# СОДЕРЖАНИЕ


1 Общие сведения ..... 5

1.1 Полное наименование системы и её условное обозначение ..... 5

1.2 Наименование предприятий, участвующих в создании Системы ..... 5

1.3 Плановые сроки начала, и окончания работ по созданию Системы ..... 5

1.4 Сведения об источниках и порядке финансирования работ ..... 5

2 Назначение и цели создания системы ..... 5

2.1 Назначение Системы ..... 5

2.2 Цель создания Системы ..... 6

3 Характеристика объектов автоматизации ..... 6

4 Требования к системе ..... 6

4.1 Общие требования ..... 6

4.1.1 Требования к структуре Системы ..... 6

4.1.2 Требования к способам и средствам обеспечения информационного взаимодействия между компонентами Системы, а также Системы со смежными системами ..... 7

4.1.3 Требования к режимам функционирования Системы ..... 8

4.1.4 Требования к диагностированию ..... 9

4.1.5 Требования к перспективе развития и модернизации Системы ..... 9

4.2 Требования к функциональным подсистемам ..... 9

4.2.1 Требования к подсистеме мониторинга событий информационной безопасности ..... 9

4.2.2 Требования к подсистеме анализа сетевого трафика и выявления атак ..... 18

4.2.3 Требования к подсистеме управления уязвимостями ..... 22

4.2.4 Требования к подсистеме многоуровневой защиты от вредоносного контента ..... 27

4.3 Требования к видам обеспечения ..... 32

4.3.1 Требования к техническому обеспечению ..... 32

4.3.2 Требования к программному обеспечению ..... 32

4.4 Общие технические требования к Системе ..... 34

4.4.1 Требования к показателям назначения ..... 34

4.4.2 Требования к защите информации от несанкционированного доступа ..... 34

4.4.3 Требования к обеспечению регистрации событий безопасности ..... 34

4.4.4 Требования по сохранности информации при авариях ..... 35

4.4.5 Требования к патентной чистоте ..... 35

5 Состав и содержание работ по созданию Системы ..... 36
6 Требования к проведению работ ..... 38
6.1 Общие требования к контролю и приёмке Системы ..... 38
6.2 Предварительные испытания ..... 38
6.3 Опытная эксплуатация ..... 38
6.4 Приёмочные испытания ..... 38
7 Требования к составу и содержанию работ по подготовке объектов автоматизации к вводу Системы в действие ..... 40

Перечень обозначений и сокращений

| | | |
|---|---|---|
| DNS | — | Domain name system |
| FTP | — | File transfer protocol |
| HTTP | — | Hypertext transfer protocol |
| HTTPS | — | HyperText transfer protocol Secure |
| LDAP | — | Lightweight Directory Access Protocol |
| NTP | — | Network Time Protocol |
| POP3 | — | Post Office Protocol Version 3 |
| RDP | — | Remote desktop protocol |
| SMB | — | Server Message Block |
| SMTP | — | Simple mail transport protocol |
| SNMP | — | Simple network management protocol |
| SQL | — | Structured query language |
| SSH | — | Secure Shell |
| SSL | — | Secure Sockets Layer |
| TAP | — | Test Access Point |
| TCP | — | Transmission Control Protocol |
| UDP | — | User Datagram Protocol |
| VNC | — | Virtual Network Computing |
| АРМ | — | Автоматизированное рабочее место |
| БД | — | База данных |
| ИБ | — | Информационная безопасность |
| ИС | — | Информационная система |
| ИТ | — | Информационная технология |
| ОС | — | Операционная система |
| ПАК | — | Программно-аппаратный комплекс |
| ПО | — | Программное обеспечение |
| СКЗК | — | Система комплексной защиты от киберугроз |
| ТЗ | — | Техническое задание |

