	Securitm ООО “Секьюритм”	Security Vision SGRC ООО “Интеллектуальная безопасность”
1. Общие технические характеристики				
1.1. Возможность использования решения как услуги (SaaS-модель);	Поддерживается	Не поддерживается	Поддерживается	Поддерживается. Есть собственный сервис SaaS с модулями управления соответствием (Compliance) и управления рисками (Risk Management).
1.2. Поддержка работы решения в сетях, изолированных от Интернет;	Не поддерживается	Поддерживается	Не поддерживается	Поддерживается, установка, функционирование и обновление решения не требует доступа к сети Интернет. Для интеграций с источниками данных, размещенных в сети Интернет, может использоваться отдельный компонент (коннектор), размещаемый в DMZ.
1.3. Открытость скриптов, алгоритмов, логики, моделей машинного обучения в решении, возможность их доработки и адаптации под требования конечного пользователя (в части подключения к проверяемым хостам, сбора данных, обработки и анализа данных, выполнения проверок и т.д.);	Не поддерживается	Не поддерживается	Частично.	Поддерживается кастомизация всех коробочных скриптов/моделей, а также есть возможность создания и имплементации произвольных пользовательских скриптов/моделей.
1.4. Поддержка собственного мониторинга встроенным функционалом решения;	Не поддерживается	Не поддерживается	Поддерживается через встроенную систему самопроверки “Мониторинг ошибок” - собственная разработка, которая проверяет работоспособность системы и всех ее компонентов, интеграций.	Поддерживается и включено в инсталляцию по умолчанию.
1.5. Поддержка собственного мониторинга через интеграции с внешними системами (например, Zabbix);	Не поддерживается	Поддерживается	Поддерживается	Поддерживается
1.6. Поддержка работы решения из внешней / облачной инфраструктуры (возможность размещения выносного компонента в DMZ, интернете, частном облаке для проведения инвентаризации и оценки инфраструктуры извне);	Не поддерживается	Частично	Поддерживается через установку нескольких связанных серверов приложения, связь серверов осуществляется по API или через файловые шары.	Поддерживается возможность установки компонентов решения (сервисов) на выделенные серверы в облачных инфраструктурах.
1.7. Поддержка работы решения в режиме multitenancy: наличие встроенного функционала по разграничению данных по тенантам, возможность присвоения тенанта пользователю, возможность присвоения тенанта данным (активам, уязвимостям, проверкам, несоответствиям, задачам и т.д.), построение иерархии тенантов, возможность переключения пользователя между доступными тенантами, возможность присвоения пользователям разных тенантов одной функциональной роли.	Не поддерживается	Поддерживается частично, с разграничением прав доступа на основе ролевой модели.	Поддерживается частично, с разграничением прав доступа на основе ролевой модели.	Поддерживается, включая иерархии от 3-х и более уровней (например, головная организация госкорпорации => множество холдингов => ДЗО каждого холдинга). Любые данные и объекты системы (активы, задачи, процедуры оценки, справочники и т.д.) могут быть разделены по тенантам. Пользователь решения имеет привязку к тенанту и имеет доступ к данным тенанта или другим данным в соответствии с иерархией тенантов. Пользователь может осуществлять переключение в иерархии тенатов в соответствии со своим уровнем доступа. Ролевая модель доступа учитывает разделение данных по тенантам, т.е. одна функциональная роль может быть назначена пользователям разных тенантов.
2. Общие организационные характеристики				
2.1. Наличие авторизованного обучения от вендора, стоимость обучения, длительность курса;	Частично. Обучение проводится в формате вебинаров.	Поддерживается. Обучение по курсам администрирования и использования решения, выдается сертификат вендора.	Частично. Цена от 240 т.р. в зависимости от объемов курса.	Поддерживается. Проводится бесплатное обучение в собственном учебном центре вендора с выдачей сертификата.
2.2. Поддержка работы MSS-провайдеров с решением;	Не поддерживается	Поддерживается	Поддерживается, сервер может быть развернут в инфраструктуре MSS провайдера для оказания услуг конечным заказчикам.	Поддерживается, предоставляются специальные лицензионные условия для провайдеров MSSP.

