Антон Ленский, РАССЭ (ГК «АйТеко»)

Владислав Вайц, МГТУ им. Н.Э. Баумана

Сравнение решений SGRC

Мы подготовили обзор и сравнение SGRC-решений, представленных на российском рынке информационной безопасности. В данном направлении работает не так много вендоров, поэтому в обзоре будут участвовать 5 игроков, из которых трое - отечественные.

Напомним, что термин SGRC означает Security Governance, Risk Management and Compliance, т.е. буквально «Управление безопасностью, рисками и соответствием законодательству». Платформы SGRC, исходя из их названия, решают следующие задачи:

- Governance - менеджмент информационной безопасности с процессами автоматизации управления активами, уязвимостями, документами, задачами, стандартами, а также с возможностью визуализации состояния ИБ и создания отчетности.
- Risk Management - управление киберрисками с автоматизацией риск-ориентированного подхода к обеспечению информационной безопасности, нацеленное на экономически обоснованный выбор оптимальных мер защиты, минимизирующих выявленные и рассчитанные риски.
- Compliance - обеспечение соответствия законодательству, отраслевым и внутренним стандартам и требованиям (комплаенс), с возможностью проведения аудитов и предоставления отчетности и результатов.

Дополнительно системы SGRC могут выполнять следующие функции:

- управление внутренними документами, базой знаний и решений, выполнение функции «внутренней Wiki» для департаментов ИБ;
- управление разнообразными бизнес-процессами, связанными с защитой информации;
- управление процессами взаимодействия с контрагентами по вопросам защиты информации;
- построение отчетов и визуализация состояния ИБ в виде интерактивных графиков и диаграмм;
- обеспечение интеграции с ОС, ПО, СЗИ для получения информации о состоянии компонент инфраструктуры;
- поддержка обработки инцидентов ИБ;
- поддержка управления процессами обеспечения непрерывности бизнеса и восстановления работоспособности;
- обеспечение поддержки принятия управленческих решений для руководства (ситуационная осведомленность).

Классические бизнес-ориентированные GRC-системы сфокусированы на более широких категориях управленческих процессов и рисков, чем специализированные SGRC-решения. Однако, специализация SGRC-продуктов на кибербезопасности привносит в решения дополнительный функционал, такой как автоматизация реагирования на инциденты ИБ, взаимодействие со средствами защиты, формирование специализированной отчетности.

В обзоре представлены основные игроки на рынке SGRC-систем:

- ePlat4m (Россия)
- Microsoft 365 Compliance Center (США)
- RSA Archer (США)
- R-Vision (Россия)
- Security Vision (Россия)

Сравнивать и анализировать данные решения мы будем по их общим, техническим и функциональным характеристикам и возможностям, делая после каждого раздела выводы.

Критерий сравнения	ePlat4m	Microsoft Compliance Center	RSA Archer	R-Vision	Security Vision
1. Сравнение общих и технических характеристик					
1.1. Требования к программному обеспечению					
Версия	1.8.6	June 2020	6.8	4.4	4.1.7
Вариант поставки	Установка on-premise и SaaS	Облачное решение (SaaS) в инфраструктуре Microsoft Azure	Установка on-premise и в облачной инфраструктуре Amazon Web Services, Microsoft Azure	Software appliance, есть возможность развернуть на физических серверах. При небольших расчетных нагрузках есть опция размещения всех компонент в режиме All-in-one (на одном сервере)	Software appliance, есть возможность развернуть на физических серверах. При небольших расчетных нагрузках есть опция размещения всех компонент в режиме All-in-one (на одном сервере)
Среды виртуализации	Нет	Облачное решение (SaaS)	VMware	VMware, VirtualBox, Hyper-V, Xen, Parallels	VMware, VirtualBox, Hyper-V, Xen, Parallels, KVM
Компоненты решения	Сервер СУБД, веб-сервер	Облачное решение (SaaS)	Сервер СУБД, веб-сервер, сервер служб	Сервер управления, сервер СУБД (может быть совмещен с сервером управления), центральный коллектор, коллектор инвентаризации	Сервер управления, сервер СУБД, сервисы коннекторов (коннекторы к источникам данных и коннекторы реагирования), сервис мониторинга
ОС	Microsoft Windows Server 2012 и выше	Облачное решение (SaaS)	Microsoft Windows Server 2012R2/2016	Сервер управления, коллекторы: CentOS 7, RHEL 7, Astra Linux CE 2.12, AltLinux Альт 8 СП Сервер СУБД: Ubuntu 14/16, CentOS 7, RHEL 7, Windows Server 2012/2016, FreeBSD 11	Сервер управления, сервисы коннекторов, сервис мониторинга: Microsoft Windows Server 2012R2 и выше, CentOS 7 и выше, RHEL 7 и выше, Ubuntu 14 и выше, Astra Linux CE, AltLinux, Альт. Сервер СУБД: Microsoft Windows Server 2012R2 и выше, CentOS 7 и

					выше, RHEL 7 и выше, Ubuntu 14 и выше, FreeBSD 11 и выше, Astra Linux CE, AltLinux, Альт
СУБД	MS SQL 2012 и выше, PostgreSQL	Облачное решение (SaaS)	MS SQL 2016	PostgreSQL v10 и выше	PostgreSQL v9.5 и выше, MS SQL 2014/2016 и выше
Клиентское ПО	Веб-браузер	Веб-браузер (Google Chrome, Mozilla Firefox, Internet Explorer, Edge)	Веб-браузер (Google Chrome, Mozilla Firefox, Internet Explorer, Edge)	Веб-браузер (Google Chrome, Mozilla Firefox, Internet Explorer)	Веб-браузер (Google Chrome, Mozilla Firefox, Internet Explorer, Edge, Yandex)
1.2. Требования к аппаратному обеспечению и инфраструктуре заказчика					
Архитектура процессора		Облачное решение (SaaS)	Любая, поддерживающая ОС сервера	x86	Любая, поддерживающая ОС сервера
Аппаратное обеспечение	8 ЦПУ 8 Гб ОЗУ	Облачное решение (SaaS)	Нет данных	В зависимости от количества активов, сценариев реагирования, пользователей системы: Сервер управления: 1– 22 ЦПУ 8 – 32 Гб ОЗУ Сервер СУБД: 1 – 16 ЦПУ 8 – 24 Гб ОЗУ Коллектор (рекомендуемые значения): 4 ЦПУ 8 Гб ОЗУ	Сервер управления: 1-12 ЦПУ 4-16 Гб ОЗУ Сервер СУБД: MS SQL/PostgreSQL: 1-16 ЦПУ 4-32 Гб ОЗУ Сервисы коннекторов, сервис мониторинга: 1-2 ЦПУ 2-4 Гб ОЗУ
Поддержка распределенного размещения компонент (географически	Нет данных	Облачное решение (SaaS), серверы распределены по всему миру	Нет данных	Да	Да

распределенные площадки, изолированные сегменты ЛВС)					
Оптимизация нагрузки (footprint) на ИТ-инфраструктуру заказчика при работе компонент решения	Нет данных	Асинхронное выполнение заданий	Нет данных	Алгоритмы оптимизации сетевого сканирования и снижения нагрузки на ЛВС	Алгоритмы оптимизации сетевого сканирования и снижения нагрузки на ЛВС, распараллеливание сканирования, разделение уровней глубины сканирования
Возможность установки обновлений решения через Интернет	Нет данных	Есть	Есть	Есть	Есть
Возможность установки обновлений решения без доступа к Интернет	Нет данных	Нет	Есть	Возможность локального обновления присутствует	Есть
1.3. Удобство эксплуатации, администрирования					
Документация	Предоставляется в виде pdf-документов	Предоставляется на веб-сайте Microsoft	Предоставляется в виде pdf-документов	Предоставляется в виде контекстной HTML-справки и в виде отдельного документа	Предоставляется в виде HTML-справки и в виде pdf-документов
Язык документации	Русский	Английский, русский (машинный перевод)	Английский	Русский	Русский
Язык интерфейса	Русский	Английский, русский (не все пункты меню	Английский	Русский, английский	Русский, английский, поддержка мультиязычности

		могут быть переведены с английского)			(возможность добавлять другие языки)
Темы оформления	Не поддерживается	Светлая, темная	Не поддерживается	Светлая, темная	Светлая, темная
Предоставляемые права доступа к ОС, на которой разворачиваются решения	Администратор	Ограниченные тенантом	Администратор	Root (полные)	Администратор/root (полные)
Методы аутентификации пользователей решения	Доменная аутентификация	Аутентификация через Azure AD	Доменная аутентификация (NTLM, Kerberos), встроенная аутентификация	Доменная аутентификация (NTLM, Kerberos), встроенная аутентификация. Примечание: доменная аутентификация требует предварительной настройки через Linux-консоль, поскольку сервер управления работает под управлением ОС Linux	Доменная аутентификация (NTLM, Kerberos, включая SSO), аутентификация посредством протокола Radius встроенная аутентификация. Примечание: поддержка назначения ролей пользователям системы на основе данных о членствах групп в Active Directory
Настройка сетевого взаимодействия	Конечный список требуемых протоколов и портов	Конечный список требуемых интернет-адресов, протоколов и портов. Список интернет-адресов может обновляться	Конечный список требуемых протоколов и портов. Как правило, везде используется порт TCP:443	Конечный список требуемых протоколов и портов, конфигурирование iptables осуществляется через Linux-консоль	Конечный список требуемых протоколов и портов, конфигурирование брандмауэра Windows осуществляется через GUI или командную строку. Конфигурирование iptables осуществляется через Linux-консоль
Настройка отображения информации	В зависимости от прав и роли пользователя	В зависимости от прав и роли пользователя	В зависимости от прав и роли пользователя	Возможность выбора пунктов из списка доступных элементов, сортировка данных, возможность	Полностью настраиваемое рабочее место для роли, предустановленные фильтры и параметры отображения, возможность настройки