# 1. Общие сведения

## 1.1. Полное наименование системы и её условное обозначение

Полное наименование системы: *Система комплексной защиты от киберугроз.*

Условное обозначение: *СКЗК*, *Система.*

## 1.2. Наименование предприятий, участвующих в создании Системы

**Заказчик:** ЗАО «АРМБИЗНЕСБАНК» (*далее — Заказчик*).

**Адрес:** Республика Армения, Ереван, улица Налбандяна, дом 48

**Почтовый индекс:** 0010

**Исполнитель:** *определяется по итогам проведения конкурсной процедуры.*

## 1.3. Плановые сроки начала, и окончания работ по созданию Системы

*Сроки начала и окончания работ определяются Договором.*

## 1.4. Сведения об источниках и порядке финансирования работ

*Источник и порядок финансирования определяется Договором.*

# 2. Назначение и цели создания системы

## 2.1. Назначение Системы

Система предназначена для:
- защиты ИТ-инфраструктуры Заказчика от целевых и массовых компьютерных атак
- поиска и сбора сведений об активах;
- сбора, обработки и хранения событий;
- выявления инцидентов информационной безопасности (ИБ) и информационной поддержки процесса управления инцидентами ИБ;
- сбора, обработки и хранения сетевого трафика;
- обнаружения атак и выявления аномалий в сетевом трафике;
- расследования инцидентов;
- ретроспективного анализа трафика.
- поиска уязвимостей активов в режиме «чёрного» и «белого» ящика;
- контроля устранения выявленных уязвимостей.
-выявления вредоносного контента в файлах и электронных письмах на антивирусном, репутационном и поведенческом уровнях.

## 2.2 Цель создания Системы

Цель проведения работ по созданию Системы является снижение ущерба от компьютерных атак на информационную инфраструктуру Заказчика путем своевременного выявления и реагирования на инциденты.

# 3. Характеристика объектов автоматизации

ИТ-инфраструктура ЗАО «АРМБИЗНЕСБАНК» является распределенной и размещена на двух территориально разнесенных площадках (находятся в разных городах).

В состав ИТ-инфраструктуры входят каналы передачи данных, сетевое оборудование и аппаратное и программное обеспечение.

Сетевая инфраструктура развернута на базе следующего оборудования:

- Cisco (Catalyst, Nexus),D-Link, FortiGate Palo Alto.

В ИТ-инфраструктуре выделено несколько сетевых сегментов.

Серверы организации развернуты как на аппаратных платформах, так и в среде виртуализации (VMWare , Hyper-V).

Общее число конечных узлов (АРМ, серверов) не превышает 1500.

Общее число пользователей не превышает 1300.

Пиковые значения нагрузки на внутренние каналы передачи данных не превышают 200Мбит/с. Среднее значение нагрузки на внутренние каналы передачи данных не превышает 100Мбит/с.

# 4. Требования к системе

## 4.1. Общие требования

### 4.1.1. *Требования к структуре Системы*

4.1.1.1. Программные средства Системы должны поддерживать развертывание как на физическом, так и на виртуальном оборудовании. На площадке *Заказчика*

4.1.1.2. Система должна быть построена по модульному принципу, обеспечивающему гибкий процесс масштабирования.

4.1.1.3. В состав системы должны входить следующие функциональные подсистемы:

– *подсистема мониторинга событий информационной безопасности в составе следующих компонентов:*

- компонент сбора данных;
- компонент обработки данных;
- компонент хранения данных;
- компонент управления;

– *подсистема анализа сетевого трафика и выявления атак в составе следующих компонентов:*

- компонент сбора сетевого трафика – обеспечивает сбор сетевого трафика на каналах связи и его анализ;
- компонент обработки данных – обеспечивает обработку результатов анализа сетевого трафика, их обогащение дополнительной информацией, а также внутреннее взаимодействие и взаимодействие со смежными системами;
- компонент обнаружения сетевых атак – обеспечивает обнаружение в сетевом трафике атак на основе правил и репутационных списков;
- компонент хранения данных – обеспечивает хранение обработанного сетевого трафика и архивное хранение исходного сетевого трафика;
- компонент управления – предоставляет возможность настройки и работы с системой через пользовательский интерфейс;

– *подсистема управления уязвимостями в составе следующих компонентов:*

- компонент сбора данных;
- компонент обработки данных;
- компонент хранения данных;
- компонент управления;

– *подсистема многоуровневой защиты от вредоносного контента в составе следующих компонентов:*

- компонент статического анализа – обеспечивает проверку файлов на основе антивирусных решений нескольких производителей, а также проверку по репутационным спискам;
- компонент поведенческого анализа - обеспечивает поведенческий анализ файлов в изолированной виртуальной среде;
- компонент хранения – обеспечивает хранение поступивших на проверку файлов и результатов проверки;
- компонент управления - предоставляет возможность настройки и работы с системой через пользовательский интерфейс.

4.1.2. *Требования к способам и средствам обеспечения информационного взаимодействия между компонентами Системы, а также Системы со смежными системами*

4.1.2.1. Для информационного обмена между компонентами Системы с использованием сети передачи данных должны использоваться унифицированные информационные способы взаимодействия с использованием стека протоколов TCP/IP и технологии канального уровня Ethernet.

4.1.2.2. Подсистема мониторинга событий информационной безопасности должна обеспечивать сбор событий от других подсистем, входящих в состав Системы.

4.1.2.3. Подсистема анализа сетевого трафика и выявления атак должна обеспечивать интеграцию с подсистемой многоуровневой защиты от вредоносного контента в части передачи на анализ передаваемых по сети файлов.