Название продукта, производителя	АльфаДок ООО “НПЦ “КСБ”	R-Vision SGRC ООО “Р-Вижн” Демонстрируется версия 5.4, заявленный вендором срок выхода: Q1 2025	Securitm ООО “Секьюритм”	Security Vision SGRC ООО “Интеллектуальная безопасность”
2.3. Дорожная карта развития решения (планируемый к внедрению функционал и ориентировочные сроки реализации, планируемые изменения в лицензионную политику).	Нет данных	Интеграция процесса управления киберрисками с аудитами.	Непрерывное увеличение количества интеграций, функций и модулей.	Расширение за счет добавления новых модулей и интеграций, машинного обучения для достижения большего охвата и автоматизации инструментами технологии auto-SGRC.
# 3. Общий функционал				
3.1. Поддержка работы с активами: возможность сканирования и инвентаризации инфраструктуры встроенными в решение средствами, возможность загрузки (импорта) данных об активах из внешних систем, агрегация и дедупликация данных по активам, возможность построения ресурсно-сервисной модели, поддержка различных типов активов, включая пользовательские типы;	Частично. Поддерживается локальное сканирование устройств с помощью утилиты “АРМ-сканер” с последующим импортом полученной информации в решение.	Частично. Поддерживается сетевое сканирование с помощью встроенного nmap.	Частично. Основной источник данных – прямые и универсальные интеграции с ИТ и ИБ системами. Встроенное сканирование icmp и nmap. Импорт данных в систему через xls/csv файлы, импорт по API. Настройка шаблонов импорта, правил объединения и сопоставления активов, их жизненного цикла в системе. Объединение активов в цифровые ресурсно-сервисные модели.	Поддерживается. Имеется собственной движок обнаружения, идентификации и инвентаризации узлов в различных сегментах сети. Имеется возможность сбора информации по активам из существующих в организации внешних систем. Имеется возможность комбинировать источники информации по активам (собственный движок и существующие системы), с последующим применением агрегации и дедупликации, а также построения взаимосвязей. Поддерживается полноценная ресурсно-сервисная модель от уровня бизнес-процессов и продуктов до уровня ПО и учётных записей.
3.2. Минимизация прав доступа к инвентаризуемым и оцениваемым активам, использование технологий ограничения доступа (например, LAPS, sudo wrappers) и скриптов настройки конечных активов для доступа с ограниченными правами;	Частично. Запуск “АРМ-сканер” выполняется с пользовательскими или административными привилегиями.	Не поддерживается	Не поддерживается	Поддерживается за счет тонкой настройки прав доступа на конечных устройствах.
3.3. Гибкость механизмов фильтрации: возможность составлять сложные поисковые запросы к объектам решения (разные условия по различным атрибутам, объединение через логические операторы «И» или «ИЛИ»), поддержка языков запроса в решении (SQL-подобные, скриптовые);	Поддерживается базовая фильтрация, поиск.	Поддерживается фильтрация, поисковые запросы. SQL-подобных запросов нет.	Частично. Поддерживается через поисковые запросы и фильтрацию. SQL-подобные запросы не поддерживаются.	Поддерживается фильтрация и составление поисковых запросов в графическом интерфейсе с low-code / no-code конструктором запросов. Возможность составления сложных условий фильтрации с использованием любых атрибутов объектов (включая пользовательские) и логических операторов “И” и “ИЛИ”.
3.4. Возможность создания пользовательских типов объектов решения в графическом конструкторе, с применением подхода low-code / no-code;	Не поддерживается	Частично. Поддерживается подход no-code.	Не поддерживается	Поддерживается. В решении реализован отдельный конструктор типов объектов, позволяющий реализовать неограниченное количество типов объектов, с возможностью создания любого количества атрибутов объектов разного типа данных, составления карточек объектов с возможностью произвольного размещения атрибутов на карточке (включая элементы визуализации – виджеты и графы), определение правил валидации и автозаполнения значений атрибутов карточки.
3.5. Поддержка использования подхода low-code / no-code для настройки правил и логики управления объектами решения;	Не поддерживается	Частично. Поддерживается подход no-code.	Не поддерживается	Поддерживается. В решении реализован полноценный конструктор, позволяющий реализовать правила доступа к атрибутам объекта (скрытие видимости, чтение, редактирование, обязательность заполнения, ограничение допустимых значений) в зависимости от ролей пользователя и комбинаций условий по атрибутам карточки (например, этапам жизненного цикла).
3.6. Связывание объектов с процессами (например, жизненным циклом заявки, инцидента);	Не поддерживается	Не поддерживается	Поддерживается, учет процессов как отдельного типа объекта может осуществляться.	Поддерживается возможность управления рабочими процессами через low-code / no-code конструктор, есть возможность управления процессами как в отдельности, так и связывать их напрямую с отдельными объектами в системе.
3.7. Мониторинг исполнения процессов с учётом длительности, версий, объектов и текущих статусов;	Не поддерживается	Частично	Поддерживается частично через настройку свойств процесса как отдельного типа объекта.	Поддерживается
3.8. Поддержка версионности для разрабатываемых процессов;	Не поддерживается	Не поддерживается	Поддерживается частично через настройку свойств процесса как отдельного типа объекта.	Поддерживается
3.9. Возможность кастомизации табличных форм, карточек и блоков в них без необходимости HTML-вёрстки;	Не поддерживается	Поддерживается	Поддерживается кастомизация состава таблиц, полей в карточке.	Поддерживается конструктором объектов, кастомизация внешнего вида позволяет группировать параметры (свойства) в блоки, управлять их размерами, форматами и стилями отображения как при помощи no-code, так и при помощи HTML (не обязательно).
3.10. Возможность кастомизации визуализации дашбордов, виджетов, меню интерфейса с применением подхода low-code / no-code;	Не поддерживается	Частично. Поддерживается подход no-code.	Частично. С базовыми элементами no-code.	Поддерживается. В решении реализован отдельный конструктор визуализации и конструктор меню. Конструктор визуализации позволяет создавать в режиме no code пользовательские виджеты с использованием любых данных решения, применением различных математических, логических и агрегационных функций, визуализации различными способами (графики, диаграммы, карты и т.д.). Дашборды представляют собой совокупность виджетов и позволяют настроить их взаимосвязь, в том числе по вводимым пользователям параметрам (например, определить период выборки данных по всем виджетам дашборда). Конструктор меню позволяет для каждой роли сформировать индивидуальный набор блоков и разделов меню, типы, состав, объем данных и функциональные возможности в разделах меню.
3.11. Возможность создания кастомизированных отчетов с применением подхода low-code / no-code;	Не поддерживается	Частично. Поддерживается подход no-code.	Не поддерживается, только встроенные отчеты.	Отчёты представляют собой совокупность виджетов и позволяют настроить их взаимосвязь, в том числе по вводимым пользователям параметрам (например, определить период выборки данных по всем виджетам дашборда). Конструктор отчётов позволяет определить форматы и способы отображения документов.
3.12. Возможность создания персонального рабочего окружения исходя из процессов и бренда организации: кастомизация гридов, быстрых фильтров, карточек и жизненного цикла объектов решения с применением подхода low-code / no-code;	Не поддерживается	Частично. Кастомизация гридов, карточек поддерживается с подходом no-code.	Частично. С базовыми элементами no-code.	Поддерживается кастомизация интерфейса, брендирование, добавление логотипов в графическом интерфейсе с low-code / no-code конструктором.
3.13. Встроенный функционал (среда разработки) для создания интеграций, политик и правил работы с объектами решения, настройки выполняемых действий по работе с объектами решения и поддерживаемыми решением процессами ИБ;	Не поддерживается	Поддерживается в виде графического редактора сценариев, конструктора коннекторов.	Не поддерживается	Поддерживается создание интеграций (коннекторов) с помощью встроенной в решение графической среды разработки с применением подхода low-code / no-code, при этом поддерживаются подсветка и проверка синтаксиса, тестирование разработанных интеграций, встроенная справка и интерактивные подсказки. Поддерживается настройка выполняемых действий с объектами решения (рабочих процессов) в графическом редакторе блок-схем с применением подхода low-code / no-code, с ветвлениями и настройкой сложных условий выполнения действий с объектами решения, с выполнением математических, логических, текстовых операций, операций с массивами, с поддержкой тестового режима «прогона» рабочих процессов.

