СОГЛАСОВАНО
Начальник управления
информационных технологий
_____Е.С. Кайбилов
«___»_____2021 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на оказание услуг по предоставлению неисключительных прав системы взаимодействия с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и реализации основных функций системы безопасности значимых объектов критической информационной инфраструктуры

№ п/п	Наименование	Кол-во (шт.)
1	PT Platform 187, основная лицензия на 250 узлов, гарантийные обязательства в течение 1 (одного) года	1

1. Условия оказания услуг

Предметом Контракта является продление неисключительных прав на использование программного обеспечения системы взаимодействия с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и реализации основных функций системы безопасности значимых объектов критической информационной инфраструктуры.

2. Цели оказания услуг

Основными целями продления неисключительных прав на использование программного обеспечения Системы является повышение эффективности информационной безопасности в организации и выполнение основных требований законодательства.

Система предназначена для взаимодействия с ГосСОПКА и реализации основных функций системы безопасности значимых объектов КИИ.

Применение Системы позволит:

– проводить непрерывную инвентаризацию информационных ресурсов и поддерживать сведения об инфраструктуре в актуальном состоянии;

– проводить анализ защищенности и выявлять уязвимости;

– автоматизировать процесс управления уязвимостями и осуществлять контроль соответствия требованиям;

– анализировать события безопасности из различных источников и выявлять инциденты;

– проводить многопоточную проверку входящих файлов и предотвращать распространение вредоносного ПО;

– управлять процессами реагирования на инциденты и проводить расследования;
автоматизировано взаимодействовать с НКЦКИ.

3. Перечень нормативно-технических документов, методических материалов, использованных при разработке ТЗ

Нормативно-технические документы, методические материалы, использованные при разработке ТЗ:
– ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения;
– ГОСТ 34.601-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания;
– ГОСТ 34.201-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем;
ГОСТ 34.602-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.

4. Требования к структуре и функционированию Системы

Система должна состоять из следующих инфраструктурных компонентов:
– Система контроля защищенности и соответствия стандартам Заказчика на базе MaxPatrol 8 разработки Positive Technologies;
– Система мониторинга событий информационной безопасности Заказчика на базе MaxPatrol SIEM разработки Positive Technologies;
– Система анализа сетевого трафика, выявления и расследования инцидентов Заказчика на базе PT NAD разработки Positive Technologies;
– Многоуровневая система защиты от вредоносного контента Заказчика на базе PT MultiScanner разработки Positive Technologies;
– Система управления инцидентами и взаимодействия с ГосСОПКА в части обнаружения, предотвращения и ликвидации последствий компьютерных атак Заказчика на базе «ПТ Ведомственный центр» разработки Positive Technologies.

Система должна представлять собой локальное разворачиваемое внутри защищаемого периметра решение. Система должна представлять из себя развернутое на одном физическом сервере решение. На сервер устанавливается комплекс программных средств, который обеспечивает выполнение следующих функций:
– инвентаризация IT-инфраструктуры;
– выявление уязвимостей информационных ресурсов и контроль их устранения;
– оценка соответствия стандартам;
– анализ событий безопасности и выявление инцидентов;
– обнаружение компьютерных атак на сетевом уровне;

– выявление и блокировка вредоносного ПО;
– управление инцидентами;
– взаимодействие с НКЦКИ.

Система должна позволять проводить мониторинг событий ИБ, инвентаризацию информационных ресурсов и выявление уязвимостей в ИТ-инфраструктуре с общим количеством узлов не менее 250.

Система должна позволять обрабатывать не менее 100 Мбит/с сетевого трафика и не менее 3000 файлов в час при проверке наличия вредоносного программного обеспечения.

Система должна позволять:

– выявлять уязвимости информационной инфраструктуры и контролировать их устранение;
– контролировать параметры настройки программных и программно-технических средств информационной инфраструктуры;
– контролировать изменения в конфигурации программных и программно-технических средств информационной инфраструктуры;
– оценивать эффективности выполнения контроля защищенности и действий, связанных с устранением нарушений безопасности;
– оценивать соответствия отраслевым и международным стандартам;
– осуществлять сбор информации об активах;
– управлять записями об активах;
– осуществлять сбор и обработку (агрегации, корреляции) событий ИБ (с сохранением результатов обработки в БД);
– создавать и управлять записями об инцидентах ИБ;
– предоставлять пользователю данные об активах, событиях и инцидентах, создания отчётов;
– выполнять реализацию разграничения доступа;
– выполнять выявление, анализ уязвимостей ИТ-инфраструктуры Заказчика;
– выполнять захват сетевого трафика;
– выполнять анализ сетевого трафика;
– выполнять обнаружение сетевых атак;
– выполнять хранение необработанного сетевого трафика;
– выполнять хранение результатов разбора сетевого трафика;
– организовать процесс расследования компьютерных инцидентов;
– передавать сведения о расследовании компьютерных инцидентов в НКЦКИ в требуемом формате обмена;
– принимать из НКЦКИ методические рекомендации и информационные сообщения;
– проводить учет информации, направленной в НКЦКИ;
– сокращать время реагирования на инцидент за счет средств автоматизации регистрации и обработки инцидентов;
– проводить анализ результатов реагирования на инциденты с помощью средств отчетности и визуализации.
– выполнять комплексную и многопоточную проверку файлов;

– выполнять ведение базы знаний по загруженным объектам и вердиктам;
– выполнять ретроспективный анализ и уведомление пользователей об обнаруженном ВПО в ранее загруженных файлах;
– осуществлять защиту от ВПО на уровне сети;
– выполнять локализацию источников распространения ВПО;
– выполнять контроль действий антивирусов;
– осуществлять анализ результатов, формирование отчетов.
Система должна состоять из следующих подсистем:
– контроля защищенности и соответствия стандартам;
– мониторинга событий информационной безопасности;
– анализа сетевого трафика, выявления и расследования инцидентов;
– защиты от вредоносного контента;
– управления инцидентами и взаимодействия с ГосСОПКА в части обнаружения, предотвращения и ликвидации последствий компьютерных атак; централизованного обновления.

Перечень функций программных средств, входящих в Систему, их назначение и основные характеристики

Перечень функций программных средств, входящих в состав Системы:
– инвентаризация информационных ресурсов:
а) инвентаризация информационных активов;
б) отслеживание изменений в ИТ-инфраструктуре;
в) сбор и обработка сведений о состоянии защищенности инфраструктуры;
г) поддержание сведений об инфраструктуре в актуальном состоянии;
– выявление уязвимостей информационных ресурсов и контроль их устранения:
а) сетевое и системное сканирование уязвимостей;
б) анализ защищенности;
в) тестирование на проникновение;
г) сканирование баз данных;
д) отчеты об устранении уязвимостей;
– оценка соответствия стандартам:
а) автоматическая проверка на соответствие техническим стандартам безопасности;
б) контроль соответствия политикам безопасности различной степени сложности;
– анализ событий безопасности и выявление инцидентов:
а) сбор и обработка событий безопасности из различных источников;
б) выявление актуальных угроз;
в) автоматическое уведомление об инцидентах;
– обнаружение компьютерных атак на сетевом уровне:
а) мониторинг и анализ сетевого трафика;
б) выявление атак, сетевых аномалий, скрытого присутствия, активностей вредоносного ПО, в т.ч. в ретроспективе;

– выявление и блокировка вредоносного ПО:
а) онлайн-проверка почтовых сообщений;
б) контроль пользовательского и корпоративного трафика;
в) ретроспективный анализ и расследование инцидентов заражения вредоносным ПО;
г) агрегация информации об угрозах;
– управление инцидентами:
а) учет и обработка инцидентов;
б) управление процессами реагирования и ликвидации последствий;
в) контроль расследования инцидентов;
– взаимодействие с НКЦКИ:
а) формирование карточки инцидента в установленном регулятором формате;
б) автоматизированное взаимодействие с инфраструктурой НКЦКИ.