4.1.2.4. Все подсистемы, входящие в состав Системы, должны поддерживать возможность входа администраторов через единую систему авторизации.

4.1.2.5. Проектируемые средства и системы при использовании веб технологий в качестве средств коммуникации должны поддерживать:

– защищённое взаимодействие по протоколу HTTPS

– применение SSL-сертификатов, подтверждающих подлинность участников взаимодействия.

4.1.2.6. Система должна взаимодействовать со следующими смежными системами:

– системами точного времени на основе протокола NTP;

– системами аутентификации на основе протокола LDAP;

– системами электронной почты на основе протокола SMTP (отправка уведомлений);

– системами разрешения доменных имен на основе протокола DNS.

а также:

– иметь возможность загрузки обновлений с серверов разработчика;

– иметь возможность уведомления ответственных лиц с помощью почтовых сообщений и технологии webhook:

– иметь возможность передачи выявленных инцидентов во внешние системы;

– захват копии трафика для его анализа (копия формируется с использованием port mirroring, TAP-устройств, и т.п.);

– системой электронной почты для самостоятельной отправки пользователями файлов на проверку и получения вердикта по проведенной проверке;

– файловым сервером для проверки файлов на общих файловых ресурсах;

– системой электронной почты на базе Microsoft Exchange (через специальный агент) для проверки и блокирования электронных писем и содержащихся в них файлов.

4.1.3. *Требования к режимам функционирования Системы*

4.1.3.1. Система должна функционировать в следующих режимах:

– штатный режим;

– режим технологического обслуживания;

– аварийный режим.

4.1.3.2. Asas В штатном режиме функционирования Система должна обеспечивать решение функциональных задач в полном объеме.

4.1.3.3. В технологическом режиме функционирования Система должна обеспечивать работу функций обновления программного обеспечения Системы, а также самодиагностики для проведения обслуживания.

4.1.3.4. В аварийном режиме функционирования Системы допускается отказ одной или нескольких подсистем, при этом не должно оказывать влияния на ИТ-инфраструктуру Заказчика. При переходе Системы в аварийный режим необходимо выполнить комплекс мероприятий по восстановлению работоспособности комплекса и устранению причин перехода Системы в аварийный режим.

4.1.4. *Требования к диагностированию*

4.1.4.1. Asa Должны предусматриваться механизмы диагностирования неисправностей в процессе установки программного обеспечения (ПО) Системы.

4.1.4.2. Система должна обеспечить индикацию собственного состояния и уведомления в интерфейсе пользователя о сбоях в работе сервисов Системы.

4.1.4.3. Система должна обеспечивать визуализацию характеристик входящего потока событий.

4.1.5. *Требования к перспективе развития и модернизации Системы*

4.1.5.1. Система должна обеспечивать возможность развития и модернизации в рамках технической поддержки разработчика:

– увеличение количества поддерживаемых источников данных (событий и типов активов), в том числе новых, ранее не поддерживаемых;

– модернизация и оптимизация правил обработки и анализа событий ИБ увеличение количества поддерживаемых для сканирования систем;

– добавление новых функциональных возможностей.

4.1.5.2. Система должна обеспечивать возможность увеличения производительности и масштабирования за счёт увеличения количества компонентов Системы и производительности их аппаратных или виртуализованных платформ.

**4.2. Требования к функциональным подсистемам**

4.2.1. *Требования к подсистеме мониторинга событий информационной безопасности*

4.2.1.1. Требования к компоненту сбора данных

4.2.1.1.1. *Требования в части управления сбором данных*

4.2.1.1.1.1. Должна обеспечиваться возможность создания, изменения, удаления, запуска, остановки задач сбора данных, также поиска и сортировки задач по их атрибутам.

4.2.1.1.1.2. Должна обеспечиваться возможность создания, изменения, удаления, а также поиска профилей, определяющих протоколы и способы сбора данных.

4.2.1.1.1.3. Должна обеспечиваться возможность создания, изменения, удаления учётных записей, необходимых для авторизации на источниках данных.

4.2.1.1.1.4. Должна обеспечиваться возможность экспорта и импорта профилей сбора данных в файл.

4.2.1.1.2. *Требования в части сбора событий*

4.2.1.1.2.1. Перечень поддерживаемых источников событий, указывается Испольнителем, в пакете документов на тендер.

4.2.1.1.2.2. Должен обеспечиваться пассивный (без подключения к источнику) сбор событий с использованием протоколов syslog, SNMP (Trap), Cisco NetFlow.