Название продукта, производителя	АльфаДок ООО “НПЦ “КСБ”	R-Vision SGRC ООО “Р-Вижн” Демонстрируется версия 5.4, заявленный вендором срок выхода: Q1 2025	Securitm ООО “Секьюритм”	Security Vision SGRC ООО “Интеллектуальная безопасность”
3.14. Механизм интеграции посредством API;	Не поддерживается	Поддерживается	Поддерживается	Поддерживаются HTTP/HTTPS протоколы, API запросы get, post, put, patch, delete, DNS.
3.15. Поддержка интеграции с корпоративной почтой посредством IMAP, POP3, SMTP, Exchange;	Поддерживается	Поддерживается	Поддерживается	Поддерживается
3.16. Поддержка интеграции с службами каталогов Windows и Linux;	Не поддерживается	Поддерживается	Поддерживается частично, только Active Directory.	Поддерживается
3.17. Поддержка интеграции через логи и события журналирования;	Не поддерживается	Поддерживается	Не поддерживается	Поддерживается в полном объеме (Syslog, EventLog).
3.18. Поддержка интеграции при помощи удалённого и локального исполнения скриптов;	Не поддерживается	Не поддерживается	Частично поддерживается - только локальное исполнение скриптов на сервере системы.	Поддерживается как удалённое выполнение скриптов (WMI, PowerShell, SSH, SshShell), так и локальное (исполняемая команда, Shell скрипт, SH, команды Bash, Unix shell, команды командной строки Windows, cmd, пакетные файлы Windows, bat и др. языки программирования (Python, Java, JavaScript).
3.19. Поддержка интеграции для чтения и записи в файлы и БД;	Не поддерживается	Поддерживается (Oracle, MS SQL, MySQL, PostgreSQL)	Не поддерживается	Поддерживаются базы данных (SQL запросы в БД: MS SQL, MySQL, Postgres и Oracle) и файлы (операции чтения/записи с машиночитаемыми файлами).
3.20. Поддержка интеграции через шины данных (Kafka);	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается Kafka (например, для интеграции Hadoop).
3.21. Возможность создания произвольной структуры и наименования разделов основного меню решения для любой роли пользователя;	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается для ролей и отдельных пользователей, с использованием конструктора меню.
3.22. Поддержка локализации наименований на английский и другие языки;	Не поддерживается, только русский язык	Локализация на русском, английском. При установке используется только английский язык.	Не поддерживается	Поддерживается локализация на любые языки, по умолчанию английский для всех объектов, свойств, статусов, наименований пунктов меню и других элементов.
3.23. Наличие функционала “Рабочий календарь” (учет только рабочих дней / часов при создании различных задач и установки сроков их выполнения), формирование актуального производственного календаря на текущий год;	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается функционал формирования рабочего календаря с учетом количества рабочих часов, выходных и праздников. Возможность импорта данных из файла или посредством интеграции с внешней системой.
3.24. Возможности технической экосистемы (единой технологической платформы): наличие опции совместной установки на одной платформе других модулей, например модулей управления инцидентами, управления уязвимостями, управления информацией о киберугрозах и т.д. (указать);	Не поддерживается	Поддерживается совместная работа на единой платформе в рамках экосистемы R-Vision EVO, включая решения TDP, UEBA, SOAR, SGRC, TIP, SIEM.	Частично	Поддерживается совместная работа на единой платформе в рамках экосистемы Security Vision в составе модулей Security Vision SOAR, VM/VS, SGRC, TIP, UEBA, AD + ML, BCP, CM, КИИ, RM.
3.25. Интеграция с внешними сервисами для получения обогащающей, контекстуализирующей, аналитической информации (внешние сервисы киберразведки, базы уязвимостей, бюллетени безопасности, базы рекомендуемых конфигураций и т.д.);	Не поддерживается	Интеграция с NVD, БДУ ФСТЭК России, НКЦКИ, Exploit-DB, Vulners.com.	Поддерживается возможность создания интеграций по API с внешними сервисами для обогащения данных (например, с системами проверки контрагентов).	Поддерживается: · KasperskyOpenTip; · Kaspersky Threats; · AttackerKB; · NVD; · OpenCVE; · VulDB; · Vulners; · НКЦКИ; · FinCERT; · Alien Vault; · MISP; · RST Cloud.
3.26. Наличие сообщества / маркетплейса для получения дополнительных интеграций, скриптов, рекомендаций, лучших практик и т.д.;	Не поддерживается	Не поддерживается	Поддерживается за счет Community-версии Securitm в облаке.	Всем действующим Заказчикам и Партнёрам предоставляется доступ к разделу Marketplace, где на безвозмездной основе представлен экспертный контент (который подлежит импорту программный продукт).
3.27. Наличие функционала и кастомизации механизма статистического анализа свойств объектов;	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается
3.28. Применение методов машинного обучения (наличие и количество предварительно настроенных и обученных моделей машинного обучения), возможность подстройки параметров моделей под конкретную инфраструктуру;	Не поддерживается	Реализовано в дополнительном модуле UEBA, входящем в экосистему R-Vision EVO.	Не поддерживается	В решении применяется 10 ML-моделей, как предобученные, так и обучающиеся на трафике.
3.29. Применение внешних LLM-моделей;	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается интеграция с любой внешней системой посредством транспортов (коннекторов), разработаны и протестированы интеграциями с ML-моделями ChatGPT и YandexGPT.
3.30. Применение методов обработки Big Data.	Не поддерживается	Не поддерживается непосредственно в решении. Реализовано в дополнительном модуле UEBA.	Не поддерживается	Применяется методы обработки больших данных, встроенный движок корреляции (не только в коробочных решениях классов SIEM, TIP и UEBA, но для любых решений на базе Платформы, статистические методы обработки с учетом весовых показателей и ML-модели.

Название продукта, производителя	АльфаДок ООО “НПЦ “КСБ”	R-Vision SGRC ООО “Р-Вижн” Демонстрируется версия 5.4, заявленный вендором срок выхода: Q1 2025	Securitm ООО “Секьюритм”	Security Vision SGRC ООО “Интеллектуальная безопасность”
4. Управление стратегией, документами и процессами ИБ (Governance)				
4.1. Поддержка использования подхода low-code / no-code для настройки правил и логики управления стратегией, документами и процессами ИБ;	Не поддерживается	Частично. Поддерживается подход no-code.	Частично. С базовыми элементами no-code.	Поддерживается. В решении реализован полноценный конструктор, позволяющий реализовать правила доступа к атрибутам объекта (скрытие видимости, чтение, редактирование, обязательность заполнения, ограничение допустимых значений) в зависимости от ролей пользователя и комбинаций условий по атрибутам карточки (например, этапам жизненного цикла). Поддерживается настройка выполняемых действий с объектами решения (рабочих процессов) в графическом редакторе блок-схем с применением подхода low-code / no-code, с ветвлениями и настройкой сложных условий выполнения действий с объектами решения, с выполнением математических, логических, текстовых операций, операций с массивами, с поддержкой тестового режима «прогона» рабочих процессов.
4.2. Поддержка создания и управления информационной (ресурсно-сервисной) моделью инфраструктуры и организации, с возможностью импорта данных по её компонентам из файлов, ИТ/ИБ-систем;	Не поддерживается	Частично. Поддерживается ресурсно-сервисная модель. Импорт данных не поддерживается.	Поддерживается частично	Поддерживается полноценная ресурсно-сервисная модель от уровня бизнес-процессов и продуктов до уровня ПО и учётных записей.
4.3. Поддержка использования подхода low-code / no-code для построения информационной (ресурсно-сервисной) модели инфраструктуры и организации;	Не поддерживается	Частично. Поддерживается подход no-code.	Частично. С базовыми элементами no-code.	Поддерживается. В решении реализован отдельный конструктор типов объектов, позволяющий реализовать неограниченное количество типов объектов для описания ресурсно-сервисной модели, с возможностью создания любого количества атрибутов объектов разного типа данных, составления карточек объектов с возможностью произвольного размещения атрибутов на карточке (включая элементы визуализации – виджеты и графы), определение правил валидации и автозаполнения значений атрибутов карточки, настройки и отображения взаимосвязей объектов.
4.4. Поддержка создания и управления связями объектов решения между собой в рамках информационной (ресурсно-сервисной) модели инфраструктуры и организации, с возможностью интерактивного перехода от одного объекта к другому (от актива к уязвимости, от требования к конфигурации и т.д.);	Не поддерживается	Частично. Поддерживается переход от активов к бизнес-процессам.	Поддерживается частично	Поддерживается отображение всей ресурсно-сервисной модели инфраструктуре на графе связей с поддержкой выполнения интерактивных действий с объектами из графа (в том числе интерактивные переходы внутрь карточек объектов).
4.5. Отображение информационной (ресурсно-сервисной) модели инфраструктуры и организации на графе связей, сетевой схеме, планах зданий/помещений, географической карте с поддержкой выполнения интерактивных действий с объектами решения;	Не поддерживается	Частично. Поддерживается создание геокарты, схемы помещений с расположением активов.	Частично. Поддерживаются графы связей, реализующие в т.ч. сетевые схемы. Интерактивные действия с объектами из графа связей не поддерживаются.	Поддерживается полностью (всё перечисленное).
4.6. Поддержка ведения и отображения статистики и бизнес-аналитики по объектам решения в рамках управления стратегией и процессами ИБ.	Не поддерживается	Частично. Поддерживается отображение данных на дашбордах.	Поддерживается	Поддерживается ведение и отображение информации в виде диаграмм, графиков, отчетов. В том числе с функциями drilldown и интерактивного перестроения зависимых виджетов, в зависимости от выбранных пользователем входных параметров.
5. Управление киберрисками (Risk Management)				
5.1. Наличие и число встроенных («коробочных») сценариев работы с киберрисками;	Не поддерживается	Не поддерживается	Не поддерживается	Ключевые коробочные сценарии работы с киберрисками: 1. Формирование области оценки 2. Моделирование угроз 3. Оценка рисков (качественная и количественная) 4. Рассылка и заполнение опросных листов 5. Формирование реестра рисков 6. Обработка рисков (задачи с различными методами: снижение риска, принятие, избегание, передача) 7. Моделирование мер защиты 8. Планирование, реализация и пересмотр 8. Моделирование Монте-Карло 9. Мониторинг ключевых индикаторов риска
5.2. Поддержка использования подхода low-code / no-code для настройки правил и логики управления киберрисками;	Не поддерживается	Частично. Поддерживается подход no-code.	Частично. С базовыми элементами no-code.	Поддерживается. В решении реализован полноценный конструктор, позволяющий реализовать правила доступа к атрибутам объекта (скрытие видимости, чтение, редактирование, обязательность заполнения, ограничение допустимых значений) в зависимости от ролей пользователя и комбинаций условий по атрибутам карточки (например, этапам жизненного цикла). Поддерживается настройка выполняемых действий с объектами решения (рабочих процессов) в графическом редакторе блок-схем с применением подхода low-code / no-code, с ветвлениями и настройкой сложных условий выполнения действий с объектами решения, с выполнением математических, логических, текстовых операций, операций с массивами, с поддержкой тестового режима «прогона» рабочих процессов.
5.3. Возможность выполнения автоматической переоценки / пересчета киберрисков при изменении активов, уязвимостей, свойств инфраструктуры, ландшафта угроз, поверхности атаки, нормативных требований и т.д.;	Не поддерживается	Поддерживается автоматический пересчет при изменении нормативных требований.	Поддерживается	Поддерживается. Непрерывная автоматическая переоценка выполняется как по расписанию, так и по факту изменения исходных данных.
5.4. Учет весовых коэффициентов (значимость, опасность) различных активов, уязвимостей, угроз и последствий их реализации, защитных мер при проведении количественной оценки рисков;	Не поддерживается	Поддерживаются критерии значимости, свойства целостности, конфиденциальности, доступности для активов.	Поддерживается частично, только для качественной оценки рисков.	Поддерживаются различные веса/метрики (риск-аппетит, вероятность реализации угрозы, вероятность противодействия угрозе, степень ущерба, диапазоны ущерба и др.).