				сохранять настроенные фильтры	состава отображаемых элементов, фильтрация с сохранением настроек, сортировка по всем данным, дополнительный функционал для сложной сортировка по всем данным
Поиск по всем объектам из единого интерфейса	Поиск по всем элементам	Поиск по всем элементам	Поиск по всем элементам	Поиск по всем элементам, в т.ч. связным	Глобальный поиск по всем объектам
Импорт, экспорт элементов решения	Экспорт в формат docx, xlsx, pdf	Некоторые элементы экспортируются в формат csv	Импорт/экспорт данных в формате xml, xls	Импорт данных об активах (типа Организации, Оборудование, Сети), результатов оценки Аудитов, требований для Аудитов, списка элементов из таблиц Excel (файл заданного шаблона). Экспорт данных об активах, списка элементов, задач, справочников (выборочно), отчетов, моделей угроз, журналов работы системы в форматах xlsx, docx, pdf. Экспорт элементов карт, схем в графический формат (png). Экспорт и импорт данных коннекторов в формат json	Импорт/экспорт любых данных в машиночитаемом виде. Экспорт отчетов в форматах xlsx, csv, docx, pdf. Импорт/экспорт любых объектов в формат csv, docx, pdf. Импорт/экспорт настроенных объектов и процессов во внутреннем формате. Экспорт элементов схем «Рабочих процессов» в графический формат (png, jpeg)

Способы оповещения пользователей	Отправка email	Отправка email, всплывающие уведомления в веб-интерфейсе	Отправка email	Отправка email	Отправка email, СМС, Telegram-уведомлений, звуковые оповещения и всплывающие уведомления в веб-интерфейсе
Настройка оповещений	Частичная настройка оповещений	Частичная настройка оповещений	Частичная настройка оповещений	Автоматическая генерация отчетов по расписанию, отправка уведомления ответственным (пользователи, роли) за определенный тип поручения (задача, уязвимость, замечание или проверка по аудиту), отправка уведомления о наступлении определенного события в системе (пользователи, активы, уязвимости, аудиты)	Возможность настроить произвольные пользовательские события для оповещения об изменениях в отслеживаемых свойствах объектов, настройка условий срабатывания оповещений (в зависимости от свойств контролируемых объектов). Полная настройка текста оповещения, с использованием атрибутов объекта, по которому происходит оповещение
Собственный API	Нет	Azure REST API	RESTful API Web API Собственный GRC API	REST API	REST API
1.4. Разграничение прав доступа к системе					
Модель разграничения доступа	Ролевая модель разграничения доступа. Дискреционная модель разграничения доступа	Ролевая модель разграничения доступа	Ролевая модель разграничения доступа	Ролевая модель разграничения доступа. Системные роли: доступ к разделам системы на чтение или изменение, например: Администратор, Пользователь, Менеджер по управлению рисками и т.д.	Ролевая модель разграничения доступа. Настраиваемые роли, на основании атрибутов объектов. Разграничение доступа ко всем объектам в системе с назначением прав на чтение, изменение, создание,

				Специальные роли: доступ к отдельным элементам системы, например: Владелец актива, Администратор безопасности, Аудитор безопасности и т.д.	выполнение групповых операций для конкретного пользователя/группы. Разрешения построены по принципу Модуль – Объект доступа – Право доступа – Политика
Поддержка гранулированного доступа	Нет данных	Да	Да	Возможность создавать пользовательские роли с разрешениями на выполнение конкретных действий с конкретными объектами, объединять пользователей в группы и назначать им роли	Возможность создавать пользовательские роли с разрешениями на выполнение конкретных действий с конкретными объектами, объединять пользователей в группы и назначать им роли. Возможность ограничивать доступ к просмотру определенных свойств конкретных объектов (например, определенных свойств активов, содержащих конфиденциальную информацию). Функционал рабочих процессов позволяет определять порядок взаимодействия с любым логическим объектом (инцидент, актив, уязвимость, задача и т.д.) различных групп пользователей, в том числе в зависимости от текущего состояния и значений свойств объекта, с

					учетом ролей и прав пользователей
1.5. Журналирование					
История действий пользователя	Ведется история действий пользователей и администраторов	Ведется история действий пользователей и администраторов	Ведется история действий пользователей и администраторов	Ведется история действий пользователей и администраторов во всех модулях, включая экспорт данных журнала и отправку его по syslog	Ведется история действий пользователей и администраторов во всех модулях, включая отправку информации об активности на email, по syslog и SNMP
Журналирование действий с объектами	Да, действия пользователей и системы	Да, действия пользователей	Да, действия пользователей и системы	Ведется история изменения всех элементов (изменение значения полей, действия с элементами, добавление объектов)	Ведется история изменения всех объектов (изменение свойств, состояний рабочего процесса, выполненных транзакций) с сохранением старого и нового значения измененного свойства
Мониторинг функционирования решения	Журналирование средствами ОС	Журналирование средствами системы	Журналирование средствами системы	Журналирование средствами ОС (текстовые файлы), журналирование путем записи событий в БД	Журналирование средствами ОС (Windows-журнал Application, текстовые файлы), журналирование путем записи событий в БД
Журнал безопасности решения	Системный журнал ОС	История входов и выходов пользователей, неудачные попытки входа, блокировки учетных записей, изменение прав доступа, изменение списка пользователей, смена пароля	История входов и выходов пользователей, неудачные попытки входа, блокировки учетных записей, изменение прав доступа, изменение списка пользователей, смена пароля	История входов и выходов пользователей, неудачные попытки входа, блокировки учетных записей, изменение прав доступа, изменение списка пользователей, смена пароля	История входов и выходов пользователей, неудачные попытки входа, блокировки учетных записей, изменение прав доступа, изменение списка пользователей, смена пароля, список IP-адресов, с которых осуществлялось подключение

1.6. Безопасность					
Защита коммуникаций между компонентами решения	Использование протоколов SSL/TLS	Использование протоколов SSL/TLS	Использование протоколов SSL/TLS	Использование протоколов SSL/TLS и возможность аутентификации по сертификатам между всеми компонентами системы, использование выданных Центром Сертификации/ Удостоверяющим Центром сертификатов. Примечание: настройка работы с PKI осуществляется через Linux-консоль	Использование протоколов SSL/TLS и возможность аутентификации по сертификатам между всеми компонентами системы, использование выданных Центром Сертификации/ Удостоверяющим Центром сертификатов
Защита доступа пользователей к веб-интерфейсу	Доступ к веб-интерфейсу через HTTPS	Доступ к веб-интерфейсу через HTTPS	Доступ к веб-интерфейсу через HTTPS	Доступ к веб-интерфейсу через HTTP/HTTPS, использование протокола TLS 1.2	Доступ к веб-интерфейсу через HTTPS, использование протокола TLS 1.2, возможность ограничения IP-адресов, которым разрешен доступ
Настройка тайм-аута веб-сессии	Нет данных	Да	Да	Да	Да
Настройка сложности и срока действия пароля (при использовании встроенной аутентификации)	Нет данных	Да	Да	Да	Да
Блокировка учетной записи при неуспешных	Нет данных	Да	Да	Алгоритм блокировки настраивается	Алгоритм блокировки настраивается

попытках аутентификации					
Двухфакторная аутентификация пользователей	Нет данных	Да, СМС, OTP	Нет данных	Да, по сертификатам	Да, по сертификатам
Ограничение доступа к решению на сетевом уровне	Нет данных	Через ограничение доступа к тенанту MS Azure	Средствами сервера MS IIS	Нет (только через iptables вручную через Linux-консоль)	Да, через веб-интерфейс: разрешение на доступ к системе только с определенного IP-адреса, из диапазона IP-адресов, из определенной подсети
Аутентификация на почтовом шлюзе	Нет данных	Да	Нет данных	Поддержка SSL-соединения, аутентификации на почтовом сервере	Поддержка SSL-соединения, аутентификации на почтовом сервере
1.7. Лицензирование					
Стоимость лицензии	Зависит от количества функциональных модулей, коннекторов к внешним ИС	По прайс-листу MS Office 365 с тарифным планом E5	Нет данных	Зависит от функционала, общего количества активов, количества коннекторов, кастомизации решения под конкретного заказчика, срока действия приобретаемой технической поддержки	Зависит от перечня выбранных функциональных модулей, количества коннекторов к источникам данных и коннекторов реагирования, возможности использовать режим высокой доступности/многонодности, выбранного уровня технической поддержки
Тип лицензии	Бессрочная	Подписка	Нет данных	Бессрочная	Бессрочная, срочная
Механизм лицензионной проверки	Нет данных	Онлайн-проверка действительности подписки	Нет данных	Лицензия устанавливается в виде файла, сопоставляемого с уникальным ID инсталляции	Лицензия устанавливается в виде текстового ключа, сгенерированного на основании уникального

					идентификатора инсталляции
Предоставление по модели SaaS	Есть	Есть	Нет данных	Нет	Нет
Техническая поддержка	В зависимости от приобретаемого уровня: 8x5 (GMT+5) Язык оказания услуги: русский	Есть Язык оказания услуги: русский, английский	Нет данных	Включает получение периодических обновлений, предоставление консультаций по использованию программного продукта, поддержку в режиме 24/7. Язык оказания услуги: русский, английский	В зависимости от приобретаемого уровня: 8x5 или 24/7, время реагирования на неисправность от 8 до 2 часов, предоставление патчей, бесплатное обновление до новых версий. Язык оказания услуги: русский, английский
Дополнительно-но		Решение поставляется в составе подписки MS Office 365 с тарифным планом E5	Нет данных	Пакеты экспертизы, комплексы требований по аудиту приобретаются отдельно	Вендор предлагает как «коробочное», так и полностью кастомизируемое под конкретного заказчика исполнение
1.8. Сертификаты					
Сертификаты	Продукт включен в Единый реестр российских программ для ЭВМ и баз данных	Нет	Нет	Сертификат соответствия ФСТЭК России № 4346 от 22.12.2020 по НДВ4, можно применять в значимых объектах КИИ 1 категории, АСУТП-1, ГИС-1, ИСПДн-1 и в информационных системах общего пользования II класса Продукт включен в Единый реестр российских программ для ЭВМ и баз данных	Сертификат соответствия ФСТЭК России № 4194 от 19.12.2019 по НДВ4 и ТУ, можно применять в значимых объектах КИИ 1 категории, АСУТП-1, ГИС-1, ИСПДн-1 и в информационных системах общего пользования II класса Продукт включен в Единый реестр российских программ для ЭВМ и баз данных