4.2.1.1.2.3. Должен обеспечиваться активный сбор событий, то есть с подключением и выполнением команд и запросов к источникам событий с использованием протоколов и механизмов: DCE/RPC (WMI), CIFS/SMB (RPC), DCOM (RPC), SSH, Telnet, OPSEC LEA, VMware API, ODBC API (MySQL protocol, PostgreSQL protocol, Tibero, MS SQL, Oracle SQL).

4.2.1.1.3. *Требования в части сбора данных об активах*

4.2.1.1.3.1. Должны обеспечиваться выявление и идентификация активов, включенных и подключенных к ЛВС на момент сканирования сети с использованием стека TCP/IP.

4.2.1.1.3.2. Должен обеспечиваться активный сбор инвентаризационной и конфигурационной информации с помощью следующих протоколов и механизмов удалённого управления: DCE/RPC (WMI), LDAP, SSH, Telnet, ODBC API, ODBC API, SNMP, OPSEC, VMware API.

4.2.1.1.3.3. При сетевом сканировании должны решаться следующие задачи:

– поиск активов (сетевых узлов ИС) в области, заданной пользователем по IP-адресам (подсетям), именам или внутрисистемным идентификаторам активов;

– ограничение или выбор числа портов и протоколов транспортного уровня, используемых при сканировании;

– сбор инвентаризационной информации (идентификация доступных сетевых служб и ПО), в том числе Система должна обеспечивать:

o идентификацию наименования и версии ОС семейства Microsoft Windows;

o идентификацию сетевых служб, использующих транспортные протоколы TCP и UDP;

– возможность подбора паролей для протоколов:

o электронной почты — SMTP, POP3;

o файловые службы — FTP;

o удалённого управления — RDP, SSH, Telnet, SNMP, VNC, Radmin, Symantec PCAnywhere, NetBIOS;

o баз данных — Microsoft SQL, Oracle DB, Sybase, DB2, MySQL, PostgreSQL;

o бизнес-приложения — SAP DIAG, SAP RFC;

o сред виртуализации — VMware vSphere;

o IP-телефония — SIP.

4.2.1.1.3.4. При выполнении системного сканирования должны решаться следующие задачи:

– подключение к выбранным активам, заданным пользователем по IP-адресам (подсетям), FQDN-именам или иным идентификаторам активов, используемым Системой;

– выбор способов (протоколов) подключения к активам и определения учётных записей, используемых для аутентификации;

– сбор идентификационной и конфигурационной информации:

o идентификационных данных об активах (IP-адрес, FQDN и другие);

o данных о составе аппаратного обеспечения (материнская плата, центральный процессор, сетевая карта и другие);

o данных о составе программного обеспечения (BIOS, ОС, общесистемное ПО и другие);

o данных о настройках ОС семейства Windows (локальные и доменные политики);

o данных о запущенных службах и задачах планировщика ОС.

4.2.1.1.3.5. Для поиска слабых паролей и пар «логин — пароль», Система должна обеспечивать:

– группировку инструкций по подбору паролей в выделенные редактируемые справочники;

– наличие заполненных справочников пар «логин — пароль»;

– возможность создавать, изменять или удалять пользовательские справочники;

– возможность определять какой справочник будет использоваться при попытке подбора пароля.

4.2.1.2. *Требования к компоненту обработки данных*

4.2.1.2.1. Компонент включает следующие группы функций:

– функции управления обработкой событий;

– функции обработки событий;

– функции управления обработкой инцидентов;

– функции обработки инцидентов;

– функции управления обработкой активов;

– функции обработки активов;

– функции управления базой знаний;

– функции базы знаний.

4.2.1.2.2. *Функциональные требования к управлению обработкой событий*

4.2.1.2.2.1. Должно обеспечиваться отображение информации о каждом исходном и обработанном событии.

4.2.1.2.2.2. Должна обеспечиваться возможность запуска и остановки работы правил обогащения и корреляции.

4.2.1.2.2.3. Должна обеспечиваться возможность определения пороговых значений нагрузки, создаваемой правилами корреляции.

4.2.1.2.2.4. Должна обеспечиваться поддержка следующих механизмов поиска и сортировки обработанных событий, в том числе должна обеспечиваться:

– сортировка и поиск событий по заданному набору атрибутов и их значениям с использованием встроенного языка запросов;

– быстрое создание фильтра путем одиночного нажатия на основных атрибутах обработанного события левой клавишей мыши;

– сохранение пользовательских фильтров для быстрого доступа к интересующим событиям.

4.2.1.2.2.5. Должна обеспечиваться возможность сохранения истории выполнения запросов и повторное использования запросов фильтрации событий из истории.

4.2.1.2.3. *Функциональные требования к обработке событий*

4.2.1.2.3.1. Должна обеспечиваться нормализация событий на основе правил (формул) нормализации.