Требования к способам и средствам связи для информационного обмена между продуктами, входящими в Систему

Унифицированное информационное взаимодействие между компонентами Системы должно обеспечиваться с использованием шины передачи данных.

Требования к режимам функционирования Системы

Режим функционирования Системы — автоматизированный, под управлением администратора.

Режим эксплуатации Системы определяется регламентом работы ИТ- и ИБ-служб Заказчика.

Система должна обеспечивать возможность работы в штатном режиме (непрерывная круглосуточная работа):

Штатный режим является основным режимом функционирования Системы, при котором поддерживается выполнение всех заявленных функций.

Требования по диагностированию системы

Система должна обеспечивать возможность записи в журналы регистрации событий информации по служебным событиям и сбоям.

Перспективы развития и модернизации системы

Система должна обеспечивать возможность модернизации путем переноса технического и/или программного обеспечения на отдельные серверы.

Требования к безопасности

Средства Системы должны обеспечивать идентификацию и аутентификацию персонала по уникальному идентификатору и паролю.

Должна быть реализована модель ролевого доступа, обеспечивающая возможность разрешения или запрета выполнения персоналом Системы заданных операций.

Требования к функциям Системы

Подсистема должна реализовывать функции сетевого и системного сканирования узлов информационной инфраструктуры.

Сетевое сканирование узлов информационной инфраструктуры должно обеспечивать инвентаризацию объектов информационной инфраструктуры, в том числе:

– серверов;
– рабочих станций и мобильных компьютеров;

сетевого оборудования.

Сетевое сканирование узлов информационной инфраструктуры должно обеспечивать получение следующей информации об объектах информационной инфраструктуры:

– доступность сетевого узла;
– доступные порты;
– доступные сетевые службы;
– версия ОС или тип устройства;
– сетевые параметры узла (имя, IP-адрес);

тип и версии сетевых служб.

Сетевое сканирование узлов информационной инфраструктуры должно обеспечивать выявление и идентификацию узлов информационной инфраструктуры, функционирующих в момент сканирования и доступных по одному из протоколов прикладного уровня, по сетевым адресам или именам с возможностью ограничения области сканирования:

– путем задания перечня сетевых адресов или имен сканируемых узлов;
– путем задания диапазонов сканируемых сетевых адресов;

путем использования комбинации указанных методов.

Сетевое сканирование узлов информационной инфраструктуры должно обеспечивать выявление и идентификацию доступных в момент сканирования портов сетевых протоколов транспортного уровня по протоколам и номерам с возможностью ограничения области сканируемых сетевых протоколов:

– путем задания перечня портов TCP;
– путем задания диапазонов портов TCP;
– путем использования комбинации вышеуказанных методов;

путем задания отдельных протоколов прикладного уровня, использующих в качестве протокола транспортного уровня UDP.

Сетевое сканирование узлов информационной инфраструктуры должно обеспечивать выявление и идентификацию уязвимостей (включая ошибки конфигурации) в реализации идентифицированных сетевых протоколов, при этом в результатах сканирования должна обеспечиваться маркировка уязвимостей, при выявлении которых не гарантируется достоверность идентификации.

Сетевое сканирование узлов информационной инфраструктуры должно обеспечивать выявление уязвимостей в доступных по протоколу HTTP веб-приложениях (как в серийно выпускаемых веб-приложениях, так и в

приложениях собственной разработки Заказчика), обусловленных ошибками, допущенными при разработке и настройке этих приложений.

Сетевое сканирование узлов информационной инфраструктуры должно обеспечивать выявление учетных записей с паролями, содержащимися в справочниках, задаваемых администратором в настройках сканирования (словарными паролями), для протоколов FTP, HTTP, POP3, RDP, SIP, SMB, SMTP, SNMP, SSH, Telnet, VNC, а также для СУБД DB2, Microsoft SQL Server, MySQL, Oracle, Sybase и приложений PcAnywhere, Radmin, SAP DIAG, SAP RFC, VMWare.

При выполнении сетевого сканирования веб-приложений должны применяться эвристические методы контроля, позволяющие обнаруживать уязвимости в соответствии с Web Application Security Consortium Threat Classification и Open Web Application Security Project.

Системное сканирование должно обеспечивать контроль следующих программных и программно-технических средств:

- Microsoft Windows 2000/XP/Vista/7/8/8.1/10;
- Microsoft Windows Server 2003/2008/2008R2/2012/2012 R2/2016;
- Red Hat Enterprise Linux 3/4/5/6/7;
- Cisco PIX/ASA;
- активное сетевое оборудование Cisco;
- активное сетевое оборудование Juniper;
- активное сетевое оборудование Huawei;
- Check Point Gaia;
- Palo Alto PAN-OS;
- Microsoft SQL Server 2005/2008/2008R2/2012/2016;
- Oracle Database Server 8i/9i/10g/11g;
- Microsoft Active Directory;
- Microsoft Exchange Server 2007/2010/2013/2016.

Системное сканирование должно обеспечивать сбор сведений о составе программного и аппаратного обеспечения сканируемого узла (в том числе информации о материнской плате, BIOS, сетевых картах, объеме ОЗУ, жестких дисках).

Системное сканирование должно обеспечивать сбор сведений о наличии уязвимостей программного обеспечения сканируемого узла.

Системное сканирование должно обеспечивать сбор сведений о конфигурации программного обеспечения в объеме, достаточном для выявления уязвимостей, обусловленных ошибками конфигурации.

Для операционных систем Microsoft Windows системное сканирование должно обеспечивать сбор сведений о фактах подключения внешних USB-устройств (в том числе отчуждаемых носителей информации), причем идентификация должна производиться с помощью идентификаторов, присвоенных устройствам при их производстве.

Для веб-приложений подсистема должна контролировать уязвимости в режимах тестирования на проникновение и (или) контроля конфигураций и установки обновлений.

При выполнении сетевого сканирования веб-приложений должны применяться эвристические методы контроля, позволяющие обнаруживать уязвимости в соответствии с Web Application Security Consortium Threat Classification version 2 и Open Web Application Security Project TOP 10.

Подсистема должна обеспечивать выявление уязвимостей, документированных в базе данных Common Vulnerabilities and Exposures (CVE). Для выявленных уязвимостей должна обеспечиваться оценка степени риска на основе правил Common Vulnerability Scoring System (CVSS).

Подсистема должна обеспечивать выявление уязвимостей, документированных в базе данных уязвимостей ФСТЭК России. Для выявленных уязвимостей должна обеспечиваться однозначная идентификация уязвимости в соответствии с:

– встроенной системой классификации и идентификации уязвимостей;

– идентификаторами базы данных уязвимостей ФСТЭК России, в случае наличия идентификатора.

Требования к функциям управления

Компоненты подсистемы должны обеспечивать возможность задания параметров сканирования.

Компоненты подсистемы должны обеспечивать возможность запуска сканирования, в том числе по заданному расписанию и с учетом запрещенных интервалов.

Компоненты подсистемы должны обеспечивать возможность просмотра результатов сканирования.