1.9. Внедрения (список заказчиков, из открытых источников)					
Внедрения	Нет данных	Нет данных	ПАО «Росбанк»	АО «РСХБ», Банк ВТБ (ПАО), ПАО «МТС-Банк», ОАО «РЖД», Банк ГПБ (АО), ФНС России, АО «СО ЕЭС»	ПАО Сбербанк, Государственная корпорация «Ростех», ПАО Банк «ФК Открытие», АО «Гознак», ФГУП «ГРЧЦ», ФСО России, ФАУ «Главгосэкспертиза России», «СДМ-Банк» (ПАО), АО «Газпром-медиа Холдинг»
1.10. Прочее					
Работа в режиме multitenancy	Нет данных	Есть	Нет данных	Да, с поддержкой разграничения доступа и ролевой модели для MSSP	Да, с поддержкой гранулярного разграничения доступа для MSSP
Отказоустойчивость	Да	Да	Нет данных	Да, в режиме Active-Passive, Active-Active	Да, аппаратное дублирование всех компонент системы, программное распределение задач для обеспечения отказоустойчивости и распределения нагрузки

Выводы по разделу №1

Решения ePlat4m и RSA демонстрируют достаточно типовой для бизнес-продуктов уровень сложности настройки, обслуживания и поддержки, если не брать в расчет разницу в стране-производителе и потенциальной стоимости решения.

Продукт ePlat4m пока не получил широкого распространения. Однако вполне правомерно, на наш взгляд, говорить о наличии позитивных перспектив реализации данного продукта на российском рынке, особенно среди государственных структур.

Решение RSA также продается в России не особенно активно. Кроме того, оно «заточено» под интеграцию в экосистеме продуктов от RSA и имеет единичные внедрения в России.

Аналогичным образом, решение от Microsoft сфокусировано на работе в стеке MS Azure и является, как и прочие Azure-решения, облачным, что накладывает ограничения на список потенциальных покупателей, учитывая строгие законодательные требования.

Решение R-Vision распространяется на рынке достаточно активно. Оно базируется на ОС Linux, что, как следствие, приводит к необходимости наличия в штате заказчика специалистов с необходимыми *NIX-компетенциями (работа в командной строке, настройка системных утилит Linux). Одновременно, однажды будучи настроенным, такое решение, скорее всего, покажет продолжительный Uptime.

Продукт Security Vision пользуется спросом на российском рынке. Security Vision может функционировать в привычной среднему пользователю Windows-среде, что упрощает процесс настройки (например, его легко интегрировать в текущую среду Microsoft Active Directory), а также несколько снижает требования к компетенциям администрирующего эту систему сотрудника. Security Vision поддерживает Open Source инсталляции на базе ОС Linux и СУБД PostgreSQL, что снижает требования к финансовым затратам на ИТ-инфраструктуру заказчика.

В плане удобства эксплуатации и администрирования наиболее привлекательными представляются Microsoft Compliance Center, R-Vision и Security Vision. Документация решения R-Vision выглядит основательной, также удобной показалась контекстная справка с поиском. У Microsoft Compliance Center и Security Vision имеется документация не только на русском, но и на английском языке, а также оказывается мультиязычная техническая поддержка.

Security Vision предлагает наибольшее разнообразие типов оповещений: отправку email, СМС, Telegram-уведомлений, звуковые оповещения и всплывающие уведомления в веб-интерфейсе. У ePlat4m, RSA Archer и R-Vision заявлена только поддержка уведомлений по email, у Microsoft Compliance Center - поддержка уведомлений по email и всплывающие уведомления в веб-интерфейсе.

В плане сертификации вполне закономерно лидируют отечественные продукты. Все три рассматриваемых нами российских системы - ePlat4m, R-Vision и Security Vision - включены в Единый реестр российских программ для ЭВМ и баз данных. R-Vision и Security Vision обладают сертификатами соответствия ФСТЭК России.

2. Сравнение функциональных возможностей 2.1. Управление информационной безопасностью					
2.1.1. Инвентаризация и управление активами					
Перечень поддерживаемых типов активов	Материальные и нематериальные активы: • процессы • информация • системы • сети • оборудование • пользователи	Материальные и нематериальные активы: • информация • системы • оборудование • ПО • уязвимости • пользователи	Материальные и нематериальные активы: • информация • системы • оборудование • ПО • уязвимости • пользователи	Два класса активов (бизнес-активы и ИТ-активы), но в рамках каждого класса можно задавать новые типы активов. Предустановленные типы активов: • Организация (подразделения) • Бизнес-процессы • Информация • Персонал • Помещения • Оборудование Сети • ПО • Домены • Уязвимости • Группы ИТ-активов (информационные системы)	Любые типы активов. Работа с активами настраивается через универсальный функционал рабочих процессов, реализующих механизм обработки и жизненного цикла логических объектов, включая активы. Предусмотрен графический редактор конструктора рабочих процессов. Предустановленные типы активов: • Бизнес-процесс • Информационная система • Техническое средство • ПО • Лицензия • Информация
Перечень поддерживаемых свойств активов	Нет данных	Свойства активов не кастомизируются	Нет данных	Свойства активов определяются в справочниках. В справочники можно добавить свои элементы. Добавление нового справочника не поддерживается. Предустановлены порядка 10 видов справочников (типы	Произвольные свойства активов, можно создавать пользовательские свойства. Поддерживается связь свойств активов с элементами справочников, баз знаний. Типы свойств: временной интервал, дата/время, группа

				активов, атрибуты безопасности, бизнес-процессы, информационные активы, типы оборудования и т.д.)	сотрудников, да/нет, дробное/целое число, текст/расширенный текст (с поддержкой HTML-разметки), связанные активы, сотрудники, файл, справочник
Связи между активами	Да	Да, связи между оборудованием, ПО, пользователями, уязвимостями	Да	Установка связей между активами типов: оборудование, группы ИТ-активов, бизнес-процессы, информация. Установка связей («Влияет на» или «Зависит от») атрибутов безопасности (целостность, конфиденциальность, доступность) между активами. Есть классификатор активов с возможностью автоматической категоризации активов по применимым нормативным требованиям. Активы связаны с модулем «Аудиты» – в свойстве актива находится привязка к проведенным аудитам, нарушениям требований на активе и связанном оборудовании, помещении,	Предусмотрена настройка типов связи («Связаны» или «Зависит от») между любыми типами объектов. Взаимодействие между активами настраивается через универсальный функционал рабочих процессов, реализующих механизм обработки любых логических объектов, включая активы. Предоставляется возможность связывать активы с любыми типами объектов в системе: документы, файлы, законодательные требования, задачи, инциденты (функционал IRP) и т.д. Поддерживается мониторинг изменения свойств связанных активов с выполнением автоматических действий

				системе, а также план работ по устранению нарушений. Активы связаны с модулем «Управление рисками» и категорированием объекта в рамках требований по защите КИИ. Поддерживается быстрый переход от актива к связанному с ним оборудованию, применимым стандартам/требованиям, инцидентам (функционал IRP)	при наступлении определяемых пользователем условий
Объем собираемой и инвентаризируемой информации об оборудовании (встроенными средствами решения)	Нет данных	• Имя устройства • IP-адрес • MAC-адрес, количество сетевых интерфейсов • Тип ОС • Тип оборудования • Имя домена • Аппаратные характеристики (ЦПУ, ОЗУ, жесткий диск) • Установленное ПО (версия) • Список доменных пользователей	Нет данных	• Имя устройства • IP-адрес • MAC-адрес, количество сетевых интерфейсов • Маска подсети • Тип ОС • Тип оборудования (в зависимости от типа установленного ПО), роль (в случае серверной ОС Windows) • Физическая/ виртуальная машина • Имя домена/рабочей группы • Аппаратные характеристики (ЦПУ, ОЗУ, жесткий диск)	• Имя устройства • IP-адрес • MAC-адрес, количество сетевых интерфейсов • Маска подсети • Тип ОС • Тип оборудования • Физическая/ виртуальная машина • Имя домена/рабочей группы • Аппаратные характеристики (ЦПУ, ОЗУ, жесткий диск) • Установленное ПО (версия, дата установки)

		• Параметры безопасности ОС • Уязвимости		• Установленное ПО (версия, дата установки) • Список локальных/доменных пользователей/ администраторов (имя пользователя, дата последнего входа) на устройстве • Список доменных групп безопасности, включенных в локальные группы безопасности на устройстве • Параметры безопасности ОС (состояние антивирусного средства с указанием версии, состояние межсетевого экрана, состояние службы обновления ОС, параметры подключения USB устройств) • Уязвимости (путем интеграции со сторонним решением vulners.com) • Дополнительные поля для ручного ввода (статус актива,	• Список локальных/доменных пользователей/ администраторов • Список доменных групп безопасности, включенных в локальные группы безопасности на устройстве • Параметры безопасности ОС • Уязвимости • Дополнительные поля для ручного ввода

				ответственный, инвентарный номер и т.д.)	
Функционал встроенных средств инвентаризации	Нет данных	Агентная инвентаризация проводится с помощью установленного на устройстве Microsoft Defender ATP, SCCM-клиента	Нет данных	• Безагентная инвентаризация осуществляется коллектором R-Vision: сканирование заданной сети с использованием nmap с последующим удаленным входом на устройство (WMI, MS RPC для Windows-систем; SSH/SNMP для Linux/Unix-систем, сетевого оборудования Cisco, Juniper, HP) • Выполнение на коллекторах системы проприетарных скриптов (типа R-Vision) для автоматизации действий по сбору инвентаризационной информации • Запуск локальных логон-скриптов VBScript на устройствах, недоступных для удаленного входа, с последующей	• Безагентная инвентаризация осуществляется коннектором сбора данных Security Vision, в котором поддерживаются следующие протоколы и механизмы: DNS, HTTP, HTTPS, IMAP, MS RPC, POP3, SMTP, SNMP, SSH, SSL, Syslog, TLS, WindowsShell, WMI; механизмы подключения к службам каталогов Active Directory и СУБД Microsoft SQL, MySQL, Oracle, PostgreSQL; механизмы API (REST, SOAP) • Универсальный коннектор Security Vision, обеспечивающий подключение практически любой системы, способной предоставить данные