4.2.1.2.3.2. Должно обеспечиваться объединение однотипных событий на основе правил агрегации.

4.2.1.2.3.3. Должно обеспечиваться обогащение событий дополнительной информацией на основе правил обогащения.

4.2.1.2.3.4. Должна обеспечиваться возможность формирования мультиязычного описания событий на основе правил локализации.

4.2.1.2.3.5. Должна обеспечиваться корреляция событий для выявления инцидентов и событий ИБ на основе правил корреляции.

4.2.1.2.3.6. Должна обеспечиваться возможность многоуровневой корреляции с передачей результатов работы одного правила корреляции на вход другим правилам корреляции.

4.2.1.2.3.7. Должно обеспечиваться наличие предустановленных правил (формул) нормализации, агрегации, обогащения, локализации и корреляции.

4.2.1.2.3.8. Должна обеспечиваться возможность использования в правилах обогащения и корреляции табличных списков — массивов данных, содержащих информацию следующих типов:

– справочных данных о наименовании портов, протоколов и иных типов технологических данных;

– данных об активах;

– репутационных данных: IP-адресов, доменных имён, хэш-сумм файлов.

4.2.1.2.3.9. Должно обеспечиваться автоматическое наполнение табличных списков информацией в ходе корреляции событий для использования в других правилах корреляции.

4.2.1.2.3.10. Должно обеспечиваться автоматическое удаление устаревших записей в табличных списках (для автоматически добавленных записей).

4.2.1.2.3.11. Должно обеспечиваться наличие предустановленных табличных списков.

4.2.1.2.3.12. Должна обеспечиваться возможность внесения поправки во временные характеристики событий для корректировки разницы часовых поясов через профили сбора данных.

4.2.1.2.3.13. Должна обеспечиваться автоматическая коррекция времени появления событий при выявлении некорректного времени на источнике.

4.2.1.2.3.14. Должна обеспечиваться возможность присвоения коррелированным событиям категорий важности.

4.2.1.2.3.15. Должна обеспечиваться обработка мультиязычных событий.

4.2.1.2.3.16. Должна обеспечиваться автоматическая ассоциация (привязка) активов с событиями.

4.2.1.2.3.17. Должно обеспечиваться автоматическое отключение правил корреляции на основе заданных пороговых значений расходования вычислительных ресурсов при корреляции.

4.2.1.2.3.18. Должно обеспечиваться оповещение пользователя об автоматическом отключении правила корреляции.

4.2.1.2.4. *Функциональные требования к управлению обработкой инцидентов*

4.2.1.2.4.1. Должно обеспечиваться отображение информации об инциденте в виде карточки инцидента.

4.2.1.2.4.2. Должно обеспечиваться управление карточками инцидентов, включая:

– ручное добавление или удаление карточки инцидента, или изменение данных карточки;

– возможность вручную связать инцидент с событиями и активами;

– возможность создания задач для пользователей Системы по расследованию, сбору доказательств и восстановлению работоспособности ИС;

– возможность сохранения проведенных мероприятий и их комментирование;

– хранение истории изменений карточки инцидента и выполнения поставленных задач.

4.2.1.2.4.3. Должна обеспечиваться поддержка механизмов фильтрации и сортировки инцидентов, включая:

– возможность сортировки и фильтрации по заданному набору атрибутов и их значениям с использованием языка запросов и (или) по группе активов;

– быстрое создание фильтров путем одного клика на основных атрибутах инцидента;

– сохранение пользовательских фильтров для быстрого доступа к интересующим карточкам инцидентов.

4.2.1.2.4.4. Должна обеспечиваться возможность экспорта и импорта карточек инцидентов в формате JSON.

4.2.1.2.5. *Функциональные требования к обработке инцидентов*

4.2.1.2.5.1. Должно обеспечиваться автоматическое формирование карточек инцидентов по результатам срабатывания правил корреляции.

4.2.1.2.5.2. Должна обеспечиваться автоматическая привязка событий и активов к инцидентам.

4.2.1.2.6. *Функциональные требования к управлению обработкой активов*

4.2.1.2.6.1. Должно обеспечиваться отображение конфигурационной информации об активе в виде карточки актива.

4.2.1.2.6.2. Должно обеспечиваться управление карточками активов, включая:

- ручное добавление, изменение, или удаление карточки актива;
- отображение даты и времени последнего обновления информации об активе;
- задание уровня значимости актива;
- задание статусов (сроков) актуальности данных.

4.2.1.2.6.3. Должно обеспечиваться ведение истории изменения карточки актива с отображением истории изменения карточек активов с возможностью:

– просмотра состояния актива на заданный момент времени или за указанный период;

– сравнения конфигураций актива в два различных момента времени.