Компоненты подсистемы должны обеспечивать возможность формирования шаблонов, задающих параметры генерации отчетов, следующих типов:

– отчет об инвентаризации узлов информационной инфраструктуры;

– отчет об изменениях в составе просканированных узлов информационной инфраструктуры;

– отчет о программном обеспечении узлов информационной инфраструктуры:

а) обязательного к установке программного обеспечения;

б) запрещенного к установке программного обеспечения;

в) программного обеспечения, отсутствующего в перечне разрешенного;

– отчет о наличии на узлах информационной инфраструктуры уязвимостей, в том числе обусловленных ошибками конфигурации программного обеспечения;

– отчет о соответствии узлов информационной инфраструктуры требованиям применимых для них технических стандартов;

– отчет о соответствии высокоуровневым стандартам (ISO/IEC 27001/27002, PCI DSS, СТО БР, РД ФСТЭК России, 3GPP, GDPR);

– отчет об изменении состава программного и аппаратного обеспечения узлов информационной инфраструктуры;

– отчет об изменениях в составе присутствующих на узлах информационной инфраструктуры уязвимостей;
– отчет об изменении в результатах оценки соответствия узлов информационной инфраструктуры требованиям технических стандартов;
– отчет о результатах оценки следующих показателей эффективности процессов управления уязвимостями и контроля соответствия стандартам:
а) величина интегральной уязвимости;
б) средняя скорость устранения уязвимостей;
в) среднее по всем узлам процентное соотношение выполненных и невыполненных требований технических стандартов;
г) процентное соотношение узлов информационной инфраструктуры полностью и не полностью соответствующих техническим стандартам;
д) периодичность сканирования узлов информационной инфраструктуры.
Компоненты подсистемы должны обеспечивать возможность генерации отчетов по заданному шаблону, в том числе — автоматически, после завершения сканирования, запущенного по расписанию.
Компоненты подсистемы должны обеспечивать возможность доставки отчетов уполномоченным сотрудникам Заказчика, в том числе — автоматически, после завершения сканирования, запущенного по расписанию.
Компоненты подсистемы должны обеспечивать возможность формирования технических стандартов и переопределения отдельных требований.
Компоненты подсистемы должны обеспечивать возможность формирования перечней запрещенного и разрешенного к установке программного обеспечения.
Компоненты подсистемы должны обеспечивать возможность формирования справочников паролей.
Компоненты подсистемы должны обеспечивать возможность формирования перечней идентификаторов санкционированно подключаемых внешних устройств.
Компоненты подсистемы должны обеспечивать возможность идентификации и аутентификации пользователей Системы по уникальному идентификатору и паролю с возможностью использования системных идентификаторов, идентификаторов ОС и идентификаторов в домене Active Directory.
Компоненты подсистемы должны обеспечивать возможность разграничения доступа пользователей к функциям Системы.
Компоненты подсистемы должны обеспечивать возможность регистрации следующих событий:
– вход пользователя в интерфейс пользователя и выход из интерфейса пользователя;
– запуск и прерывание операций по сканированию компонентов информационной системы.
Компоненты подсистемы должны обеспечивать возможность регистрации событий, включая следующие параметры:
– дата и время события;

– краткое описание события;
идентификатор пользователя либо узла, вызвавшего событие.

Требования к подсистеме мониторинга событий безопасности

Подсистема должна обеспечивать централизованную настройку и мониторинг работы модулей сбора событий из единой консоли управления.
Компоненты Системы должны обеспечивать удаленный (сетевой) и локальный сбор событий.
Компоненты Системы должны обеспечивать как пассивный (без подключения к источнику), так и активный (с подключением к источнику) сбор событий.
Компоненты Системы должны обеспечивать возможность сбора событий в режиме, близком к режиму реального времени.
Управление сбором событий из различных типов источников должно осуществляться из единой консоли.
Система должна обеспечивать возможность фильтрации и поиска задач сбора данных по их атрибутам.
Учетные данные, необходимые для активного подключения к источникам, должны храниться в единой базе.
Должна быть обеспечена возможность использования одной записи с учетными данными для подключения к различным источникам с целью минимизации трудозатрат на корректировку учетных данных.
Система должна обеспечивать коррекцию времени в событиях от источника без дополнительной настройки источника.
Система должна обеспечивать стабильную работу с событиями, полученными от источников с некорректным временем.
Сбор событий должен быть реализован посредством модулей сбора данных на основе сохраняемых профилей.
В Системе должны быть предусмотрены предустановленные профили для сбора данных.
Пользователи Системы должны иметь возможность создавать собственные профили для сбора данных на базе системных (с возможностью редактирования различных параметров профиля, например, портов подключения, названий и полей таблиц, из которых производится сбор, частоты забора данных, количества передаваемых сообщений).
Система должна обеспечивать сбор событий с использованием следующих механизмов и протоколов:
– сенсор в терминах протокола Cisco NetFlow;
– сообщения стандарта syslog по протоколам TCP и UDP;
– SNMP;
– SMB;
– WMI;
– текстовые файлы в форматах 1CEnterprise8, AccordSucuCsvLog, FtpFileLog, Oracle Listener Log, SharePointServer, WindowsFileLog;
– отслеживание изменений в БД следующих схем данных: DeviceLockLog, Dr

Web Database, ForefrontEndpointProtectionLog, InfoWatchTrafficMonitor6.1, InfoWatchTrafficMonitorLog, KasperskySecurityCenter, Kontinent_ServerAccessLog, LinterVS_SAVZ, LinterVS_SOA, LinterVS_UD_NSD, LumensionEndpointSecurity, McAfeeEpoLog, McAfeeEpoLog4.5, OdbcLog MSSQL, OdbcLog Oracle, OracleAuditTrail, SCCMDetectSoftware, SCCMDetectUSBDevices, SCCMEvents, SecretNetLog, SecretNeLog_Oracle, SymantecEPMSecurityEvents, SymantecEPMSystemEvents, SymantecEPMVirusAlert, SystemCenterOperationsManager, Vipnet_StateWatcher, ZecurionZGate;

– OPSEC LEA;
– Windows Event Log;
– результаты выполнения команд на сервере по протоколу SSH;
– события платформы виртуализации VMware vSphere;
– сбор сведений о сетевых соединениях на основе анализа сетевого трафика.

Система должна поддерживать получение данных из источников, указанных в таблице ниже.

Таблица 1 – Перечень поддерживаемых источников событий

№ п/п	Наименование источника	Версия
Системы аутентификации, авторизации, учета		
1.	Cisco ACS	5.x
2.	RSA Authentication Manager	8.2, 8.3
3.	Avanpost IDM	5.3
Системы предотвращения утечек информации		
4.	InfoWatch Traffic Monitor	4.1, 6.1, 6.7
5.	Zecurion zGate (основной журнал)	7
6.	Zecurion zGate (журнал Zgate Proxy)	7
7.	«Конфидент», Dallas Lock	8.0, сборка 347.20, редакции К, С
Системы защиты приложений		
8.	Cisco Email Security Appliance (ESA)	7
9.	Positive Technologies Application Firewall	—
10.	McAfee Web Gateway	7.5
Бизнес-приложения		
11.	Microsoft SharePoint Server	2013
12.	1С:Предприятие	8.2, 8.3
13.	New Security Technologies SafeInspect	2.1
Системы управления базами данных		
14.	Microsoft SQL Server	2005, 2008, 2012, 2014
15.	Oracle Audit Trail	10g, 11g, 12c
16.	Oracle Database	10g, 11g, 12c