Название продукта, производителя	АльфаДок ООО “НПЦ “КСБ”	R-Vision SGRC ООО “Р-Вижн” Демонстрируется версия 5.4, заявленный вендором срок выхода: Q1 2025	Securitm ООО “Секьюритм”	Security Vision SGRC ООО “Интеллектуальная безопасность”
5.5. Моделирование киберрисков статистическими методами (например, методом Монте-Карло);	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается моделирование методом Монте-Карло.
5.6. Наличие мастеров моделирования угроз, управления киберрисками (пошаговое сопровождаемое решением заполнение данных для формирования базовых документов);	Не поддерживается	Не поддерживается	Поддерживается	Да, моделирование угроз выполняется пошагово. Все процессы сопровождаются различного рода справочной навигацией.
5.7. Связь процесса управления киберрисками с процессом управления соответствием, учет несоответствий как киберрисков;	Не поддерживается	Частично. Поддерживается связь рисков с активами, инцидентами.	Не поддерживается	Поддерживается двусторонняя связь реализованных/внедряемых мер защиты между модулями Compliance и Risk Management.
5.8. Моделирование киберрисков с применением методов машинного обучения, искусственного интеллекта;	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается
5.9. Поддержка проведения финансовой оценки киберрисков (с учетом оценочной стоимости активов, проведения атаки, реализации контрмер);	Не поддерживается	Поддерживается с помощью задания финансовой ценности актива, финансовых параметров мероприятий по обработке риска.	Не поддерживается	Поддерживается
5.10. Поддержка управления операционными рисками в соответствии с Положением ЦБ РФ №716-П;	Не поддерживается	Частично. Поддерживается схема оценки по 716-П	Не поддерживается	Поддерживается, отдельный функциональный модуль.
5.11. Мониторинг уровня киберрисков с применением ключевых индикаторов риска;	Не поддерживается	Не поддерживается	Поддерживается возможность создания ключевых индикаторов риска.	Поддерживается. Возможность использовать в качестве источников информацию из внешних систем и других решений вендора, в частности: различные атрибуты активов из AM, уязвимости из VM, инциденты из SOAR.
5.12. Отчетность по киберрисками: сводные отчеты по операционным рискам, ключевым индикаторам риска;	Не поддерживается	Не поддерживается, отчетность выпускается не по форме ЦБ РФ, а по форме вендора	Не поддерживается	Поддерживается
5.13. Визуализация состояния ИБ: предустановленные дашборды по операционным рискам, ключевым индикаторам риска.	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается
5.14. Визуализация: предустановленная интерактивная тепловая карта рисков (drilldown)	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается, с интерактивными переходами (drilldown).
6. Управление соответствием требованиям (Compliance)				
6.1. Наличие и число встроенных (“коробочных”) сценариев работы с оценкой соответствия и аудитами безопасности;	Не поддерживается	Не поддерживается	Поддерживается ручная экспресс-оценка, оценка через меры, оценка через метрики и уязвимости, опросы.	Ключевые коробочные сценарии работы с оценкой соответствия: 1. Жизненный цикл НМД 2. Жизненный цикл Мер защиты 3, Формирование области оценки соответствия 4. Универсальный процесс оценки соответствия различным НМД 5. Рассылка и заполнение опросных листов 6. Подготовка плана мероприятия по устранению несоответствий 7. Обработка задач на устранение несоответствий
6.2. Поддержка использования подхода low-code / no-code для настройки правил и логики управления соответствием требованиям;	Не поддерживается	Частично. Поддерживается подход no-code.	Частично. С базовыми элементами no-code.	Поддерживается. В решении реализован полноценный конструктор, позволяющий реализовать правила доступа к атрибутам объекта (скрытие видимости, чтение, редактирование, обязательность заполнения, ограничение допустимых значений) в зависимости от ролей пользователя и комбинаций условий по атрибутам карточки (например, этапам жизненного цикла). Поддерживается настройка выполняемых действий с объектами решения (рабочих процессов) в графическом редакторе блок-схем с применением подхода low-code / no-code, с ветвлениями и настройкой сложных условий выполнения действий с объектами решения, с выполнением математических, логических, текстовых операций, операций с массивами, с поддержкой тестового режима «прогона» рабочих процессов.
6.3. Поддержка импорта данных (отчетов, протоколов) мониторинга ИБ и прохождения мероприятий внутреннего контроля (включая опросы работников и самооценки), внешней оценки соответствия или аудита безопасности, оценки защищенности (пентест, Red Team, Bug Bounty), аттестации информационных систем;	Не поддерживается	Поддерживается в виде отображения на дашбордах	Частично поддерживается для импорта наборов требований, другие типы документов можно загрузить в решение в виде вложений.	Поддерживается, как вручную пользователем из файла в интерфейсе системы, так и посредством интеграции с использованием механизма коннекторов.
6.4. Поддержка ретроспективного анализа: ведение и отображение динамики соответствия требованиям, приведения в соответствие, проверки результатов приведения в соответствие, соблюдения SLA-метрик;	Поддерживается	Поддерживается в виде отображения на дашбордах	Частично	Поддерживается ведение и визуализация динамики оценки соответствия.
6.5. Поддержка восстановления конфигураций активов в эталонные безопасные значения в ручном и автоматическом режимах для соответствия требованиям;	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается, отдельный функциональный модуль SPC.
6.6. Возможность создания политик допустимых действий по устранению несоответствий в отношении определенных объектов (активов, информационных систем);	Не поддерживается	Не поддерживается	Не поддерживается, действия на конечных устройствах не выполняются.	Поддерживается