4.2.1.2.6.4. Должно обеспечиваться управление списком активов, включая:

– поиск активов по их атрибутам;

– группировку активов в статические и динамически формируемые группы:

- членство в статических группах определяется пользователем;
- членство в динамических группах определяется Системой автоматически на основе информации об активе (IP-адресов, ОС и т.п.).

– построение иерархии групп активов.

4.2.1.2.6.5. Должен обеспечиваться контроль ключевых показателей процесса управления активами путём реализации настраиваемых политик и (или) правил, включая:

– активацию или деактивацию политики (правила);

– добавление, изменение или удаление политики (правила).

4.2.1.2.6.6. Должны реализовываться следующие политики (правила):

– определение и (или) изменение сроков актуальности и устаревания данных об активе;

– определение перечня активов, на которые действует правило;

– присвоение значимости активам.

4.2.1.2.7. *Функциональные требования к обработке активов*

4.2.1.2.7.1. При активации политики (правила) должны выполняться все настроенные в нём действия, при деактивации — состояние активов должно изменяться на исходное, существовавшее до активации политики (правила).

4.2.1.2.7.2. Должно обеспечиваться автоматическое создание карточек активов на основе информации, собранной в результате выполнения задач сбора данных.

4.2.1.2.7.3. Должно обеспечиваться автоматическое изменение инвентаризационной и конфигурационной информации об активах в результате выполнения задач сбора данных.

4.2.1.2.7.4. Должна обеспечиваться поддержка следующих механизмов фильтрации и сортировки активов:

– сортировка и фильтрация перечня активов по заданному набору атрибутов и их значениям;

– быстрое создание группы фильтрации путем одиночного нажатия левой клавиши мыши на значения основных атрибутов актива;

– возможность отображения активов, удовлетворяющих условиям заданного фильтра.

4.2.1.2.7.5. Должна обеспечиваться поддержка работы с топологией сети, включая:

– построение и визуализация топологии сети на уровне L3 модели OSI на основе собранной Системой информации;

– возможность проверки сетевой доступности между активами на основе собранной Системой информации;

– возможность отображения активов, удовлетворяющих условиям заданного фильтра.

4.2.1.2.7.6. Должна обеспечиваться возможность мониторинга обработки активов для оценки нагрузки на Систему.

4.2.1.2.8. *Функциональные требования к управлению базой знаний*

4.2.1.2.8.1. Должно обеспечиваться управление (в том числе создание, изменение и удаление) элементов базы знаний:

– правилами (формулами) нормализации, агрегации, локализации, обогащения и корреляции;

– макросами, используемыми при создании правил корреляции;

– табличными списками следующих типов:

  - с данными об активах, автоматически заполняемыми в результате выполнения задач сбора данных;
  - со справочными данными, обеспечивающими представление технологической информации в человекочитаемой форме;
  - с репутационными данными — наборами индикаторов компрометации;
  - на основе автоматически заполняемых списков, используемых правилами корреляции и обогащения для временного хранения информации.

4.2.1.2.8.2. Должна обеспечиваться возможность использования графического конструктора при создании пользовательских правил корреляции, предоставляющего:

– возможность использования предустановленных и пользовательских макросов;

– автоматическое формирование представления правила в формате встроенного языка запросов;

– возможность формирования и редактирования пользовательских правил корреляции встроенным языком запросов напрямую из конструктора правил.

4.2.1.2.8.3. Должна обеспечиваться проверка синтаксической корректности разработанных правил (формул) нормализации, агрегации, локализации, обогащения и корреляции.

4.2.1.2.8.4. Должна обеспечиваться возможность установки выбранных пользователем правил из базы знаний в Систему.
4.2.1.2.8.5. Должно обеспечиваться хранение и управление (в том числе активация, деактивация) табличных списков.
4.2.1.2.8.6. Должна обеспечиваться группировка материалов базы знаний в отдельные папки по выбору пользователя.
4.2.1.2.8.7. Должна обеспечиваться поддержка экспорта и импорта контента базы знаний.

4.2.1.2.9. *Функциональные требования к компоненту базы знаний*

4.2.1.2.9.1. Должно обеспечиваться формирование и хранение базы всех (как активных (используемых), так и неиспользуемых правил (формул) нормализации, агрегации, обогащения, локализации и корреляции.
4.2.1.2.9.2. Должно обеспечиваться формирование и хранение табличных списков.
4.2.1.2.9.3. Должно обеспечиваться формирование и хранение макросов (шаблонов фильтров событий, используемых при создании правил корреляции).
4.2.1.2.9.4. Должна обеспечиваться валидация пользовательских правил (формул), табличных списков, макросов с проверкой их структуры, синтаксиса, корректности указанных условий и совместимости правил между собой.