№ п/п	Наименование источника	Версия
17.	Oracle MySQL	5.7.10
18.	Oracle Net Listener	10g, 11g, 12c
Системы защиты конечных узлов		
19.	Код безопасности Secret Net	7.6, 7.7
20.	Код безопасности Secret Net Studio	8.2, 8.3, 8.4
21.	Код безопасности vGate	2.7, 2.8, 3.0
22.	ESET Security Management Center	7.0
23.	Kaspersky Administration Kit	8.x
24.	Kaspersky Endpoint Security	10
25.	Kaspersky Security Center	8, 9, 10
26.	Symantec Endpoint Protection	12.1, 14
27.	Lumension Endpoint Security	4.4
28.	SmartLine DeviceLock DLP	7.3, 8.1
Антивирусное программное обеспечение		
29.	Kaspersky Security для Microsoft Exchange Servers	9
30.	Kaspersky Security для Microsoft SharePoint Server	9
31.	Kaspersky Security для Linux Mail Server	8.0
32.	Dr.Web Enterprise Security Suite	6, 10
Системы электронной почты		
33.	Microsoft Exchange Server	2003, 2007, 2010, 2013, 2016
34.	Postfix	2, 3
35.	Sendmail	8.x
Сетевые устройства		
36.	Avaya (Nortel) ERS	5500
37.	QTech QSW	3450-28T, 6500-52F, 8300-52F
38.	Cisco IOS	12.x, 15.x
39.	Cisco NX-OS	4.x, 5.x, 6.x, 7.x
40.	Cisco WLC	7.x
41.	Juniper JunOS	11.x, 12.x, 13.x, 14.x
42.	HPE Comware Software	5.x, 7.x
43.	Huawei	VRP 5.110
Системы защиты сети		
44.	Arbor Networks Peakflow	7.6, 8.x
45.	WatchGuard FireWare XTMv	11.12.2
46.	Positive Technologies MaxPatrol 8	—
47.	Palo Alto Networks PAN-OS	6, 7, 8
48.	KerioControl Technologies	9.0

№ п/п	Наименование источника	Версия
49.	Check Point GAiA OS	76, 77.10, 77.20, 77.30, R80
50.	S-Terra VPN Gate	4.1
51.	«Код безопасности», АПКШ «Континент»	3.7
Межсетевые экраны		
52.	Cisco ASA	8.x, 9.x
53.	FortiNet Fortigate	5.4.x
54.	McAfee (Forcepoint) Next Generation Firewall	5.3
Системы обнаружения и предотвращения вторжений		
55.	Cisco IPS	6.x
56.	Suricata	3.1
57.	Snort	2.9, 3
Операционные системы		
58.	FreeBSD	4.9–9.2
59.	Microsoft Windows	XP (только WMI), Vista, 7, 8, 8.1, 10, Server 2003 и Server 2003 R2 (только WMI), Server 2008, Server 2008 R2, Server 2012, Server 2012 R2
60.	Debian	7, 8, 9
61.	IBM AIX	5.3, 6.1, 7.1
62.	SUSE Linux Enterprise Service	11.x, 12.x
63.	CentOS	6.x, 7.x
Прокси-серверы		
64.	Cisco Web Security Appliance (WSA)	8.0
65.	Squid	3.0–3.5
66.	Entensys UserGate Proxy & Firewall	6
67.	Microsoft Forefront TMG	7.0
Системы виртуализации		
68.	VMware vSphere Hypervisor (ESXi)	5.5, 6.0, 6.5
69.	VMware vCenter	5.5, 6.0, 6.5
Веб-серверы		
70.	Apache HTTP Server	2
71.	Nginx	1.8, 1.9
72.	Microsoft Internet Information Services (IIS)	6.0, 7.5, 8.5
Системы динамической адресации		
73.	Microsoft DHCP Server	2008, 2012
74.	Microsoft DHCP Client	2008, 2012
75.	Microsoft Wndows DNS Server	2008, 2012
Системы управления обновлениями и конфигурацией		
76.	Microsoft Windows Server Update Services	Windows Server 2008,

№ п/п	Наименование источника	Версия
	(WSUS)	2008R2, 2012, 2012 R2
Удостоверяющие центры		
77.	Microsoft Certification Authority (CA)	Windows Server 2008, 2008R2, 2012, 2012 R2
78.	RSA Certificate Manager	6.9
Системы мониторинга сети		
79.	Infotecs ViPNet StateWatcher	3.2
80.	Microsoft System Center Operations Manager (SCOM)	2012R2
Системы организации терминального доступа		
81.	Microsoft Windows Terminal Services	6.3

Система должна позволять подключать источники событий новых типов посредством дополнения множества правил преобразования событий (нормализации, агрегации).
Система должна позволять разрабатывать пользовательские модули сбора для работы с неподдерживаемыми поставщиками программных средств Системы протоколами передачи событий на скриптовом языке Python. Разработка и работа с такими модулями должна осуществляться через интерфейс Системы.
Запуск пользовательских модулей сбора должен осуществляться средствами агента Системы. Запуск модулей сторонними планировщиками не допускается в целях обеспечения информационной безопасности.
Система должна обеспечивать централизованную настройку и мониторинг работы модулей сбора событий из единой консоли управления.
При выполнении иерархической инсталляции Система должна обеспечивать отображение связей между площадками и возможность настройки правил репликации событий в цепочке иерархии.
Система должна обеспечивать возможность мониторинга источников, позволяя отслеживать:
– задержку между временем возникновения событий и временем их получения Системой;
– количество событий, получаемых в единицу времени.

Требования к функциям управления активами
Система должна обеспечивать идентификацию и добавление активов путем:
– сбора и анализа событий;
– сетевого сканирования для обнаружения узлов сети;
– анализа защищенности по методам черного и белого ящика;
– анализа сетевого трафика;
– добавления актива пользователями (вручную).
Система должна обеспечивать идентификацию сетевых служб, использующих протоколы TCP и UDP в качестве протоколов транспортного уровня.

Система должна обеспечивать выявление и идентификацию активов, функционирующих в момент сканирования.
Система должна обеспечивать сбор идентификационных данных об активах (IP-адреса, имени узла, FQDN). Механизм идентификации должен обеспечивать выявление и корректную работу с кластерными конфигурациями активов.
Система должна обеспечивать выявление и идентификацию доступных в момент сканирования портов, использующих сетевые протоколы транспортного уровня.
Система должна обеспечивать сбор сведений о составе программного и аппаратного обеспечения сканируемого актива.
Система должна обеспечивать сбор параметров конфигурации актива по следующим протоколам удаленного управления: WMI, SAP RPC, SSH, Telnet, ODBC, SNMP, Checkpoint OPSEC.
Система должна обеспечивать автоматическую привязку событий к активам при условии, что в событии содержится идентификационная информация.
Система должна обеспечивать построение иерархии групп активов и управление ею.
Система должна обеспечивать автоматическое определение типа и роли узла по результатам сканирования в режимах черного или белого ящика.
Система должна обеспечивать построение и визуализацию топологии сети на актуальный момент времени на уровне L3 модели OSI.
Система должна иметь следующие механизмы для управления списком активов:
– фильтрацию активов по заданному набору атрибутов и их значений с использованием специализированного языка запросов (в том числе с возможностью объединения запросов);
– отображение активов, удовлетворяющих условиям запроса, в таблице активов и на топологии;
– возможность сохранения пользовательских запросов для последующего быстрого доступа к ним;
– функции группировки и сортировки активов, анализа данных об активах.
Система должна обеспечивать отображение активов, участвовавших в событии или инциденте, на топологии сети.
Система должна обеспечивать расчет сетевой достижимости между выбранными активами на топологии с учетом протоколов и портов.
Система должна обеспечивать возможность задания активам уровня значимости и использование этой величины при количественной оценке опасности событий ИБ и инцидентов.
Система должна обеспечивать возможность мониторинга доступности активов (узлов, сетевых сервисов и устройств).
Система должна обеспечивать отслеживание изменений конфигурации активов, включая:
– просмотр состояния актива на заданный момент времени в прошлом;
– сравнение конфигураций актива в разные моменты времени;

– экспорт истории конфигурации актива.

Система должна обеспечивать возможность просмотра информации об уязвимостях актива с указанием оценки CVSS и идентификатора CVE.

Система должна позволять объединять активы в динамические группы исходя из собранных данных об их конфигурации. Формирование динамических групп должно осуществляться как на основе пользовательских запросов, так и при помощи интерактивного конструктора запросов.