Название продукта, производителя	АльфаДок ООО “НПЦ “КСБ”	R-Vision SGRC ООО “Р-Вижн” Демонстрируется версия 5.4, заявленный вендором срок выхода: Q1 2025	Securitm ООО “Секьюритм”	Security Vision SGRC ООО “Интеллектуальная безопасность”
6.7. Возможность отмены действия (ручного, автоматического) по приведению в соответствие;	Не поддерживается	Не поддерживается	Не поддерживается, действия на конечных устройствах не выполняются.	Поддерживается, отдельный функциональный модуль SPC.
6.8. Возможность поддержки технологии динамических сценариев устранения несоответствий;	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается
6.9. Наличие мастера проведения оценки соответствия требованиям (пошаговое сопровождаемое решением заполнение данных для формирования базовой оценки);	Не поддерживается	Не поддерживается	Поддерживается	Да, процесс проведения оценки осуществляется пошагово. Все процессы сопровождаются различного рода справочной навигацией.
6.10. Возможность сопоставления сведений о несоответствии с релевантной информацией об инцидентах, уязвимостях, киберрисках на активе с соответствующей адаптацией способа и приоритета устранения несоответствия;	Не поддерживается	Поддерживается	Не поддерживается	Поддерживается
6.11. Использование внешних сервисов для получения обогащающей информации и рекомендаций по приоритизации, устранению недостатков конфигураций, уязвимостей (сервисы БДУ ФСТЭК России, CISA KEV, NIST NVD, Microsoft, Vulners.com, VulDB.com, OpenCVE.io, AttackerKB, Exploit-DB и т.д.).	Не поддерживается	Поддерживается через решение RV Endpoint. Интеграция с NVD, БДУ ФСТЭК России, НКЦКИ, Exploit-DB, Vulners.com.	Поддерживаются MITRE ATT&CK, БДУ ФСТЭК (старая и новая), уязвимости НКЦКИ, уязвимости БДУ ФСТЭК, CVE, каталог ПО CPE.	Поддерживается: БДУ ФСТЭК, NVD NIST, Microsoft, репозитории Linux (Debian, Ubuntu, Oracle, RHEL, Astra Linux, Alt Linux, Red OS и др.), OpenCVE, VulDB, Vulners.com, AttackerKB, Exploit-DB, НКЦКИ.
7. Управление безопасностью КИИ				
7.1. Возможность ведения реестра субъектов и объектов КИИ;	Поддерживается	Поддерживается	Поддерживается	Поддерживается
7.2. Реализация процесса категорирования объектов КИИ;	Поддерживается	Поддерживается	Частично	Поддерживается, категорирование производится в соответствии с требованиями ПП-127.
7.3. Автоматизация расчётов показателей значимости объектов КИИ;	Поддерживается	Поддерживается	Поддерживается	Поддерживается, расчет показателей критериев значимости ОКИИ производится в соответствии с требованиями ПП-127.
7.4. Формирование регуляторной отчётности по субъектам и объектам КИИ.	Поддерживается	Поддерживается	Частично	Поддерживается
8. Управление непрерывностью бизнеса				
8.1. Реализация процесса Business Impact Analysis;	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается проведение анализа воздействия на деятельность (Business Impact Analysis) с формированием опросных листов на основе данных графа связей объектов, автоматизированным формированием вопросов для опросных листов, анализом заполненных опросных листов, автоматическим обновлением соответствующих данных по объектам в ресурсно-сервисной модели.
8.2. Расчёт параметров RPO, RTO, MTD;	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается задание и автоматический расчет метрик: · Максимально допустимый период прерывания деятельности (MTPD / MTD); · Целевая продолжительность восстановления (RTO); · Целевая точка восстановления (RPO).
8.3. Формирование планов устранения недостатков;	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается
8.3. Формирование планов непрерывности;	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается, с включением в планы следующей информации: · Конкретные шаги по устранению сбоев; · Условия активации и деактивации плана; · Роли и обязанности, ключевые контакты; · Описание методов и средств коммуникации.
8.4. Реализация процесса тестирования планов непрерывности;	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается создание планов тестирования, в которых закладывается процедура проверки готовности и полноты планов непрерывности и восстановления для каждого инцидента (аварии, катастрофы), с формированием отчета о проведении тестирования и с механизмом планирования регулярных тестирований.
8.5. Учёт инцидентов нарушения непрерывности.	Не поддерживается	Не поддерживается, присутствует только в решении RV SOAR.	Не поддерживается	Поддерживается, с формированием отчетов и отображением информации на дашбордах.

Выводы

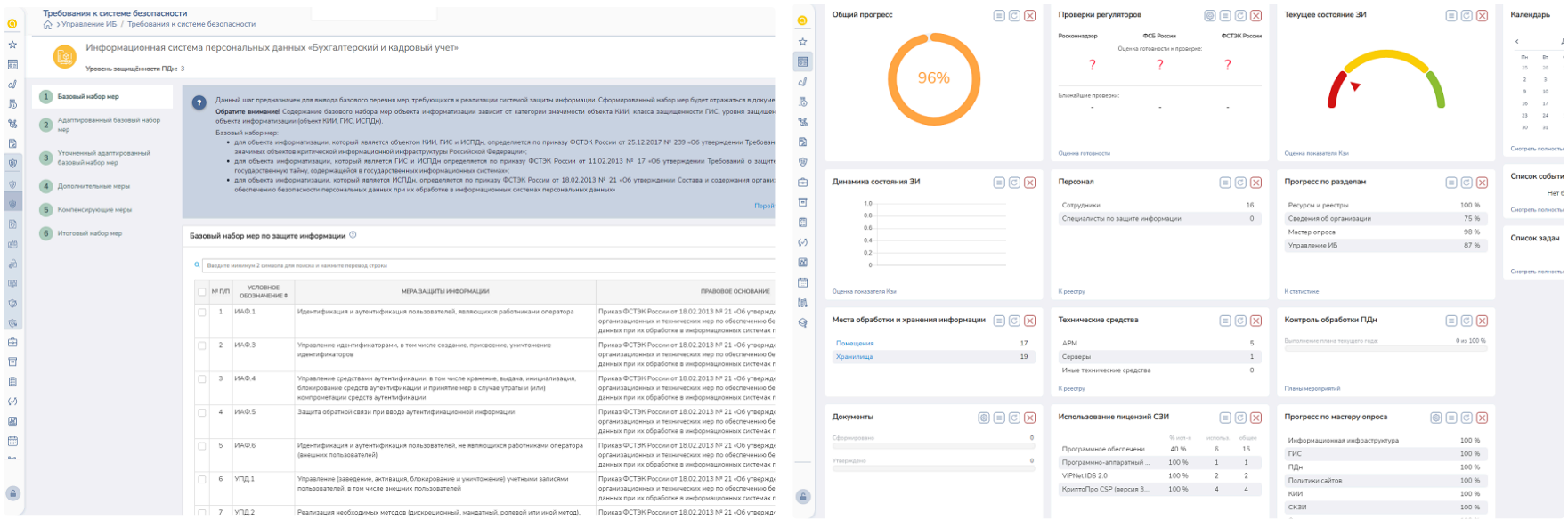
В сравнении принимали участие российские решения класса SGRC, которые могут быть установлены локально и позволяют автоматизировать следующие процессы кибербезопасности:

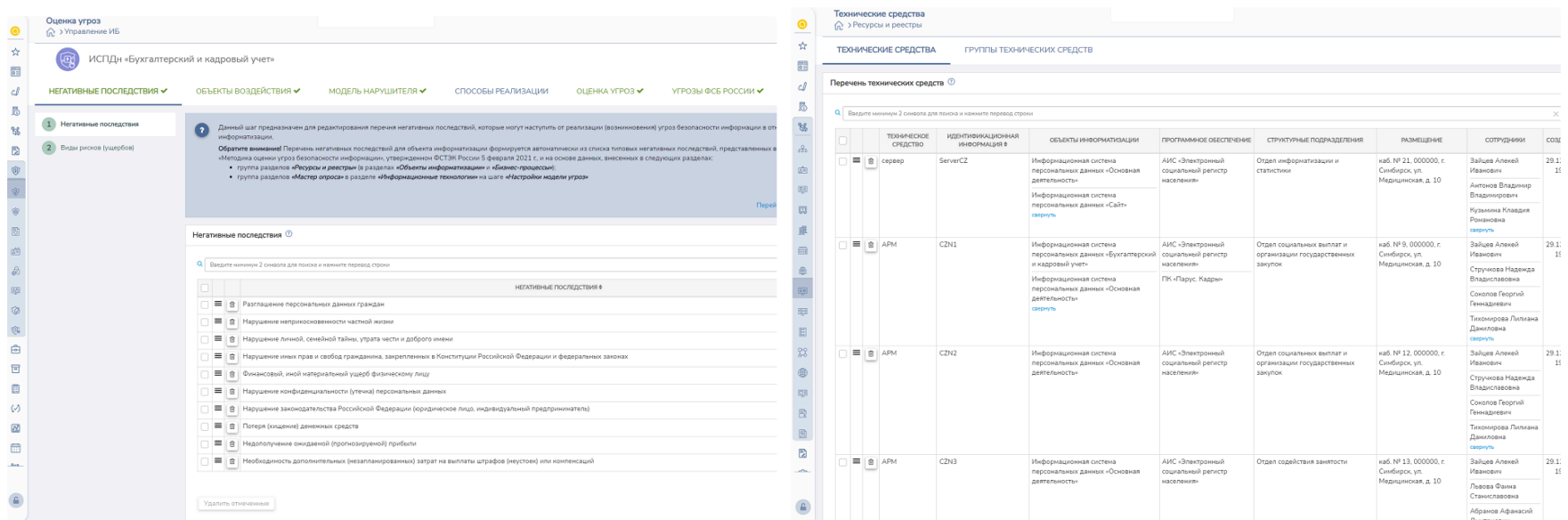
- Управление стратегией, документами и процессами ИБ (Governance);

- Управление киберрисками (Risk Management);
- Управление соответствием требованиям (Compliance).

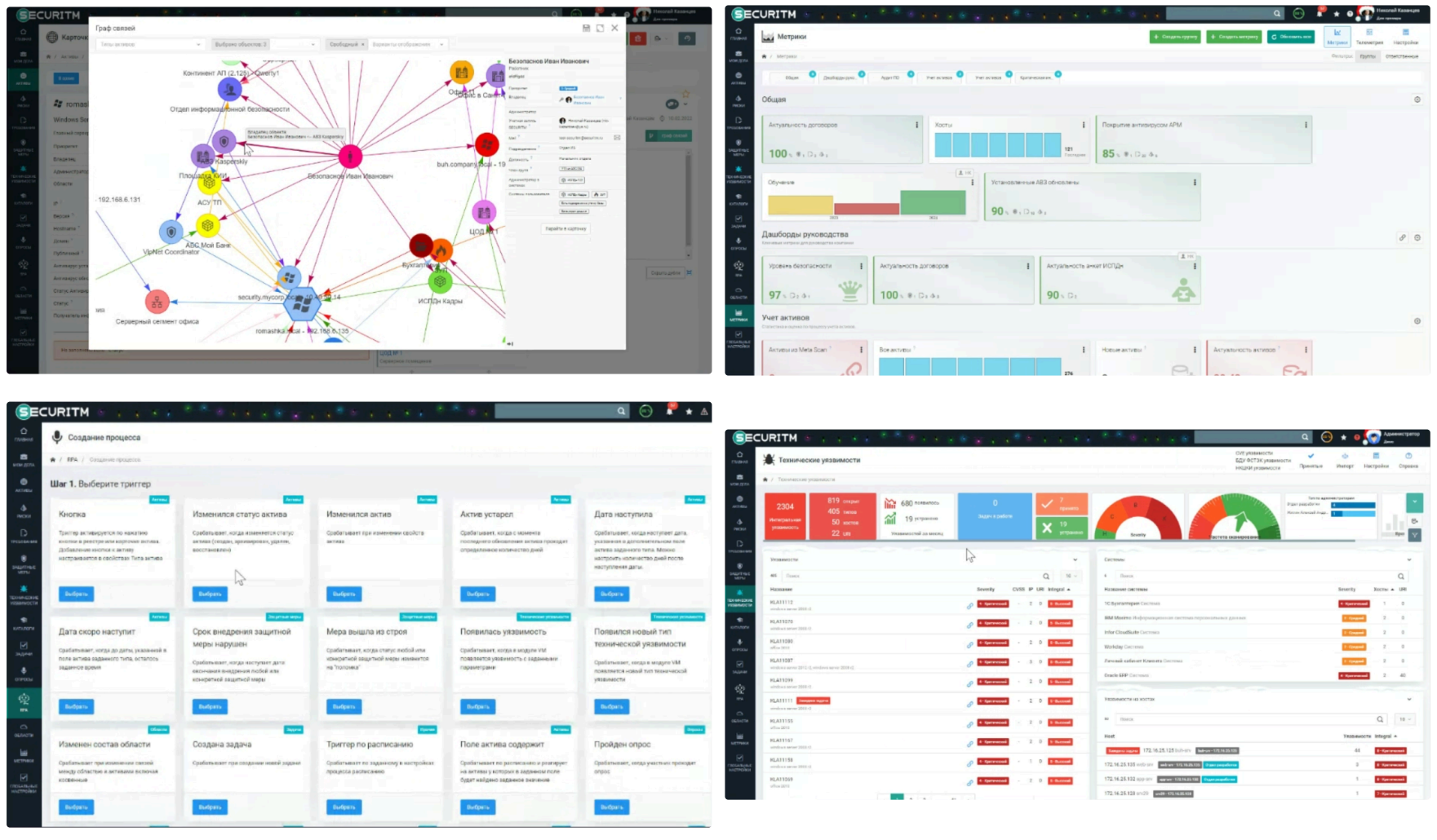
По результатам сравнения были выявлены следующие особенности и ограничения рассмотренных решений:

АльфаДок: Данное решение позволяет упростить формирование пакета документов по требованиям законодательства для защиты ГИС, объектов КИИ, персональных данных. Функционал включает автоматизацию базовых комплаенс-процессов, таких как проведение классификации ИСПДн и ГИС, категорирование объектов КИИ, моделирование угроз, нарушителей и формирование сценариев реализации угроз, а также разработка отчетной документации, оценка соответствия и визуализация состояния ИБ на дашбордах. Однако для формирования документов предполагается ручное заполнение опросных листов и форм экспертами, а список предустановленных интеграций ограничен утилитой для локального сканирования устройств “АРМ-сканер”. В базовой версии решение АльфаДок - облачное, но может быть установлено и локально. Сертификат ФСТЭК России отсутствует. Продукт подходит для рынка SMB, где данные аспекты менее важны.