4.2.1.3. *Требования к компоненту хранения*

4.2.1.3.1. Должна обеспечиваться возможность хранения исходных и (или) обработанных событий.

4.2.1.3.2. Должна обеспечиваться поддержка хранения данных на внешних системах хранения.

4.2.1.3.3. Компонент хранения должна обеспечивать хранение выявленных в различные моменты времени сведений об активах.

4.2.1.4. *Требования к компоненту управления*

Должны реализовываться следующие группы функций:

– управление доступом;
– управление обновлениями;
– управление иерархией;
– предоставление пользовательского интерфейса.

4.2.1.4.1. *Функциональные требования к управлению доступом*

4.2.1.4.1.1. Должна обеспечиваться идентификация, аутентификация и авторизация пользователей Системы на основе учётных записей.
4.2.1.4.1.2. Должна обеспечиваться реализация ролевой модели управления доступом к функциям Системы.
4.2.1.4.1.3. Должна обеспечиваться возможность управления (в том числе создание или изменение) учётными записями пользователей Системы:

– логинами и паролями;
– ролями (в том числе для отдельных площадок в иерархии);
– методами аутентификации (локальная база или LDAP-аутентификация).

4.2.1.4.1.4. Должна обеспечиваться поддержка интеграции с внешними системами аутентификации по протоколу LDAP.
4.2.1.4.1.5. Должно обеспечиваться бесшовное соотнесение ролей пользователей Системы с ролями Microsoft Active Directory.
4.2.1.4.1.6. Должна обеспечиваться возможность генерации пользовательских паролей.
4.2.1.4.1.7. Должна обеспечиваться возможность блокировки учётной записи.
4.2.1.4.1.8. Должно обеспечиваться журналирование действий пользователей:

– с активами;
– с событиями;

– с инцидентами;
– с функциями управления иерархией;
– с функциями управления сбором данных;
– с функциями управления Системой;
– вход или выход из Системы.

4.2.1.4.1.9. Должна обеспечиваться возможность фильтрации журналов регистрации событий по пользователям и их действиям в Системе.

4.2.1.4.2. *Функциональные требования к управлению обновлениями*

4.2.1.4.2.1. Должно обеспечиваться получение обновлений ПО и базы знаний.

4.2.1.4.2.2. Должна обеспечиваться возможность распространения файлов обновлений ПО на отчуждаемых носителях информации.

4.2.1.4.2.3. Должна обеспечиваться возможность ручного запуска обновлений ПО и автоматического обновления базы знаний.

4.2.1.4.3. *Функциональные требования к пользовательскому интерфейсу*

4.2.1.4.3.1. Должен обеспечиваться доступ пользователям для:

– администрирования Системы с помощью: веб-интерфейса и (или) графического интерфейса, и (или) интерфейса командной строки;
– выполнения основных функций Системы с помощью веб-интерфейса.

4.2.1.4.3.2. Должно обеспечиваться уведомление о изменения статусов основных системных сущностей (активов, задач сбора данных, состояния системы) с их отправкой на электронную почту или по POST-запросу.

4.2.1.4.3.3. Должно обеспечиваться уведомление о сбоях в работе сервисов и отображение состояния Системы в интерфейсе пользователя.

4.2.1.4.3.4. Должна обеспечиваться визуализация и настройка статистических данных о результатах функционирования Системы с использованием панелей мониторинга:

– визуализации подлежат оперативные данные о событиях, инцидентах, активах и состоянии работоспособности Системы в виде графиков, диаграмм и таблиц, закрепляемых за отдельными виджетами;
– настройка должна обеспечивать:
  - возможность создания пользовательских виджетов с использованием графического конструктора и с указанием необходимых источников данных и их типов визуализации (график, диаграмма, таблица);
  - возможность настройки периодичности обновления виджетов.

4.2.1.4.3.5. Должно обеспечиваться предоставление пользователю панелей мониторинга, содержащих настраиваемые виджеты.

4.2.1.4.3.6. Должно обеспечиваться наличие предустановленных панелей мониторинга и обеспечиваться возможность создания пользовательских панелей мониторинга.

4.2.1.4.3.7. Должно обеспечиваться создание виджетов по событиям, инцидентам и активам.

4.2.1.4.3.8. Должно обеспечиваться наличие предустановленных виджетов по активам, событиям и инцидентам:

– количество активов;
– значимость активов;
– актуальность данных об активах;
– количество событий;
– средний поток событий;
– распределение среднего потока событий;
– количество инцидентов;
– инциденты по уровню опасности;
– инциденты по категории.