Система должна позволять добавлять в модель актива пользовательские поля и их описание.

Система должна позволять выполнять экспорт данных об активах в табличный список.

Требования к функциям обработки событий

Система должна обеспечивать нормализацию событий с использованием встроенных формул.

Система должна поддерживать возможность создания пользователями собственных формул нормализации.

Система должна обеспечивать агрегацию событий с использованием встроенных правил.

Система должна обеспечивать поддержку мультиязычных событий.

Система должна обеспечивать возможность корреляции событий в режиме, близком к режиму реального времени.

Система должна обеспечивать возможность проверки ранее полученных событий на наличие в них актуальных индикаторов компрометации.

В состав Системы должны входить встроенные правила корреляции, обеспечивающие выявление целенаправленных атак в автоматическом режиме.

В состав Системы должны входить встроенные правила корреляции, обеспечивающие в автоматическом режиме контроль действий пользователей и администраторов, выявление аномалий:

– выявление активности на рабочих станциях в ночное время и выходные (праздничные) дни;

– контроль VPN-соединений;

– контроль выполнения команд, которые могут угрожать информационной безопасности КИС, на серверах и сетевом оборудовании;

– контроль учетных записей;

– контроль изменения конфигурации на сетевом оборудовании и серверах;

– контроль установки и запуска новых сервисов ОС и сетевых служб.

Система должна предоставлять пользователю интерфейс создания пользовательских правил корреляции (визуальный конструктор привил корреляции) и возможность создания пользовательских правил корреляции на основе встроенных системных правил.

Система должна обеспечивать возможность управления списком активных правил корреляции с отображением статистики их срабатывания.

Система должна обеспечивать функцию многоуровневой корреляции, когда результаты срабатывания правил корреляции подаются на вход другому правилу корреляции.
Система должна обеспечивать контроль потребляемой коррелятором памяти и при достижении порогового значения отключать нагружающие ее правила корреляции.
Система должна обеспечивать использование табличных списков при формировании правил корреляции. Пользователю должна быть доступна возможность их создания, удаления и редактирования через графический интерфейс.
Функциональность табличных списков должна позволять выполнять:
– контроль времени жизни записей в таблице (TTL);
– индексацию выделенных колонок в целях ускорения доступа к записям;
– определение первичного ключа таблицы;
– импорт и экспорт всего содержимого табличного списка.
При обращении к табличным спискам из правил корреляции должны быть доступны функции:
– создания, обновления, удаления строк, а также очистки всей таблицы;
– обогащения корреляционного события найденными данными из табличного списка;
– выполнения математических функций инкремента, декремента, вычисления максимального, минимального и среднего при вставке данных в табличный список;
– выполнения математических функций вычисления максимального, минимального, среднего и подсчета общего числа строк при выборке данных из табличного списка.
Система должна обеспечивать возможность задания правил обогащения событий, поступающих в систему, данными из табличных списков (в том числе данными из репутационных списков).
Система должна обеспечивать хранение исходных и нормализованных событий.

Требования к функциям управления событиями
Система должна содержать текстовое описание каждого события, предоставленное экспертами вендора.
Система должна обеспечивать категоризацию событий.
Система должна иметь следующие механизмы для управления списком событий:
– фильтрацию событий по группе активов и периоду;
– фильтрацию событий по заданному набору атрибутов и их значений с использованием специализированного языка запросов;
– сохранение пользовательских фильтров для последующего быстрого доступа к интересующим событиям (с возможностью создания иерархического списка фильтров);

– функции группировки и сортировки событий в выводе на экран по всем доступным полям;
анализ данных о событиях с помощью математических операций.

Требования к функциям управления инцидентами

Система должна обеспечивать автоматическое и ручное формирование инцидентов при обнаружении критичных с точки зрения пользователя событий.
Система должна обеспечивать импорт инцидентов из специально подготовленных файлов.
Система должна обеспечивать категорирование инцидентов.
Система должна обеспечивать управление автоматической генерацией инцидентов.
Система должна обеспечивать формирование инцидента с автоматической и ручной привязкой к нему событий.
Система должна обеспечивать просмотр и редактирование карточки инцидента.
Для управления списком инцидентов Система должна иметь следующие механизмы:
– фильтрации инцидентов по группе активов и периоду;
– фильтрации инцидентов по заданному набору атрибутов и их значений с использованием специализированного языка запросов;
– фильтрации инцидентов с использованием системных и пользовательских фильтров;
– сохранения пользовательских фильтров для последующего быстрого доступа (с возможность создания иерархического списка фильтров);
– сортировки инцидентов по времени создания, статусу, критичности, категории, названию.
Система должна обеспечивать возможность построения процесса расследования инцидента: формирования поручений для расследования, определения порядка реагирования и устранения последствий инцидентов, назначения ответственных лиц.
Система должна обеспечивать хранение истории расследования инцидента.
Система должна обеспечивать наличие журнала изменений инцидента для регистрации изменений атрибутов и состояний инцидента.

Требования к функциям отправки уведомлений

Система должна обеспечивать возможность формирования и отправки уведомлений (по электронной почте):
– об изменении списка активов в Системе;
– изменении состава выбранных динамических групп активов (включении, исключении активов);
– событиях и инцидентах — при их попадании под системный или пользовательский фильтр;
– выходе параметров потока событий за пределы допустимых значений;
– выполнении задач сбора данных;

– состоянии Системы.

Система должна обеспечивать возможность отправки уведомления об изменении числа активов и изменениях в группах активов с помощью механизма webhook.

Система должна обеспечить индикацию собственного состояния и уведомления в интерфейсе пользователя о сбоях в работе, критичных для штатного функционирования сервисов.

Требования к функциям визуализации и построения отчетов

Система должна предоставлять оперативные данные об активах, событиях, инцидентах и мониторинге функционирования Системы в виде графиков, диаграмм и таблиц на виджетах и дашбордах.

Система должна обеспечивать возможность создания и конфигурирования пользовательских дашбордов.

Система должна предоставлять возможность экспорта отчетов как минимум в одном из следующих форматов: PDF, XLSX, CSV.

Система должна обеспечивать отображение следующих статистических данных по инцидентам в графическом формате (на виджетах):

– созданные инциденты,
– закрытые инциденты за период,
– незакрытые инциденты по уровню опасности,
– среднее время устранения инцидента.

Система должна обеспечивать выпуск отчетов (стандартных и пользовательских) вручную или по расписанию.

Система должна предоставлять пользователю интерфейс создания пользовательских отчетов с данными об активах, событиях и инцидентах (конструктор отчетов).

Система должна обеспечивать возможность формирования отчетов из состава имеющихся шаблонов:

– по активам,
– событиям,
– инцидентам,
– мониторингу.

Система должна обеспечивать построение следующих отчетов по активам:

– инвентаризация групп пользователей Windows,
– инвентаризация аппаратного обеспечения,
– инвентаризация операционных систем,
– инвентаризация узлов с открытыми портами,
– инвентаризация сетевых сервисов,
– инвентаризация ресурсов общего доступа,
– инвентаризация ресурсов общего доступа по узлам,
– инвентаризация программного обеспечения,
– инвентаризация пользователей Windows,
– инвентаризация служб Windows.

Система должна обеспечивать построение следующих отчетов по инцидентам:
- распределение новых инцидентов по времени,
- распределение утвержденных инцидентов по времени,
- распределение инцидентов в работе по времени,
- все открытые инциденты по времени,
- распределение разрешенных инцидентов по времени,
- распределение закрытых инцидентов по времени,
- все завершенные инциденты по времени.