				отправкой собранных данных в POST-запросе на коллектор • Универсальный коннектор для интеграции с произвольными базами типов MS SQL, Oracle, PostgeSQL, импорт данных из произвольной Excel-таблицы • Собранные данные о полномочиях пользователей на устройствах агрегируются в справочнике «Привилегии пользователей» • Возможность задавать пользовательские группы ПО с отнесением к ним различного ПО путем применения regex-выражений • Поиск установленного ПО в задаваемых пользователями каталогах • Сканирование обнаруженных подсетей, связанных с сетевыми адаптерами	в машиночитаемом виде • Алгоритм дедупликации данных гибко настраивается в соответствии с логическими правилами (сравнение свойств событий) • Механизм настройки правил фильтрации и группировки позволяет настраивать любую логику выборки, связывания и группирования полученных сведений о просканированных активах • Возможность мониторинга сетевой доступности, качества связи с устройствами и состояния работоспособности активов (по протоколам ICMP, TCP, UDP, SNMP, Syslog) с визуализацией полученных данных на графиках • Возможность удаленного входа на просканированное

				проинвентаризированных устройств • Алгоритм дедупликации активов (учитывается уникальность MAC, UID, наличие файла-маркера на просканированной системе)	оборудование (по RDP, SSH) • Менеджеры коннекторов реагирования могут автоматически распределять задачи между собой для обеспечения отказоустойчивости и распределения нагрузки в процессе инвентаризации
Объем собираемой и инвентаризируемой информации об оборудовании (по данным от подключенных систем)	Количество данных зависит от конкретной системы-источника	• Установленное ПО (версия, количество инсталляций, лицензий, срок действия лицензий) • Аппаратные характеристики • Уязвимости	Количество данных зависит от конкретной системы-источника	• Установленное ПО (версия, количество инсталляций, лицензий, срок действия лицензий) • Аппаратные характеристики • Уязвимости • Пользователи (доменные): ФИО, имя учетной записи, должность, подразделение, данные о прохождении awareness-программ • Состояние средств защиты информации на устройствах (статус DLP-агентов, антивирусов, средств защиты от НСД и т.д.)	Количество данных зависит от конкретной системы-источника. Ниже представлены примеры популярных источников: Kaspersky Security Center: Сетевое имя, сетевой адрес, сервер антивируса, домен, время последней доступности, время последнего обновления, время последнего сканирования, группа антивируса, видимость узла, статус установки агента, статус запуска агента, статус службы защиты в режиме реального времени, платформа ОС, количество выявленного вредоносного ПО, количество невылеченного вредоносного

					ПО, архитектура процессора, время последней загрузки, операционная система, версия и наименование антивируса, дата обновления баз сигнатур. MaxPatrol 8: сетевой адрес, сетевое имя операционная система, установленное программное обеспечения, версии ПО, путь установки ПО, полная информация по всем уязвимостям. MS SCCM: сетевой адрес, идентификаторы, домен, сетевое имя, операционная система, MAC адрес, статус активации автообновления. Указанный выше список не является конечным: другие источники-системы передают в систему свои перечни данных
Настройки механизма инвентаризации	Нет данных	Автоматическое сканирование, сканирование по требованию	Нет данных	Настройка запуска скриптов автоматизации (целевая группа устройств, расписание запуска). Настройка политики назначения атрибутов – логика заполнения свойств обнаруженных активов (например, связь устройства с информационной системой,	Механизм инвентаризации гибко настраивается в рамках логического рабочего процесса инвентаризации. Предусмотрены ручные (выполнение действий по команде пользователя) и автоматические (выполнение действий при наступлении определенных условий) транзакции-действия на

				группирование активов по задаваемым критериям). Настройка политики обнаружения ПО (поиск определенных файлов и каталогов на устройствах). Настройка политик сканирования (расписание, используемые учетные записи, сканируемые подсети ЛВС). Настройка политики защищенности персонала – построение карты «уязвимостей» сотрудников в зависимости от результатов учебных фишинговых атак и прохождения сотрудниками обучения в системе «Антифишинг»	целевой системе, настраиваемые в рамках рабочего процесса инвентаризации с использованием графического редактора. В качестве действий предусмотрено создание нового объекта, изменение свойств текущего объекта, наполнение справочников, выполнение скриптов автоматизации (Bash, PowerShell, Batch, cmd, Java, Javascript, Python), выполнение запросов к системам (SNMP, SOAP, REST, DNS), выполнение запросов к базам данных (MS SQL, MySQL, Oracle, PostgreSQL). Предусмотрен чат по объектам, в рамках которого пользователи системы могут общаться по связанным с активом задачам
Возможности интеграции со сторонними решениями	MaxPatrol 8 MaxPatrol SIEM Micro Focus ArcSight ESM RedCheck Механизмы:	Aruba ClearPass Policy Manager AttackIQ Platform Azure Sentinel Better Mobile BitDefender Blue Hexagon Corrata	MaxPatrol 8 Micro Focus ArcSight ESM Nessus Qualys RSA Netwitness SIEM, другие продукты RSA Symantec SIM	Active Directory AlienVault Atlassian JIRA Cisco (SSH, REST) CMDB iTop Forcepoint AP-DATA Fortinet FortiMail Fortinet FortiSandbox	Active Directory Apache Kafka Atlassian Confluence Atlassian JIRA Cisco (SSH, REST, SNMP) Cisco FirePower Cisco IronPort/ESA CMDB iTop

	RDBMS (ODBC, OLEDB) SOAP WS REST WS LDAP POP3/SMTP XML (файл) MS EXCEL (файл)	CyberMDX CyberSponse CyOps Cymulate Cyren Wen Filter Delta Risk ActiveEye Demisto IBM QRadar Lookout MTP Micro Focus ArcSight ESM MISP ThreatSharing Morphisec Nexpose Rapid7 Palo Alto RSA Netwitness SIEM SafeBreach ServiceNow Skybox Splunk Swimlane Symantec Endpoint Protection Mobile THOR Cloud ThreatConnect Vectra NDR XM Cyber Zimperium		Gigamon GigaVue-Fm Group IB Bot-Trek Intelligence HP Comware HP SM (REST) IBM QRadar Imperva InfoWatch Device Monitor InfoWatch Traffic Monitor Juniper Kaspersky Fraud Prevention Kaspersky Security Center Lieberman ERPM MaxPatrol 8 MaxPatrol SIEM McAfee ePO McAfee ESM Micro Focus ArcSight ESM Micro Focus UCMDB MS Exchange MS SCCM MS SQL MS System Center Endpoint Protection MS TMG MySQL Naumen CMDB Naumen Service Desk Nessus Nexpose Rapid7 OpenStack OpenVAS Oracle DB Palo Alto PostgreSQL QLikView	CheckPoint CheckPoint SandBlast FireEye FireEye IPS Fortinet Fortimail Fortinet FortiSandbox Fortinet SIEM Gigamon GigaVue-Fm HP SM (REST, SOAP) HP SM ADV IBM MQ IBM QRadar (REST) Imperva SecureSphere InfoWatch Traffic Monitor Juniper Kaspersky IPS Kaspersky Security Center Lieberman ERPM MailArchiva MaxPatrol 8 MaxPatrol SIEM McAfee ESM Micro Focus ArcSight ESM MS Exchange MS SCCM MS SQL MS System Center Endpoint Protection MS TMG MXtoolBox MySQL Naumen Service Desk Nessus OpenStack Oracle DB

				Qualys RedCheck Secret Net Secret Net Studio Solar JSOC Splunk StoneGate Symantec Endpoint Protection VMware Vulners.com Zabbix Антифишинг Примечание: При интеграции с Active Directory собираются ограниченные свойства учетных записей (ФИО, имя учетной записи, должность, подразделение), отсутствует возможность настройки получения значений иных свойств. Получаемые от интегрированных систем данные ограничены статусом СЗИ, техническими характеристиками устройств, списком устройств, пользователей, ПО, уязвимостей. Подключение новой системы занимает от 1 дня	OTRS Palo Alto Ping-Admin.ru PostgreSQL QLikView Qualys RedCheck RSA Netwitness SIEM RuSIEM ScanOVAL Skybox (REST, SOAP) Splunk Symantec Critical System Protection Symantec Endpoint Protection Symantec IPS TripWire URLScan.io VirusTotal VMware ESXi VMware vCenter Zabbix 1С АС Банка Государственные интернет-сервисы (ФССП, ЕГРЮЛ, ЕГРИП и т.д.) КИБ СёрчИнформ Консультант + Портал ДЗО СКУД (различные производители) СПАРК-Интерфакс ФПСУ-IP ФПСУ-TLS

					Примечание: С подключаемых систем можно получать, обрабатывать, нормализовать и загружать в Security Vision любые данные, которые может предоставить целевая система, в том числе неструктурированные (XML, JSON, CSV, TXT, Binary). Поддерживаются запросы к внешним общедоступным сервисам (Google API, Яндекс API). Подключение новой системы занимает 1-2 часа
Необходимые права доступа для сбора инвентаризационных данных	**Нет данных**	Агентная инвентаризация	Нет данных	Для сканирования Windows-систем требуется предоставить учетной записи права локального администратора на целевом устройстве.	Для сканирования Windows-систем требуется предоставить учетной записи права локального администратора на целевом устройстве. Для подключения к Active Directory можно использовать стандартные полномочия пользователя домена
Метрики процесса инвентаризации активов	**Нет данных**	Визуализация устранения уязвимостей, применения рекомендованных настроек безопасности,	Нет данных	Типы метрик: время реагирования на инцидент (функционал IRP), исполнение сроков реагирования, понесенный и	Любые требующиеся метрики, задание пользовательских алгоритмов и логики