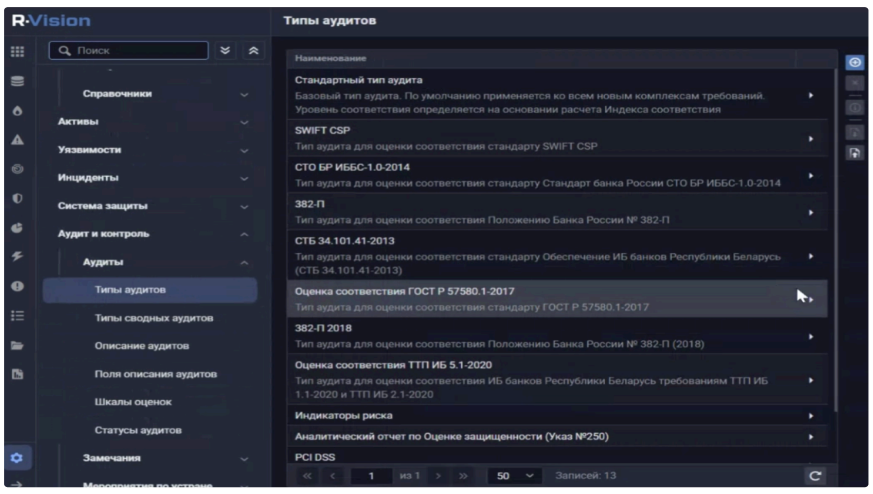


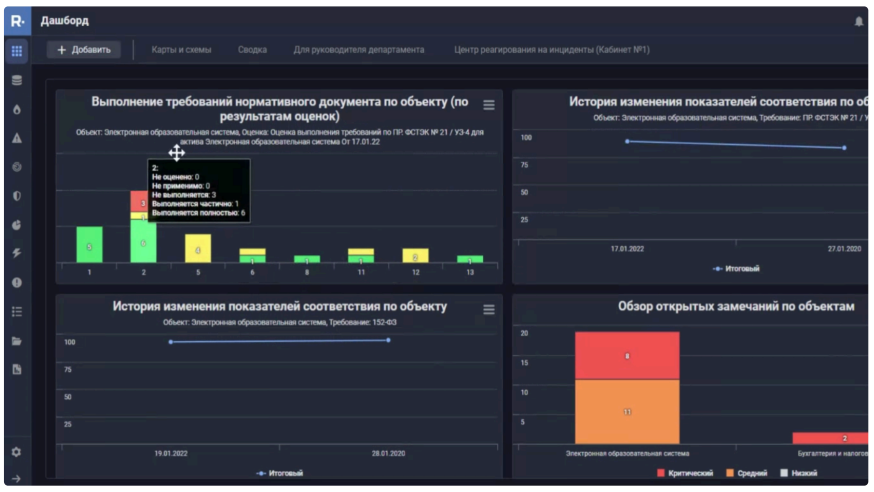


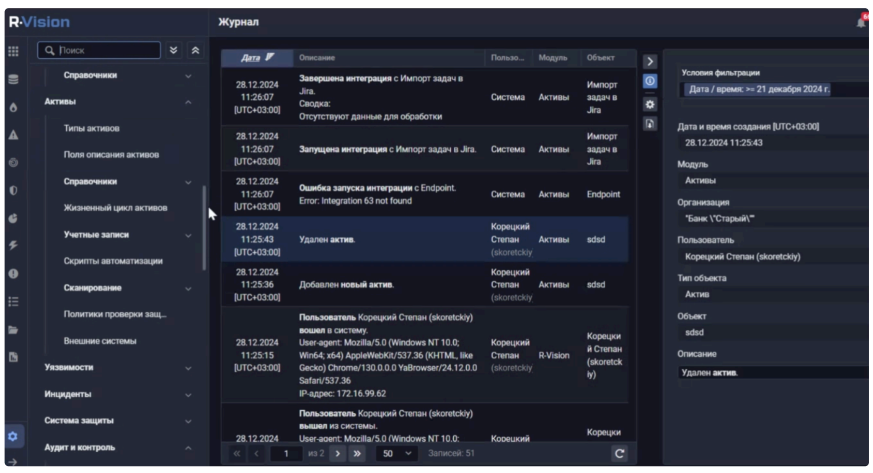
Securitm: Продукт обладает прозрачной ценовой политикой и может быть использован в бесплатном облачном режиме (Community-версия). В базовой версии решение - облачное, но может быть установлено и локально. В on-prem режиме поддерживается ряд интеграций с российскими и зарубежными ИТ/ИБ-продуктами, а также выполнение операций по триггеру в модуле роботизации - запуск скриптов и API-запросов. Слабой стороной можно считать отсутствие встроенной поддержки количественной оценки киберрисков и работы с операционными рисками по 716-П ЦБ РФ, отсутствие собственного движка сканирования активов (используется nmap), небольшое число предустановленных интеграций. Сертификат ФСТЭК России отсутствует. Добавление нового функционала требует доработки и включение часов разработки в пакет решения, подход low-code / no-code не поддерживается, но присутствуют базовые элементы no-code. Продукт подходит для рынка SMB, где данные аспекты менее важны.

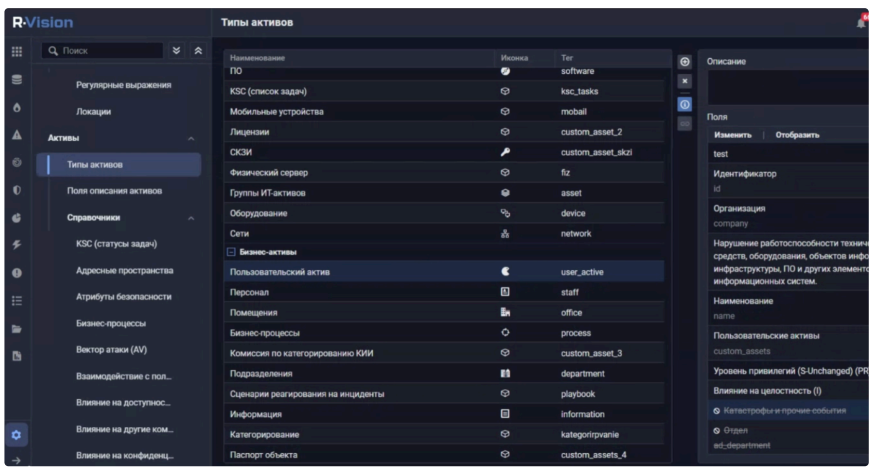


R-Vision SGRC: Данный продукт входит в экосистему R-Vision EVO и за счет интеграции с вендорскими продуктами для управления уязвимостями, техническими аудитами и киберинцидентами позволяет комплексно подойти к оценке. Решение поддерживает большое число интеграций с российскими и зарубежными ИТ/ИБ-продуктами, имеет широкие возможности по управлению киберрисками, позволяет формировать различную отчетность по ИБ. Продукт достаточно зрелый и позволяет обеспечить быстрое развертывание. Однако, отсутствует интеграция киберрисков и аудитов, а некоторая часть функционала решения становится доступной лишь при интеграции с дополнительными продуктами R-Vision, что повышает общую стоимость. Кроме того, решение “заточено” под ряд типовых задач, и для его настройки под нестандартные требования или специфические бизнес-процессы может потребоваться обращение к вендору. В обзоре участвовала самая последняя версия 5.4, которая пока что официально не была представлена; версия 5.3 сертифицирована во ФСТЭК России по 4 уровню доверия.