Система должна позволять автоматически обновлять список активов, событий и инцидентов в выводе на экран через определенные промежутки времени.
Графический интерфейс пользователя должен быть реализован по технологии Web.

Требования к функциям обновлений
Система должна обеспечивать возможность обновления и расширения встроенных баз знаний вендора, в том числе формул нормализации и правил корреляции, в рамках действующей лицензии.
Система должна обеспечивать возможность обновления компонентов Системы без потери накопленных данных.

Требования к функциям разграничения доступа пользователей подсистемы
Система должна обеспечивать идентификацию и аутентификацию пользователей по уникальному идентификатору и паролю.
Система должна обеспечивать идентификацию и аутентификацию пользователей через сторонний LDAP-сервер.
В Системе должна быть реализована модель ролевого доступа, обеспечивающая возможность разрешения или запрета доступа пользователей к информации об определенных узлах (активах).
Система должна обеспечивать регистрацию действий пользователей при работе с компонентами Системы.

Требования подсистеме анализа сетевого трафика, выявления и расследования инцидентов
Подсистема должна обеспечивать захват с выбираемого пользователем сетевого интерфейса, подключенного к каналу связи с пропускной способностью не более 100 Мбит/с, всего сетевого трафика.
Подсистема должна обеспечивать запись захваченного сетевого трафика в файлы формата PCAP.
Подсистема должна обеспечивать импорт сетевого трафика из файлов формата PCAP.
Подсистема должна обеспечивать использование сетевых фильтров для захвата и записи сетевого трафика. Сетевые фильтры должны ограничивать захват сетевого трафика по следующим параметрам:

- протокол транспортного уровня;
- сетевой порт или группа портов;
- IP-подсеть или группа IP-подсетей;
- IP-адрес или группа IP-адресов.

Подсистема должна обеспечивать запись и хранение сырого сетевого трафика с последующей автоматической перезаписью файлов сетевого трафика, превышающих указанный лимит от объема хранилища. Максимальный объем хранящегося сырого сетевого трафика необходимо рассчитывать исходя из 90% загрузки канала связи с пропускной способностью не более 100 Мбит/с.

Подсистема должна обеспечивать хранение обработанного сырого сетевого трафика в процентном соотношении от объема хранилища.

Подсистема должна обеспечивать хранение индексов не менее 2 суток.

Подсистема должна обеспечивать анализ сетевого трафика с возможностью разбора сетевого и транспортного уровней:

- TCP;
- UDP;

Подсистема должна обеспечивать определение и разбор следующих протоколов прикладного уровня:

- ICMP;
- HTTP;
- DNS;
- SSL/TLS (при наличии ключа);
- SSH;
- SMTP;
- POP3;
- IMAP4;
- Telnet;
- FTP;
- TFTP;
- NTP;
- SIP;
- SNMP;
- VLAN;
- DCE/RPC;
- NFS;
- SMB;
- PGSQL;
- MySQL;
- RDP;
- VNC.

Подсистема должна обеспечивать возможность работы с туннелированными протоколами:

- IP-IP;
- IPv6-IPv4;

– GRE.

Подсистема должна обеспечивать определение географической принадлежности IP-адресов, участвующих в сетевом взаимодействии.

Подсистема должна обеспечивать извлечение файлов и данных, передаваемых по протоколам прикладного уровня (HTTP, SMTP, FTP, SMB, TFTP, POP3, IMAP4, NFS).

Подсистема должна отправлять извлеченные из сетевого трафика файлы на дальнейший анализ данных для выявления ВПО в подсистему защиты от вредоносного контента.

Подсистема должна обеспечивать определение имен, типов передаваемых файлов и их контрольных сумм.

Подсистема должна обеспечивать сравнение контрольных сумм передаваемых файлов с черным списком.

Подсистема должна обеспечивать определение доменных имен узлов на основании захваченного сетевого трафика.

Подсистема должна обеспечивать возможность реконструирования сессии.

Подсистема должна обеспечивать сбор информации о баннерах сетевых приложений, участниках сетевого взаимодействия (ОС и др.).

Подсистема должна обеспечивать проверку всех обнаруженных доменных имен, IP-адресов и URL-ссылок по белым и черным спискам.

Подсистема должна обеспечивать расшифровывание пассивным методом (при наличии ключа), данных, передаваемых с помощью протоколов, обеспечивающих шифрование (например, протоколы SSL, TLS) с их дальнейшей индексацией на прикладном уровне.

Подсистема должна обеспечивать поиск и сохранение данных, позволяющих идентифицировать приложения, участвующих в сетевом взаимодействии («баннеры» и т.д.).

Подсистема должна обеспечивать постоянную индексацию, в режиме реального времени, всего захватываемого сетевого трафика с сохранением в БД следующей полученной информации:

– время (начало, конец сессии);
– IP-адреса узлов;
– протокол транспортного уровня;
– номера портов;
– протокол прикладного уровня;
– объем переданных данных;
– доменные имена узлов;
– разобранные поля протоколов прикладного уровня.

Подсистема должна обеспечивать постоянную индексацию в режиме реального времени следующих служебных полей:

– сетевые IP-адреса;
– используемые номера сетевых портов;
– FQDN-имена;
– тип протокола транспортного уровня.

Подсистема должна обеспечивать поиск сетевого соединения по сохраненным данным со следующими параметрами для атак:
- по статусу атаки;
- по опасности атаки;
- по классу атаки;
- по направлению атаки.

Подсистема должна обеспечивать поиск сетевого соединения по сохраненным данным со следующими параметрами для уязвимостей:
- по CVE;
- по вероятности эксплуатации уязвимости.

Подсистема должна обеспечивать поиск сетевого соединения по сохраненным данным со следующими параметрами для файлов:
- по имени;
- по хеш-сумме (MD5);
- по MIME-типу;
- по magic-типу;
- по отправителю или получателю;
- по статусу;
- по офсету.

Подсистема должна обеспечивать поиск сетевого соединения по сохраненным данным со следующими параметрами для узла:
- по DNS-имени;
- по ASN;
- по IPv4-адресу;
- по IPv6-адресу;
- по MAC-адресу;
- по используемому порту;
- по местоположению (организация, город, регион, страна);
- по ОС;
- по вхождению в репутационный список, а также по цвету и типу репутационного списка.

Подсистема должна обеспечивать поиск сетевого соединения по сохраненным данным со следующими параметрами для сессии:
- по статусу;
- по причине завершения соединения;
- по количеству переданных пакетов;
- по TCP-флагу;
- по TCP-флагу TC;
- по TCP-флагу TS;
- по TCP-статусу.

Подсистема должна обеспечивать поиск сетевого соединения по протоколам прикладного и транспортного уровней.

Подсистема должна обеспечивать поиск сетевого соединения по VLAN.

Подсистема должна обеспечивать построение сетевых связей узлов (в том числе по заданным фильтрам).

Подсистема должна обеспечивать построение графиков по соединениям, удовлетворяющим заданным пользователем условиям:

- распределение протоколов прикладного уровня;
- топ доменных имен;
- топ источников и получателей по количеству соединений;
- топ HTTP User-Agent;
- топ HTTP Server;
- карта мира с распределением источников;
- обнаруженные атаки.

Подсистема должна обеспечивать возможность создания компьютерных инцидентов на основе сетевых сессий и обнаруженных компьютерных атак для отправки их в подсистему мониторинга событий безопасности.

Подсистема должна обеспечивать просмотр сохраненной в системе информации о сессиях.

Подсистема должна обеспечивать полнотекстовый поиск, wildcard-поиск.

Подсистема должна обеспечивать возможность составлять запросы в wireshark-подобном формате.

Подсистема должна обеспечивать выгрузку выбранной пользователем сессии в формате PCAP.

Подсистема должна обеспечивать доступ пользователей к системе по веб-интерфейсу.