		состояния информационной безопасности (Security Score, Compliance Score) в виде графиков		предотвращенный ущерб. Создание дополнительных пользовательских метрик не поддерживается. Метрики ведутся для активов типа «Организация» («Подразделения»), «Бизнес-процессы», «Группы ИТ-активов». Поддерживается изменение пороговых значений для метрик и задание персональных метрик для определенных активов. Визуализация метрик: графический (графики, цветовая индикация) и цифровой (текст) вид	сравнения, произвольные пороговые значения. Создание метрик для любого типа логических объектов, включая активы. Визуализация метрик: в виде интерактивных диаграмм и дашбордов с функцией Drill-Down, графиков, отчетов
2.1.2. Управление уязвимостями					
Источники информации об уязвимостях	Интеграция со сканерами уязвимостей	Собственный репозиторий, репозиторий MITRE	Интеграция со сканерами уязвимостей	Полученные по результатам инвентаризации данные об установленном ПО соотносятся с базой уязвимостей Vulners.com, которая агрегирует данные из различных репозиториев уязвимостей (CVE, вендорские базы). Интеграция с БДУ ФСТЭК России. Интеграция со сканерами уязвимостей	Интеграция с БДУ ФСТЭК России, ПО ScanOVAL. Интеграция со сканерами уязвимостей. Возможна интеграция с любым репозиторием уязвимостей

Критерии критичности уязвимостей	Соответствует критериям, используемым сканерами уязвимостей	Соответствует нотации CVSS v3	Соответствует критериям, используемым сканерами уязвимостей	Собственная метрика критичности R-Vision (5 уровней)	Гибко настраивается. По умолчанию соответствует нотации CVSS v3
Типы уязвимостей	• Уязвимости ПО	• Уязвимости ПО • Уязвимости конфигураций	• Уязвимости ПО	• Уязвимости ПО	• Уязвимости ПО • Уязвимости конфигураций
Данные об уязвимостях	Нет данных	Нет данных	Нет данных	• Описание уязвимости • Источник • Уровень критичности • Связанные узлы/группы активов/сети/ оборудование • Информация для устранения уязвимости • Временные метрики (даты обнаружения, открытия, последнего обновления, устранения, закрытия, установки отметки «ложное срабатывание»)	• Количество уязвимых активов • Статус устранения уязвимости • Источник • Идентификаторы в различных системах • Описание • Краткое описание • Способ исправления: • CVSS (базовая оценка) • CVSS (временная оценка) • CVSSv3 (базовая оценка) • CVSSv3 (временная оценка) • Метрики эксплуатируемости базовой оценки • Метрики эксплуатируемости временной оценки • Ссылки • Наличие публично доступного эксплойта

					• Дата первого обнаружения • Дата последнего обнаружения • Время устранения • Время закрытия
Настройка процесса управления уязвимостями	Нет данных	Установка статусов уязвимостей. Ручное или автоматическое назначение ответственного за устранение уязвимостей и постановка сроков	Нет данных	Установка статусов уязвимостей (открыта/закрыта) вручную или автоматически по результатам инвентаризации/сканирования. Ручное или автоматическое назначение ответственного за устранение уязвимостей и постановка сроков (в зависимости от уровня критичности). Оповещение ответственных по email. Возможность вручную завести инцидент по результатам обнаружения определенной уязвимости, при этом в свойствах инцидента отсутствует динамическое обновление информации об активах с обнаруженной впоследствии аналогичной уязвимостью	Процесс управления уязвимостями гибко настраивается в рамках логического рабочего процесса управления уязвимостями. Предусмотрены ручные (выполнение действий по команде пользователя) и автоматические (выполнение действий при наступлении определенных условий) транзакции-действия в целевой системе, настраиваемые в рамках рабочего процесса управления уязвимостями с использованием графического редактора. В качестве действий предусмотрено создание нового объекта, изменение свойств текущего объекта, наполнение справочников, выполнение скриптов автоматизации (Bash, PowerShell, Batch, cmd, Java,

					Javascript, Python), выполнение запросов к внешним системам, выполнение запросов к базам данных. Выполнение скриптов автоматизации позволяет запустить произвольный процесс обработки уязвимостей (установка/удаление ПО, изменение ключей реестра, конфигурационных файлов, настроек устройств и т.д.). Рабочий процесс управления уязвимостями может включать в себя постановку задач на устранение уязвимостей, маршрутизацию задач исполнителям, контроль качества и сроков устранения уязвимостей и т.д. Предусмотрен чат по объектам, в рамках которого пользователи системы могут общаться по связанным с уязвимостью задачам
Виртуальный патчинг уязвимостей	Нет	Нет	Нет	Нет	Да, путем выполнения скриптов автоматизации

(используя встроенный функционал решения)					
2.1.3. Управление задачами, документами, требованиями					
Настройка процесса управления задачами	Поддерживается ручное и автоматическое создание задач	Поддерживается ручное создание задач	Поддерживается ручное создание задач	Поддерживается ручное и автоматическое создание задач. Автоматически задачи создаются из модулей «Аудит и контроль» и «Инциденты» в результате привязки замечаний по аудиту к активам организации или добавления действий по инциденту	Процесс управления задачами гибко настраивается в соответствии с логическим рабочим процессом, с выполнением автоматических и ручных действий. Процесс управления задачами может полностью воспроизвести принятый в организации механизм обработки заявок любого характера, включая не только ИБ/ИТ-задачи, но и произвольные бизнес-процессы
Функционал процесса управления задачами	Возможность устанавливать степень критичности задачи, контроля исполнения, отправки оповещений по email. Возможность создавать отчетность по задачам	Просмотр задач в интерфейсе системы. Возможность устанавливать степень критичности задачи, контроля исполнения, отправки оповещений по email	Просмотр задач в интерфейсе системы. Возможность устанавливать степень критичности задачи, контроля исполнения, отправки оповещений по email	Возможность просматривать информацию по задачам, формировать список задач, добавлять комментарии и документы к задачам, экспортировать задачи в Excel-файл. Присутствует светофорная индикация статуса задачи, назначаются 4 уровня важности задачи.	Автоматические и ручные действия по задаче могут включать в себя уведомление пользователей, выполнение скриптов автоматизации на целевой системе, создание подзадач (декомпозиция), назначение ответственных в зависимости от свойств задачи, эскалацию задачи при превышении сроков выполнения или увеличении критичности и т.д.

				Возможность присвоения задачи ответственному, оповещения по email, распределения подзадач сотрудникам с указанием родительской задачи (декомпозиция).	Ведение перечня задач во взаимосвязи с ролевой моделью. В системе присутствуют функции сервис-деск с маршрутизацией и отслеживанием задач по линиям L1-L2-L3 Центров SOC. Присутствует возможность управления задачами с использованием функционала «Базы знаний/решений», в которой накапливается и анализируется информация по ранее решенным задачам с возможностью поиска наиболее подходящего решения на основе нейронной сети с динамическими весовыми коэффициентами и с механизмом «обучение с учителем». Предусмотрен чат по объектам, в рамках которого пользователи системы могут общаться по назначенным задачам

Настройка процесса управления документами и требованиями	Настройка процесса управления требованиями подразумевает создание перечня стандартов и нормативных требований, используемых при проведении аудитов	Использование встроенного перечня стандартов и рекомендаций, составление своего перечня	Использование встроенного перечня стандартов и рекомендаций, составление своего перечня	Настройка процесса управления требованиями подразумевает создание перечня стандартов и нормативных требований, используемых при проведении аудитов. Требования связываются со списком контрольных проверок, поддерживается создание пользовательских контрольных проверок и задание их весовых коэффициентов. Управление документами осуществляется путем создания списка документов, описывающих защитные меры (регламенты, политики) с указанием утверждающего, даты создания и планового пересмотра с напоминанием о сроках. Документ связывается с объектами ИТ-инфраструктуры, подпадающими под его действие	Настройка процесса управления требованиями подразумевает создание перечня стандартов и нормативных требований, используемых при проведении аудитов. Создание рабочего процесса для управления документами и требованиями/стандартами позволяет реализовывать произвольную логику их обработки: назначение ответственных и сроков пересмотра с оповещением, изменение свойств других объектов (например, повышение критичности актива при попадании его в поле действия отраслевого/ государственного стандарта), объединение в группы, экспорт/импорт и т.д.
Функционал процесса управления документами и требованиями	Поддерживается добавление пользовательских стандартов и	Поддерживается добавление пользовательских стандартов и	Поддерживается добавление пользовательских стандартов и	Поддерживается добавление пользовательских стандартов и нормативных требований.	Поддерживается добавление пользовательских документов, стандартов и нормативных требований.

	нормативных требований	нормативных требований. Поддерживается создание пользовательских контрольных проверок (assessments)	нормативных требований	Поддерживается создание контрольных проверок, объединяемых в группы и чек-листы, для отслеживания соответствия требованиям и назначенным защитным мерам. Список защитных мер: пользовательский список, типовой каталог защитных мер R-Vision, SANS CIS Critical Security Controls v6, v7. Загрузка, изменение, удаление в системе произвольного документа (в т.ч. с файловым вложением), с автоматическим назначением ответственного за загруженный объект	Список защитных мер: пользовательский список, авторский каталог защитных мер Security Vision, SANS CIS Critical Security Controls v6, v7
2.1.4. Мониторинг состояния информационной безопасности					
Визуализация	Типы панелей графического отображения: • Карты • Дашборды Функционал Drill-Down	Типы панелей графического отображения: • Карты (режимы карт: карта мира, схемы взаимосвязей) • Графики • Дашборды Функционал Drill-Down	Типы панелей графического отображения: • Графики • Дашборды	Типы панелей графического отображения: • Карты (режимы карт: карта мира, карта сетей, планы помещений, схемы взаимосвязей) • Графики • Схемы • Дашборды Типы графиков:	Встроенный конструктор отчетов и дашбордов для использования любых данных и тонкой настройки отображаемой информации. Визуализация произвольных данных, получаемых путем создания SQL-запросов к БД. Экспорт графических представлений в форматы pdf, jpg, png.