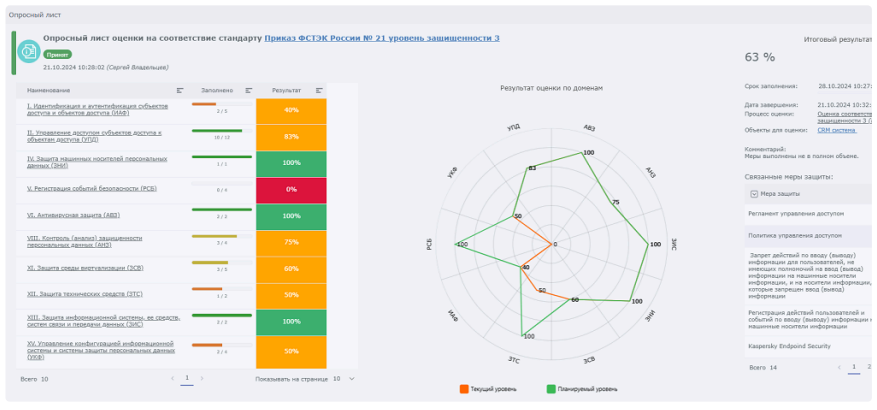


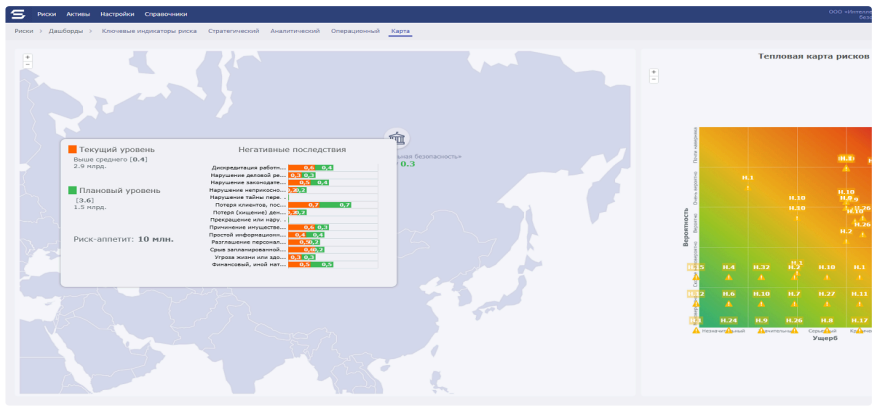


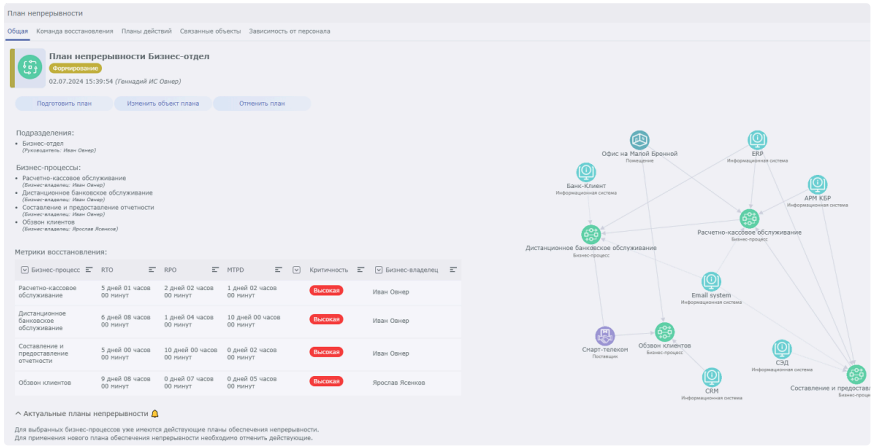


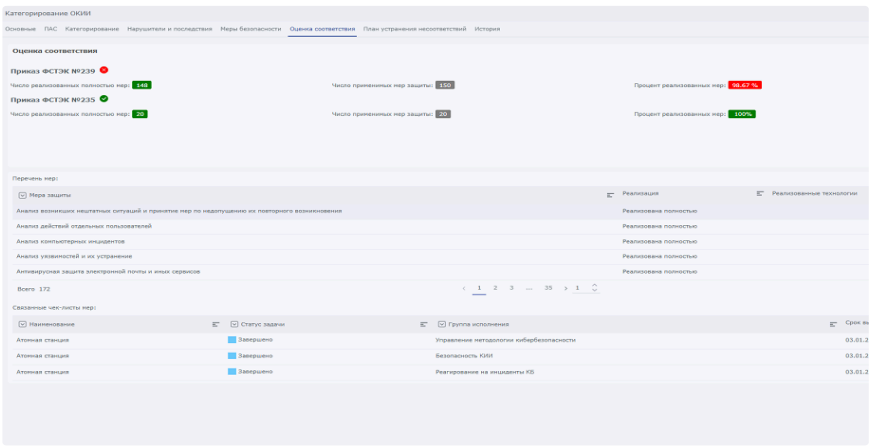


Security Vision SGRC: Это платформенное решение сочетает в себе функционал ряда модулей Security Vision, что позволяет консолидировать данные по активам, уязвимостям, киберинцидентам, данным аналитики киберугроз, а также обогатить информацию из внешних аналитических сервисов. Такой подход позволяет выстроить целостную картину состояния ИБ на основе объективных данных и использовать их в автоматизируемых процессах кибербезопасности в том числе с использованием технологии auto-SGRC. Вендор предлагает решение-конструктор, которое за счет технологий low-code / no-code может быть настроено заказчиками под себя без привлечения разработчиков и доработок со стороны производителя. Кроме того, поддерживается построение ресурсно-сервисной модели инфраструктуры и компании, моделирование рисков методом Монте-Карло, функционал управления непрерывностью и восстановлением бизнеса. Продукт отличается интеграцией с большим количеством ИТ/ИБ-продуктов и интернет-сервисов, гибкостью и возможностью тонкой настройки под любые особенности процессов компании, что может пригодится не только отделу ИБ, но и бизнес-подразделениям. К сожалению, решение предлагает лишь небольшой выбор встроенных ML-моделей и ограниченное число поддерживаемых внешних GPT-моделей, а также потребует прохождение обучения в учебном центре вендора для качественного администрирования. Ввиду комплексности функций продукт требует время на развертывание, но документация и справка компенсируют данный аспект. Продукт имеет сертификаты ФСБ, ФСТЭК, ОАЦ.









Редакция благодарит за помощь в подготовке обзора:

Команду Альфадок, за предоставление тестового доступа
Степана Корецкого, руководителя presale-группы, R-Vision
Ольгу Папину, менеджера по продуктовому маркетингу, R-Vision
Николая Казанцева, CEO Securitm
Романа Овчинникова, директора департамента внедрения, Security Vision
Андрея Амираха, руководителя отдела технического пресейла, Security Vision