Подсистема должна обеспечивать предоставление отчетов в следующих форматах:

- DOC;
- PDF.

Подсистема должна обеспечивать предоставление данных о сессиях в следующих форматах:

- CSV;
- JSON.

Подсистема должна обеспечивать поддержку сигнатур сетевых атак в формате систем Snort и Suricata.

Подсистема должна обеспечивать возможность создания собственных сигнатур.

Подсистема должна обеспечивать регистрацию фактов срабатывания сигнатур.

Подсистема должна обеспечивать оповещение средств защиты информации Заказчика о фактах срабатывания сигнатур по протоколу Syslog.

Подсистема должна обеспечивать блокировку сетевых соединений при срабатывании сигнатур.

Требования к подсистеме защиты от вредоносного контента

Подсистема должна осуществлять комплексную и многопоточную проверку файлов с использованием множественных антивирусных ядер на наличие ВПО.

Подсистема должна обеспечивать безопасность данных при передаче и обработке. При работе с веб-интерфейсом все передаваемые данные должны защищаться при помощи HTTPs с использованием SSL-сертификата.
Подсистема должна помещать любые файлы, скачиваемые пользователем из хранилища просканированных файлов, в ZIP-архивы с паролем *infected*.
Подсистема должна выполнять ведение базы знаний по загруженным объектам и вердиктам.
Подсистема должна выполнять проверку файлов, извлеченных подсистемой анализа сетевого трафика, выявления и расследования инцидентов из сетевого трафика при передаче данных по протоколам прикладного уровня HTTP, SMTP, FTP, SMB, TFTP, POP3, IMAP4, NFS, для выявления ВПО.
Подсистема должна поддерживать следующие варианты загрузки объектов для анализа:
– анализ файлов, загружаемых вручную пользователями в Систему, в том числе и анонимно;
– анализ файлов, отправляемых пользователями на выделенный почтовый адрес Системы;
– выявление и анализ передаваемых файлов в зеркалированном с сетевого оборудования на Систему потоке протоколов SMTP, HTTP, POP3, IMAP, FTP, SMB;
– выявление и анализ файлов, прикрепленных к электронным письмам, посредством направления копий писем на Систему;
– выявление и анализ файлов, передаваемых в Web-трафике посредством интеграции с системами защиты через протокол ICAP;
– мониторинг и анализ файлов в сетевых папках общего доступа (анализ файлов в заданной входной папке и перекладывание файлов в зависимости от вердикта в выходную папку или в карантин).
Подсистема должна поддерживать следующие методы сжатия:
– application/gzip (Gzip);
– application/x-compress (Z);
– application/x-bzip2 (Bzip2);
– application/x-xz (XZ).
Подсистема должна поддерживать следующие форматы сообщений электронной почты:
– application/CDFV2-corrupt (Outlook MSG);
– message/partial, message/rfc822, multipart/mixed, multipart/alternative, multipart/related (Eml Message).
Подсистема должна уметь извлекать файлы из архивов следующих форматов:
– application/x-rar (RAR);
– application/x-7z-compressed (7z);
– application/zip (ZIP);
– application/x-tar (Tar).
Подсистема должна распаковывать вложенные архивы до второго уровня.

Требования к функциям сканирования

Подсистема должна осуществлять сканирование файла на наборе следующих антивирусных решений:

– Bitdefender GravityZone;
– Clam AntiVirus;
– ESET Gateway Security;
– Avira.

Подсистема должна обеспечивать анализ архивов, защищенных паролем.

По завершению статического анализа, подсистема должна возвращать следующую информацию:

– итоговый вердикт (высокая опасность, подозрительный, чистый);
– название вредоносного ПО для каждого из антивирусных решений;
– вердикт каждого из антивирусных решений (опасный, потенциально опасный, угроз не обнаружено), с применением которого проводилось сканирование;
– версия антивирусных решений, с применением которых проводилось сканирование;
дата обновления антивирусных баз.

Требования к функциям хранения

Подсистема должна обеспечивать хранение следующих данных:

– метаданных проверяемых файлов;
– значения хэш-функций проверяемых файлов;
– даты и времени сканирования;
– информацию об антивирусах, которые производили проверку (имя, версия ядра, версия антивирусной базы, результат сканирования).

Подсистема должна позволять пользователям выполнять следующие действия с отсканированными файлами:

– скачивать;
– просматривать историю сканирований и статистику ретроспективного анализа;
– добавлять комментарии и метки.

Подсистема должна позволять пользователям выполнять поиск файла в хранилище отсканированных файлов.

Подсистема должна обеспечивать возможность ограничения объема и ротирования хранилища.

Требования к функциям ретроспективного анализа

Подсистема должна выполнять повторную проверку файлов, прошедших через систему, в случае обновления сигнатурных баз антивирусных решений.

Подсистема должна выполнять повторную проверку файлов, прошедших через систему, в случае обновления репутационных списков.

Требования к функциям управления угрозами

Подсистема должна обеспечивать агрегацию угроз — группировку по файлу.

Подсистема должна осуществлять управление жизненным циклом угроз: создание, закрытие и повторное открытие как единичных угроз, так и групп.

Подсистема должна иметь механизм фильтрации по следующему набору из отображаемых атрибутов угроз:

- время обнаружения угрозы;
- тип (изменения результатов, пропущенные, заблокированные);
- состояние обработки (необработанные, обработанные);
- источник;
- тип вредоносного ПО (по классификации);
- название вредоносного ПО (вердикт);
- механизм поиска угроз по имени файла или значению хеш-функции.

Требования к функциям мониторинга

Подсистема должна отслеживать состояние всех подсистем, входящих в состав подсистемы защиты от вредоносного контента. В случае каких-либо отклонений, должен осуществляться перезапуск проблемного сервиса.

Подсистема должна информировать пользователей о текущем статусе работоспособности подсистемы защиты от вредоносного контента через веб-интерфейс.

Требования к функциям управления

Подсистема должна обеспечивать аутентификацию обслуживающего персонала на основании имени учетной записи и пароля.

Подсистема должна обеспечивать функцию разграничения доступа обслуживающего персонала к настройкам системы.

Подсистема должна обеспечивать отправку результатов анализа по протоколу Syslog на выделенный сервер.

Подсистема должна обеспечивать возможность задания словарей паролей, для анализа архивов, защищенных паролем.

Подсистема должна обеспечивать возможность автоматического обновления баз антивирусных решений.

Подсистема должна обеспечивать возможность добавления, изменения, отключения, удаления источников для сканирования.

Требования к подсистеме управления инцидентами и взаимодействия с ГосСОПКА в части обнаружения, предотвращения и ликвидации последствий компьютерных атак

Подсистема должна позволять отправлять инциденты в НКЦКИ.

Подсистема должна осуществлять организацию обмена информацией об инцидентах с НКЦКИ в автоматизированном режиме (посредством API).

Подсистема должна осуществлять учет информации, направленной в НКЦКИ.

Подсистема должна позволять запрашивать содействие в расследовании инцидентов у НКЦКИ.

Требования к функциям управления пользователями

Подсистема должна позволять создавать группы пользователей с указанием следующих атрибутов:

– название;
– сокращенное название;
– бренд;
– адрес электронной почты;
– юридические реквизиты:

а) форма юр. лица;
б) ИНН;
в) КПП;
г) ОГРН.

Подсистема должна позволять создавать и редактировать роли доступа и права доступа.

Подсистема должна позволять редактировать права доступа пользователей.

Требования к функциям управления субъектами

Подсистема должна позволять выполнять следующие действия с субъектами:

– создавать субъект;
– деактивировать субъект;
– просматривать информацию о субъекте;
– изменять параметры субъекта.