				• Аудит и контроль • Управление инцидентами (более 10 предустановленных диаграмм) • Управление активами (более 10 предустановленных диаграмм) • Управление рисками, включая визуализацию ущерба от киберинцидентов Функционал карт: • Отображение инцидентов, активов, уязвимостей, групп ИТ-активов на географических картах • Функционал Drill-Down (переход с карты на инциденты/активы с просмотром подробных сведений), • Поиск активов по карте • Переход с активов на сетевую схему • Отображение активов на планах помещений • Экспорт карт (формат png)	Импорт графических представлений из форматов jpg, png. Во всех графических представлениях предусмотрен поиск по объектам, функционал Drill-Down, быстрый переход к связанным объектам (активам, инцидентам). Графические представления (виджеты) с поддержкой интерактивного взаимодействия для формирования дашбордов любого состава и конфигурации. Предустановленные типы отображения данных для виджетов: • Линейный график • Гистограмма • Таблица • Секторная диаграмма • Список • Календарь инцидентов Предустановленные панели визуализации: • Операционный дашборд (информация

				• Импорт пользовательских планов помещений (форматы png, jpg) Функционал графиков: • Указание пользовательского временного диапазона для построения графика • Построение произвольных графиков • Построение графиков по параметрам заранее созданного фильтра • Конструктор графиков (типы диаграмм: круговая, столбчатая, линейная) Функционал схем: • Связывание произвольных типов инцидентов/активов друг с другом • Визуализация активов на сетевой схеме Функционал дашбордов: • Диаграммы и метрики, отображающие историю, текущие	по киберинцидентами) • Тактический дашборд (статистическая информация, визуализация динамики инцидентов) • Общий дашборд по рискам (визуализация динамики киберрисков, распределение рисков, история) • Расширенный дашборд по рискам для информационных систем (распределение рисков, история) Географическая карта с визуализацией зданий, населенных пунктов, планеты. Отображение характеристик, взаимосвязей, взаимодействий между объектами, включая активы и инциденты, с отображением доступности устройств и сервисов. Визуализация предустановленных объектов на карте:

				статусы, события и статистику • Визуализация данных по оборудованию, рискам, показателям соответствия (аудиту), уязвимостям, ПО, ОС	• Активы (инциденты, уязвимости, риски, связанные с активами) • Инциденты (с визуализацией источников атак и атакуемых активов) • Филиалы и отделения (отображение активов и консолидированной информации по географическим пунктам)
Отчетность	Экспорт отчетов в форматах docx, xlsx, pdf. Создание отчетов по расписанию и вручную, отправка по email. Создание пользовательских отчетов	Экспорт отчетов в форматах csv, pdf. Создание отчетов по расписанию и вручную, отправка по email. Создание пользовательских отчетов	Экспорт отчетов. Создание отчетов по расписанию и вручную, отправка по email. Создание пользовательских отчетов	Экспорт отчетов в форматах docx, pdf. Создание отчетов по расписанию и вручную, отправка по email. Создание пользовательских отчетов. Предустановленные отчеты: • Отчет по киберрискам • Отчет по соответствию требованиям (ГОСТ Р 57580.2-2018, ГОСТ Р ИСО/МЭК 27001-2006, 187-ФЗ, 152-ФЗ, НПА ФСТЭК России (Приказы №№ 17, 21, 31, 239), внутренние требования) • Банковская отчетность (382-П, СТО БР, PCI DSS) • Отчет по аудитам	Встроенный конструктор отчетов и дашбордов для использования любых данных и тонкой настройки отображаемой информации. Создание отчетов по произвольным данным, получаемым путем создания SQL-запросов к БД. Полная настройка под нужды заказчика. Экспорт отчетов в форматах xlsx, docx, pdf, xml, csv. Создание отчетов по расписанию и вручную, доставка по email/в файл/по API в форматах xml, pdf, doc, xls, ppt. Возможность построения сводных отчетов по параметрам справочников/

				• Отчет по всем типам активов • Отчет по уязвимостям • Отчет по инцидентам (сводка, статистика, распределение) • Отчет по формам ЦБ РФ (0403202, 0403203) • Модель Угроз (по требованиям ФСТЭК России)	перечней, использования аналитических и прогнозных инструментов анализа данных с графическим отображением, интеграции с внешними системами визуализации. Автоматизация внутренней отчетности по существующим формам и конструктор отчетов для любых форм: • по аудитам разного типа и отдельным сканированиям и пентестам • по результатам оценки по методикам компании, динамике ее изменения • по выполнению задач отдела и линий обработки задач; • в соответствии с технологией auto-SGRC; Предустановленные отчеты: • Отчет по киберрискам (сводный, детализированный) • Отчет по соответствию требованиям (ГОСТ Р

					ИСО/МЭК 27001-2006, 187-ФЗ, 152-ФЗ, GDPR, НПА ФСТЭК России (Приказы №№ 17, 21, 31, 235, 239), внутренние требования) • Банковская отчетность (ГОСТ Р 57580, 382-П, СТО БР, PCI DSS, 672-П, 683-П, 684-П, SWIFT CSCF 2020) • Отчет по аудитам, включая функционал «Кабинет аудитора» – выделенную и изолированную рабочую область для проведения внешних аудитов • Отчет по всем типам объектов, включая инциденты, активы и уязвимости (динамика, статистика) • Отчет по формам ЦБ РФ (0403202, 0403203) • Модель Угроз (по требованиям ФСТЭК России)

Повышение осведомленности	Внутренняя система тестирования знаний пользователей	Проведение учебных фишинговых рассылок, сбор статистики, обучение внутри системы	Нет данных	Проведение учебных фишинговых атак и прохождение сотрудниками обучения в системе «Антифишинг»	Возможность автоматизированной рассылки контента: создание/получение (вручную, из внешних ресурсов), классификация и хранение, отправка разными каналами (email, API). Возможность удаленного анкетирования, форм обратной связи. Возможность запроса материалов/обучения-методических консультаций и т.д.
Автоматическая корректировка настроек средств и систем	Нет	Частично (может быть реализовано с применением функционала MS Flow / Power Automate)	Нет	Нет	Да, с помощью механизма auto-Compliance (авторская технология auto-SGRC): автоматическое изменение настроек ОС/ПО/СЗИ для соответствия внутренним нормативным требованиям / возврата к baseline-настройкам
2.2. Управление киберрисками					
Настройка процесса управления киберрисками	Этапы настройки процесса управления киберрисками: • Ручной выбор активов для проведения оценки рисков • Назначение владельца риска	Этапы настройки процесса управления киберрисками: • Классификация данных • Подключение коннекторов данных	Этапы настройки процесса управления киберрисками: • Определение бизнес-контекста управления рисками • Оценка рисков	Этапы настройки процесса управления киберрисками: • Подготовка, создание оценки: выбор методики оценки рисков, допустимых уровней риска, оценки ценности актива. Данные заполняются	Этапы настройки процесса управления киберрисками: • Определение карты рисков организации • Формирование перечня актуальных угроз информационной безопасности (по

	• Оценка рисков: качественная оценка рисков • Частичный автоматический расчет рисков для связанных активов • Обработка рисков: создание плана обработки рисков • Формирование отчетности	• Выбор и назначение политик управления данными (настройка DLP, Retention Policies, прав доступа) • Автоматическая оценка рисков • Формирование отчетности	• Настройка метрик рисков и контролей • Реагирование на изменение рисков и ошибки контролей	через опросник. Настройка справочника со степенями финансового, административного и репутационного ущерба, задание ценности активов • Идентификация рисков: указание источников угроз, предпосылок и реализованных защитных мер (заполняются автоматически, если для актива ведется учет защитных мер). Список рисков выстраивается автоматически на основании связей в каталогах рисков, при этом учитываются связи активов • Оценка рисков: возможно выполнить автоматически на основании внесенных сведений либо вручную с привлечением экспертов. Доступен просмотр подробной	БДУ ФСТЭК России, пользовательский перечень) • Формирование перечня уязвимостей, через которые возможна реализация угроз (типовые уязвимости, пользовательский перечень) • Формирование перечня мер защиты (типовые меры защиты, пользовательский перечень) • Определение области оценки и сбор информации о текущих бизнес-процессах • Формирование модели угроз и нарушителя для каждого актива • Проведение комплексной автоматизированной оценки рисков ИБ с привлечением экспертов от различных структурных подразделений

				информации о рисках (источники, предпосылки, защитные меры, инциденты, план обработки) • Обработка рисков: создание плана обработки рисков, указание мероприятий (вручную или заполнение из свойств риска). Типы мероприятий: внедрение/изменение защитной меры/разовое мероприятие (т.е. минимизация риска), уход от риска, передача риска. Для каждого мероприятия указываются ответственный, сроки, рассчитывается стоимость мероприятия. Есть возможность оценить стоимость реализации всего плана обработки рисков. Поддерживаются просмотр плана обработки рисков актива из свойств	• Выработка плана обработки рисков, контроль за стадиями его выполнения и результатами применения защитных мер Процесс управления киберрисками гибко настраивается в соответствии с логическим рабочим процессом с выполнением автоматических и ручных действий. Процесс управления киберрисками может полностью воспроизвести принятый в организации механизм обработки рисков любого характера, включая выстраивание системы управления операционным риском (СУОР) по требованиям ЦБ РФ

				актива и просмотр всех запланированных мероприятий по обработке рисков. • Утверждение результатов оценки рисков • Формирование отчетности	
Функционал процесса управления киберрисками	Поддерживается выполнение следующих действий для управления киберрисками: • Формирование модели угроз • Проведение оценки рисков, в т.ч. производных рисков для связанных активов	Поддерживается выполнение следующих действий для управления киберрисками: • Автоматическое формирование списка рекомендаций • Тестирование рекомендованных действий • Выполнение рекомендованных действий • Назначение ответственных • Контроль статуса задач	Поддерживается выполнение следующих действий для управления киберрисками: • Проведение оценки рисков • Подготовка и контроль реализации плана обработки рисков • Оценка эффективности предпринимаемых мер по обработке киберрисков	Поддерживается выполнение следующих действий для управления киберрисками: • Формирование модели угроз • Проведение оценки рисков, в т.ч. производных рисков для связанных активов • Автоматический поиск актуальных рисков на основе каталогов угроз (по авторской «типовой базе угроз ИБ R-Vision», по БДУ ФСТЭК России, по пользовательскому каталогу угроз) • Подготовка и контроль реализации плана обработки рисков • Оценка экономической эффективности предпринимаемых мер	Поддерживается выполнение следующих действий для управления киберрисками: • Ведение реестра рисков (уязвимости, вероятность реализации угроз, активы под угрозой) • Проведение быстрой оценки рисков сотрудниками компании собственных бизнес-процессов без привлечения сотрудников подразделения ИБ • Визуализация информации о киберрисках на дашбордах • Автоматическое формирование отчетов по управлению рисками

				по обработке киберрисков Методологии (схемы) оценки рисков: • Пользовательская схема оценки • Авторская схема оценки рисков R-Vision • Упрощенные качественные схемы оценки • Упрощенные количественные схемы оценки • Схема оценки угроз по проекту «Методики моделирования угроз безопасности информации» ФСТЭК России • По методике оценки рисков ЦБ РФ (РС БР ИББС-2.2-2009) • По международным методологиям (ALE, FAIR, ISO 27005, NIST, OCTAVE) Предустановленные справочники: • моделирование угроз • моделирование нарушителя	Методологии (схемы) оценки рисков: • Пользовательская схема оценки • Схема оценки угроз по проекту «Методика моделирования угроз безопасности информации» ФСТЭК России • По методике оценки рисков ЦБ РФ (РС БР ИББС-2.2-2009) • По международным методологиям (FAIR, OCTAVE, ALE, ISO 27005, , NIST, Quantitative Risk Assessment Method) Предусмотрены ручные (выполнение действий по команде пользователя) и автоматические (выполнение действий при наступлении определенных условий) транзакции-действия, настраиваемые в рамках рабочего процесса управления киберрисками с использованием графического редактора. В качестве действий

				• проведение оценки рисков Создание пользовательских справочников не поддерживается, но возможно добавить новые элементы в существующие справочники. Поддерживается создание пользовательских критериев оценки ценности активов. Поддерживается выстраивание связи между оценкой риска актива и произошедшими с ним инцидентами. Поддерживается создание пользовательских угроз, ограниченных типами угроз в соответствии с методологией 1119-ПП в части актуальности угроз использования НДВ в системном/прикладном ПО. Поддерживается журналирование всех выполненных действий при работе с киберрисками.	предусмотрено создание нового объекта (включая, например, заявку на заполнение экспертом опросника по рискам), оповещение ответственных сотрудников (например, владельцев риска), выполнение скриптов автоматизации (Bash, PowerShell, Batch, cmd, Java, Javascript, Python), выполнение запросов к внешним системам, выполнение запросов к базам данных. Выполнение скриптов автоматизации позволяет запустить процесс обработки киберрисков (изменение настроек устройств и СЗИ/ПО/ОС, установка/удаление ПО, возврат активов в baseline-состояние). Рабочий процесс управления каберрисками может включать в себя постановку задач по выполнению пунктов плана обработки рисков, маршрутизацию задач исполнителям, контроль

					качества и сроков предпринимаемых мер по обработке рисков и т.д. Предусмотрен чат по объектам, в рамках которого пользователи системы могут общаться по связанным с конкретным риском/угрозой/ уязвимостью/мерой защиты задачам. Поддерживается журналирование всех выполненных действий в рамках рабочего процесса управления киберрисками
2.3. Управление аудитами и соответствием требованиям (комплаенс)					
Настройка процесса управления аудитами и соответствием требованиям	Нет данных	Этапы настройки процесса управления аудитами и соответствием требованиям: • Выбор релевантных стандартов • Доработка списка требований под конкретную инфраструктуру • Выбор мер защиты (контролей)	Нет данных	Этапы настройки процесса управления аудитами и соответствием требованиям: • Загрузка в систему перечня требований/стандартов для проведения аудита • Настройка шкалы оценок, уровней замечаний по аудиту, а также комплекса контрольных проверок, связанных с требованиями применимых стандартов	С помощью механизма auto-Compliance (авторская технология auto-SGRC) процесс управления аудитами и соответствием требованиям гибко настраивается в соответствии с логическим рабочим процессом. Этапы настройки процесса управления аудитами и соответствием требованиям: • Формирование списка требований

		• Проведение оценки соответствия • Назначение задач, ответственных • Отчетность, контроль выполнения		• Планирование аудитов с поддержкой выполнения данного действия из свойств актива. Актив связывается с перечнем реализуемых защитных мер и применимых к нему требований • Проведение проверки с поддержкой отправки email-уведомления о дате проверки, совместной работы (простановка оценок и замечаний по аудиту, общение в чате по аудиту), возможность прикрепить вложение к задаче аудита, создание отчетов • Внесение и анализ замечаний по аудиту с выбором замечаний из выпадающего списка или заполнение вручную • Формирование и контроль реализации планов по устранению замечаний, создание соответствующей задачи, декомпозиция	• Настройка рабочего процесса управления аудитами и соответствием требованиям • Сбор информации и статистики • Создание объектов контроля • Подготовка чек-листов • Проведение оценки выполнения требований • Формирование отчетности • Подготовка «Кабинета аудитора» – выделенной и изолированной рабочей области для проведения внешних аудитов • Корректировка настроек устройств, ПО, СЗИ, ОС для автоматического устранения выявленных замечаний

				мероприятий и задач на подзадачи	
Функционал процесса управления аудитами и соответствием требованиям	Поддерживается выполнение следующих действий для управления аудитами и соответствием требованиям: • Создание моделей нарушителей и моделей угроз по требованиям ФСТЭК и ФСБ • Подготовка документации для соответствия законодательству по защите персональных данных • Конструирование программы аудита, формирование плана и группы аудита • Создание пользовательских критериев оценки с указанием весовых коэффициентов	Поддерживается выполнение следующих действий для управления аудитами и соответствием требованиям: • Выбор требований для конкретной индустрии (финансы, энергетика, образование, медицина, государственные организации) • Выбор применимых законодательных требований, в том числе GDPR, HIPAA, SEC, SoX и т.д. • Планирование мероприятий для соответствия нормативам GDPR, ISO 27001, NIST 800-53 • Создание собственных требований	Поддерживается выполнение следующих действий для управления аудитами и соответствием требованиям: • Выбор требований (Use Case) для конкретной индустрии • Выбор применимых требований • Создание собственных требований • Уведомление ответственных за задачи	Поддерживается выполнение следующих действий для управления аудитами и соответствием требованиям: • Подготовка и контроль замечаний по аудиту с автоматическим созданием соответствующей задачи ответственному сотруднику на устранение недостатков, с синхронизацией статусов задачи и замечания, с уведомлением ответственных по email, с поддержкой отправки задач на устранение замечаний во внешние системы Service Desk • Проведение контрольных проверок – контроль выполнения законодательных норм и защитных мер. Назначение контрольных проверок активам после связывания активов с защитными мерами и	Поддерживается выполнение следующих действий для управления аудитами и соответствием требованиям: • Централизованное управление процессом проведения аудитов, с обеспечением постоянной актуальности данных • Выполнение скриптов автоматизации позволяет запустить процесс устранения выявленных в ходе аудита замечаний (изменение настроек устройств и СЗИ/ПО/ОС, установка/удаление ПО, возврат активов в baseline-состояние) • рабочий процесс управления аудитами и соответствием требованиям может включать в себя постановку задач по выполнению пунктов плана аудита,

	• Формирование отчетности, списка замечаний • Возможность прикрепления свидетельств выполнения аудитов	• Уведомление ответственных за задачи по email • Выполнение действий с помощью конструктора MS Flow / Power Automate с возможностью частичной автоматизации выполняемых действий.		комплексами требований. Задание периодичности контрольных проверок, назначение ответственных сотрудников, аудиторов. Ручное формирование списка требований для контрольных проверок. Ручное проведение оценки выполнения требований контрольной проверки: назначение ответственных экспертов, объединение их в рабочие группы, проведение оценки экспертным методом с обоснованием, выставление оценки по аудиту на основании проведенных контрольных проверок • Расчет количественного индекса соответствия требованиям на основании оценок экспертов, с учетом весовых коэффициентов	маршрутизацию задач исполнителям, контроль качества и сроков предпринимаемых мер по устранению выявленных в ходе аудита замечаний и т.д. • Запуск аудита и связанных активностей в рамках единого процесса • Формирование и автоматическое отслеживание расписания аудитов • Возможность формирования собственных методик аудита (по методикам компании) • Проведение GAP-анализа (сравнение текущего и целевого состояния • Предусмотрен чат по объектам, в рамках которого пользователи системы могут общаться по связанным с аудитом и соответствием требованиям задачам

				требований. Возможность добавлять пользовательские методики оценки с помощью конструктора типов аудита с использованием формул, таблиц, списков • Визуализация проведенных контрольных проверок: вывод таблиц со списком оценок по аудитам, графических диаграмм (дашбордов) Поддержка привлечения разных экспертов на разных этапах управления аудитами и соответствием требованиям. Поддержка просмотра результатов аудитов и планов работ по устранению замечаний непосредственно из свойств актива. Поддержка выполнения простых (один актив – один опросный лист) и сводных (несколько опросных листов по нескольким активам,	• Поддерживается журналирование всех выполненных действий в рамках рабочего процесса управления аудитами и соответствием требованиям Модули автоматизации: • аудиторских отчетов • учета внешних потоков ПДн организации, ДЗО и компаний экосистемы • процесса проведения контроля обработки и защиты данных в компаниях экосистемы и партнеров организации • процедуры учета и мониторинга результатов контроля обработки и защиты данных в компаниях экосистемы и партнеров организации • процесса проведения экспертизы в отношении пилотов процессов, учет