Подсистема должна хранить и поддерживать в актуальном состоянии следующую информацию о субъекте:

– наименование субъекта;
– отрасль и тип субъекта, реквизиты (ИНН, КПП, ОГРН, ОКТМО), адреса;
– данные о добавленных документах и перечень ответственных лиц с указанием их контактных данных;
– данные о связанных с субъектом эксплуатируемых объектах;
– данные об уязвимостях информационных ресурсов;
– данные об атакуемых информационных ресурсах и источниках атак.

Требования к функциям управления объектами

Подсистема должна позволять выполнять следующие действия с объектами:

– создавать объект;
– деактивировать объект;
– просматривать информацию об объекте;
– изменять параметры объекта.

Подсистема должна хранить и поддерживать в актуальном состоянии следующую информацию об объекте:

– наименование объекта;

– данные о субъекте-эксплуатанте;
– категория объекта;
– тип объекта;
– обрабатываемая информация;
– юридический, почтовый и физический адрес объекта;
– данные о соглашениях на предоставление услуг:
а) поставщик услуг;
б) основание;
в) срок действия;
г) дата подключения;
д) услуги в рамках соглашения:
1) обнаружение компьютерных атак;
2) предупреждение компьютерных атак;
3) расследование компьютерных инцидентов;
4) реагирование на компьютерные инциденты.

Требования к функциям управления ИТС

Подсистема должна позволять выполнять следующие действия:
– создавать ИТС;
– деактивировать ИТС;
– просматривать информацию об ИТС;
– изменять параметры ИТС.

Подсистема должна хранить и поддерживать в актуальном состоянии следующую информацию об ИТС:
– название системы;
– субъект;
– объект;
– IP-адрес ресурса;
– адрес домена;
– классификация информационной системы:
а) значимость системы;
б) тип системы;
– тип обрабатываемой информации.

Требования к функциям управления инцидентами

Подсистема должна позволять выполнять следующие действия:
– создание карточки инцидента;
– просмотр карточки инцидента;
– изменение параметров инцидента;
– изменение статуса инцидента;
– выпуск отчетов по новым инцидентам по времени.
– переход из карточки инцидента в подсистему мониторинга событий безопасности по технологии «Drill Down».

Подсистема должна позволять поддерживать в актуальном состоянии информацию об инцидентах, используя следующие методы:
– ручное заведение инцидента;
– автоматизированное формирование карточки инцидента из подсистемы мониторинга событий безопасности.
Подсистема должна предоставлять информацию по инцидентам, основываясь на следующих параметрах:
– связанные с инцидентами субъекты, объекты и ИТС;
– дата фиксации инцидента;
– дата регистрации инцидента;
– тип инцидента;
– ответственные лица;
– идентификаторы;
– источники инцидента (создан вручную или добавлен из подсистемы мониторинга событий безопасности).
Подсистема должна хранить и поддерживать в актуальном состоянии следующую информацию об инциденте:
– название;
– описание;
– дата и время обнаружения инцидента;
– категория и тип инцидента;
– источник;
– приоритет инцидента (низкий, средний, высокий или критический);
– пользователь системы, который назначен ответственным за расследование инцидента, а также технический специалист.
Подсистема должна позволять создавать шаблоны рекомендаций для различного типа инцидентов.
Подсистема должна позволять предоставлять рекомендации по инцидентам из числа имеющихся шаблонов.
Компоненты подсистемы должны позволять указывать взаимосвязь между инцидентами.
Компоненты подсистемы должны позволять создавать задачу, связанную с расследованием инцидента.
Подсистема должна позволять добавлять относящиеся к инциденту вложения и передавать их в НКЦКИ.

Требования к функциям управления задачами
Подсистема должна предоставлять возможность создавать задачи для организации работ по расследованию инцидентов.
Компоненты подсистемы должны позволять указывать следующие атрибуты задачи:
– название;
– описание;
– срок выполнения;

– приоритет;
– тип (расследование, сбор доказательств, восстановление);
– ответственный за исполнение.

Подсистема должна позволять добавлять вложения к задачам.

Компоненты подсистемы должны позволять указывать взаимосвязь созданной задачи с инцидентами.

Требования к функциям управления статистикой

Подсистема должна обеспечивать просмотр следующей статистической информации о компьютерных атаках на информационные ресурсы:
– количество заведенных в подсистеме субъектов;
– количество заведенных в подсистеме объектов;
– количество заведенных в подсистеме ИТС;
– количество инцидентов в подсистеме;
– количество закрытых инцидентов;
– количество открытых инцидентов;
– диаграмма распределения созданных инцидентов за выбранный период времени;
– диаграмма распределения инцидентов по статусу за выбранный период времени;
– первые десять субъектов с наибольшим количество инцидентов.

Подсистема должна представлять статистические данные следующим образом:
– в виде количественного показателя;
– таблицы;
– диаграммы с распределением данных во времени.

Подсистема должна позволять выполнять фильтрацию инцидентов по расположению в группах.

Требования к функциям управления активами

Подсистема должна позволять выполнять следующие действия с активами:
– просматривать информацию об активе;
– изменять данные паспорта актива;
– изменять ОС и ПО актива;
– выпускать отчеты по активам.

Подсистема должна позволять поддерживать в актуальном состоянии сведения об активах, используя следующие методы:
– ручной ввод данных;
– импорт данных из подсистемы мониторинга событий безопасности в автоматическом режиме.

Подсистема должна позволять выполнять поиск активов по определенным параметрам с использованием фильтров.

Подсистема должна хранить и поддерживать в актуальном состоянии следующую информацию об активе:
– информация о системе;

- сетевая конфигурация;
- самые опасные уязвимости;
- уязвимости ОС и ПО;
- контекстные метрики CVSS и значимость актива;
- интегральная уязвимость ОС;
- интегральная уязвимость ПО.

Требования к подсистеме централизованного обновления

Подсистема должна реализовывать централизованное обновление компонентов подсистем. В качестве источника обновлений должен использоваться доступный из сети Интернет сервер производителя программного обеспечения Системы.

Подсистема должна реализовывать возможность автоматического обновления компонентов Системы с автоматической выгрузкой обновлений с сервера организации-разработчика системы.

Подсистема должна реализовывать возможность доставки обновлений с помощью отчуждаемых носителей информации.

Подсистема должна обеспечивать хранение полученных обновлений.

Подсистема должна реализовывать оповещение компонентов Системы о доступности новых обновлений.

Подсистема должна предусматривать в своем составе локальный сервер обновлений, обеспечивающий автоматическое централизованное обновление всех компонентов Системы, в том числе сканирующих модулей, размещенных в изолированных структурных подразделениях.

Подсистема должна обеспечивать возможность обновления и расширения встроенных баз знаний вендора, в том числе формул нормализации и правил корреляции, в рамках действующей лицензии.

Подсистема должна обеспечивать возможность обновления компонентов Системы без потери накопленных данных.

Требования к программному обеспечению

Программное обеспечение, используемое для функционирования подсистемы контроля защищенности и соответствия стандартам, подсистемы мониторинга событий безопасности, подсистемы анализа сетевого трафика, выявления и расследования инцидентов, должно быть сертифицировано в системе сертификации Федеральной службы по техническому и экспортному контролю, а также должно быть зарегистрировано в едином реестре российских программ для электронных вычислительных машин и баз данных.

5. Требования по обеспечению конфиденциальности при оказании услуг

В период оказания услуг и после их окончания Исполнитель не должен разглашать и использовать конфиденциальную информацию, принадлежащую Заказчику, которая может стать ему известной в ходе оказания услуг.

Исполнитель несет ответственность за соблюдение этого требования в соответствии с законодательством Российской Федерации.

Начальник отдела
информационной безопасности **Гудков Д.О.**