				проверка по различным стандартам) аудитов. Поддержка комплексных проверок: агрегирование нескольких аудитов в одну итоговую оценку соответствия. Автоматический динамический пересчет показателей аудита при изменении методики проверки, автоматическое выполнение проверок по расписанию, автоматическая рассылка уведомлений пользователям. Импорт/экспорт результатов оценки в формат Excel. Импорт требований для аудита из формата Excel. Предустановленные стандарты для оценки соответствия: 152-ФЗ, НПА ФСТЭК России (Приказы №№17, 21, 31, 239), PCI DSS (3.1, 3.2), SWIFT's Customer Security Programme, ISO 27001, ГОСТ Р ИСО/МЭК 27001-2006, 382-П, СТО БР ИББС-1.0-2014, ГОСТ Р 57580.2-2018	материалов и результатов экспертизы • формирования чек-листов • формирования отчетности в части внешнего контроля и экспертизы Сквозное соответствие проверок в разных стандартах и нормативах компании, без необходимости повторять проверки под каждый стандарт. Наличие метрик и анализа проведенных аудитов. Возможность импорта в систему результатов ранее сделанных аудитов с целью работы с ними. Ролевая модель формирования и согласования отчета об аудите. Ведение плана устранения замечаний аудитов, с автоматическим

					отслеживанием и оповещением. Возможность удаленного анкетирования с отделенной функцией верификации, возможностью вложения файловых и иных свидетельств аудита. Визуализация исполнения расписания аудитов: • прогресс по числу выявляемых замечаний • скорость устранения замечаний • своевременная подготовка и выполнения плана устранения замечаний • статистика замечаний Экспорт результатов оценки в форматы xlsx, docx, pdf. Импорт требований для аудита из формата csv, xlsx. Предустановленные стандарты для оценки соответствия: 187-ФЗ, 152-ФЗ, GDPR, НПА ФСТЭК России (Приказы №№17, 21, 31, 235, 239), PCI DSS (3.1,

					3.2), SWIFT's Customer Security Programme, SWIFT CSCF 2020, ISO 27001, ГОСТ Р ИСО/МЭК 27001-2006, 382-П, 672-П, 683-П, 684-П, СТО БР ИББС-1.0-2014, ГОСТ Р 57580.2-2018
Автоматическое соответствие стандартам	Нет	Нет	Нет	Нет	Да, с помощью механизма Auto-Compliance (авторская технология auto-SGRC): автоматическое изменение настроек ОС/ПО/СЗИ для соответствия нормативным требованиям. Автоматизация соответствия требованиям: • ГОСТ Р 57580.1 • 382-П • PCI DSS • 187-ФЗ • GDPR • ISO 2700X • и др. Автоматизируется любой собственный стандарт предприятия.
Поддержка обеспечения безопасности КИИ	Нет данных	Нет	Нет	Возможности системы для поддержки обеспечения безопасности КИИ: • Учет субъектов КИИ • Сбор характеристик субъектов КИИ	Возможности системы для поддержки обеспечения безопасности КИИ: • Агрегация сведений: о субъекте КИИ, о лице, эксплуатирующем ОКИИ, об ОКИИ, о

				• Оценка критичности процессов субъекта КИИ • Сбор данных о составе объекта КИИ (ОКИИ) • Инвентаризация оборудования и ПО в ОКИИ с занесением в карточку ОКИИ • Формирование перечня ОКИИ моделирование угроз для ОКИИ по методике ФСТЭК России • Расчет категории значимости для ОКИИ • Учет мер защиты ОКИИ • Проведение аудита на соответствие Приказу ФСТЭК России №239 для значимых ОКИИ (ЗОКИИ) • Формирование пакета документов для предоставления в ФСТЭК России	взаимодействии ОКИИ и сетей электросвязи, о программных и программно-аппаратных средствах, используемых на ОКИИ • Формирование сведений об угрозах безопасности информации и категориях нарушителей в отношении ОКИИ (с участием экспертов) • Формирование возможных последствий в случае возникновения компьютерных инцидентов (с участием экспертов) • Присвоение категорий значимости ОКИИ (с участием экспертов) • Формирование организационных и технических мер, применяемых для обеспечения безопасности ЗОКИИ (с выгрузкой

					результатов в .pdf и .docx) • Поддержка процесса пересмотра категории значимости • Формирование списка контрольных мероприятий (чек-листа) базового набора мер ЗОКИИ на основе присвоенной категории и адаптация набора базовых мер в соответствии с угрозами и особенностями ЗОКИИ (с выгрузкой в .docx) • Создание и контроль исполнения задач по реализации недостающих мер • Поддержка процедуры вывода из эксплуатации ОКИИ (формирование комплекта документов)

Выводы по разделу №2

В плане управления информационной безопасностью, как и в предыдущем разделе, наиболее привлекательно выглядят американская Microsoft Compliance Center и отечественные R-Vision и Security Vision. Они лидируют по объемам собираемой и инвентаризируемой информации об оборудовании, возможностям интеграции со сторонними решениями, управлению уязвимостями (отметим, что по типам обрабатываемых уязвимостей лидируют Microsoft Compliance Center и Security Vision – они обрабатывают как уязвимости ПО, так и уязвимости конфигураций, в то время как ePlat4m, RSA и R-Vision обрабатывают только уязвимости ПО). В части управления задачами, документами, требованиями наряду с Microsoft Compliance Center, R-Vision и Security Vision некоторые неплохие возможности демонстрирует и ePlat4m. В плане мониторинга состояния информационной безопасности также наиболее привлекательны Microsoft Compliance Center, R-Vision и Security Vision. При этом Security Vision предоставляет наиболее широкие возможности визуализации информации и создания отчетности.

В управлении киберрисками и соответствием законодательным требованиям ePlat4m и RSA демонстрируют довольно скромные функциональные возможности. Система RSA к тому же достаточно закрыта и ориентирована больше на западного потребителя, либо на российскую «дочку» такой компании.

Функциональность решения от Microsoft в этом плане гораздо более развита. Особенно обращает на себя внимание автоматизация с использованием MS Flow / Power Automate, которая позволяет гибко управлять ИТ и ИБ процессами, а также решать большое количество бизнес-задач.

Функционал управления киберрисками R-Vision выделяется тем, что, по нашему мнению, продукт изначально был «заточен» под банки; есть и широкий набор предустановленных банковских отчетов. Данное решение с большой долей вероятности хорошо подойдет для финансовых организаций, в которых осуществляются стандартные банковские бизнес-процессы и которым будет достаточно предустановленных схем работы с рисками, комплаенсом и отчетностью. Из минусов решения R-Vision можно выделить слабые возможности настройки под нужды конкретных организаций. Многие функциональные возможности и даже некритичные параметры «зашиты» в системе и не поддаются настройке и изменению силами конечного потребителя: например, процессы управления активами и уязвимостями достаточно прямолинейны, без поддержки ветвистых процессов, а процессы управления рисками и соответствием законодательству не подойдут крупным компаниям с разветвленной структурой и сложными процессами.

Security Vision отличается гибкостью настройки, что позволяет конечному пользователю системы не только менять параметры имеющихся процессов управления ИБ, но и создавать свои процессы, которые будут максимально соответствовать принятым в организации. Однако, следует учесть, что для качественной настройки этого решения потребуется выделить существенные временные ресурсы, а также желательно иметь в штате специалиста, поддерживающего эту систему (благо, вендор проводит обучение для своих заказчиков и партнеров). Из существенно выделяющихся новаций Security Vision: 1. Модуль анализа инцидентов, содержащий модель машинного обучения и выполненный с возможностью автоматического определения команд реагирования на инцидент и передачи команд реагирования на инцидент на подключенные внешние системы и устройства является воплощением практического использования искусственного интеллекта при решении прикладных задач ИБ. 2. Функционал auto-SGRC (авторская технология), позволяющий в режиме реального времени обеспечивать соответствие требованиям регуляторов и собственных стандартов, автоматически корректировать настройки ОС, ПО и СЗИ, не имеет аналогов на отечественном рынке.

Общие выводы

В обзоре участвовали SGRC-продукты, достаточно разные как по идеологии и архитектуре, так и по функциональным возможностям.

ePlat4m фактически представляет собой «коробочное» решение без возможности гибкой и точной настройки, однако, по ряду параметров представляется перспективным и обладающим актуальными базовыми параметрами.

Решение от Microsoft заслуживает высокой оценки. В плане функционала особо хотелось бы отметить автоматизацию с использованием MS Flow / Power Automate, что позволяет гибко управлять ИТ и ИБ процессами, а также решать большое количество бизнес-задач. Минусом данного решения для отечественных заказчиков может стать тот факт, что Microsoft Compliance Center функционирует в облачной инфраструктуре Azure и оптимизирован под эту экосистему, поэтому отдельно использовать его не получится. Решение RSA Archer, хоть и не является облачным, также сфокусировано на применении в стеке продуктов компании RSA. Главным минусом решений от Microsoft и RSA является потенциальная сложность их закупки и применения во многих отечественных компаниях, связанных строгими законодательными нормами.

Решение R-Vision обладает развитым функционалом и, на наш взгляд, ориентировано на банки, причем с довольно типовыми бизнес-процессами: глубокая кастомизация и настройка разнообразных нюансов работы решения силами пользователя не предусмотрены. Однако, данный продукт создает впечатление крепкого монолита, который, будучи однажды настроенным, сможет удовлетворить требования ряда финансовых организаций.

Решение Security Vision выглядит наиболее гибким из всех рассмотренных продуктов и, по нашему мнению, способно воспроизвести достаточно сложные бизнес-процессы и адаптироваться под потребности заказчика из любой отрасли. Security Vision предлагает наибольшее разнообразие типов и возможностей коннекторов подключения. Однако, безусловно, это предполагает длительную настройку и оптимизацию продукта под индивидуальные особенности каждой конкретной организации. Существенным плюсом выглядит и функционал auto-SGRC, используемый Security Vision для автоматизации соответствия нормативным требованиям, с изменением настроек контролируемой инфраструктуры.

Заметным отличием российских систем - ePlat4m, R-Vision и Security Vision – является их включенность в Единый реестр российских программ для ЭВМ и баз данных. Кроме того, R-Vision и Security Vision обладают сертификатами соответствия ФСТЭК России.