4.2.1.4.3.9. Должна обеспечиваться возможность настройки, построения, отправки и экспорта отчётов, за счёт:

– наличия предустановленных форм отчётов;

– возможности создания пользовательских форм отчётов с помощью конструктора отчётов, позволяющего:

- задать последовательность объектов отчёта (текста, изображений, актуальной информации из виджетов);
- задать тип визуализации данных (диаграммы, графики, гистограммы);
- настроить внешний вид отчёта (колонтитулы, легенду, подписи к объектам отчёта).

– возможность выпуска отчётов вручную или по расписанию, в том числе с отправкой на заданный адрес электронной почты;

– возможность экспорта отчётов в один из следующих форматов: PDF, XLSX.

4.2.2. *Требования к подсистеме анализа сетевого трафика и выявления атак*

4.2.2.1. *Требования к компоненту сбора сетевого трафика*

4.2.2.1.1. Захват сетевого трафика с выбранного сетевого интерфейса.

4.2.2.1.2. Захват сетевого трафика с использованием фильтров по следующим параметрам:

– протокол транспортного уровня;

– сетевой порт или группа портов;

– IP-подсеть или группа IP-подсетей;

– IP-адрес или группа IP-адресов.

4.2.2.1.3. Импорт сетевого трафика из файлов формата pcap.

4.2.2.1.4. Анализ захваченного сетевого трафика и реконструкция сессий с возможностью разбора протоколов:

– IP (IPv4, IPv6);

– TCP;

– UDP;

– ICMP;

– DHCP;

– HTTP;

– DNS;

– SSL/TLS (при наличии ключа);

– SSH;

– SMTP;

– POP3;

– IMAP;

– Telnet;

– FTP;

– TFTP;

– NTP;

– SIP;

– SNMP;

– DCE/RPC;

– KERBEROS;

– LDAP;

– NFS;

– SMB;

– NTLM.

4.2.2.1.5. Извлечение файлов и данных, передаваемых по протоколам прикладного уровня (HTTP, SMTP, FTP, SMB, TFTP, POP3, IMAP, NFS).

4.2.2.1.6. Запись захваченного сетевого трафика в файлы формата pcap.

4.2.2.2. *Функции компонента обработки данных*

4.2.2.2.1. Обогащение информации о сетевом взаимодействии следующими данными:

– географическая принадлежность IP-адресов, участвующих в сетевом взаимодействии;

– имена, типы передаваемых файлов и их контрольные суммы;

– доменные имена узлов на основании захваченного сетевого трафика;

– информация о баннерах сетевых приложений, участниках сетевого взаимодействия (IP, MAC, ОС и др.);

– принадлежность обнаруженных доменных имен, IP-адресов и URL-ссылок, а также передаваемых файлов к репутационному списку.

4.2.2.2.2. Индексация всего захватываемого сетевого трафика с сохранением в БД следующей полученной информации о сессии:

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

4.2.2.3. *Функции компонента обнаружения сетевых атак*

4.2.2.3.1. Выявление компьютерных атак в захваченном трафике на основе правил и репутационных списков.

4.2.2.3.2. Ретроспективный анализ сетевого трафика и выявление в нем атак.

4.2.2.3.3. Автоматический ретроспективный анализ сетевого трафика и выявление атак при обновлении репутационных списков.

4.2.2.3.4. Автоматическая классификация и определение уровня опасности атак.

4.2.2.3.5. Обнаружение DGA-доменов среди доменных имен отправителя и получателя, а также при разрешении имен с помощью DNS.

4.2.2.3.6. Возможность использования правил и репутационных списков:

- встроенных;
- пользовательских;
- предоставляемых экспертными организациями (Emerging Threats).

4.2.2.3.7. Поддержка правил обнаружения сетевых атак в формате Suricata.

4.2.2.3.8. Отправка информации о выявленных атаках во внешние системы по протоколу syslog.

4.2.2.4. *Функции компонента хранения данных*

4.2.2.4.1. Хранение исходного сетевого трафика в формате pcap в течении заданного времени.

4.2.2.4.2. Хранение обработанного сетевого трафика (индексов) в течение заданного времени.

4.2.2.5. *Функции компонента управления*

4.2.2.5.1. Доступ пользователей к подсистеме через веб-интерфейс.

4.2.2.5.2. Доступ пользователей к подсистеме через интерфейс командной строки.

4.2.2.5.3. Управление учетными записями пользователей (создание, изменение, удаление, блокирование).

4.2.2.5.4. Разграничение доступа пользователей к функциям подсистемы.

4.2.2.5.5. Регистрация действий пользователей в подсистеме:

- вход/выход в веб-интерфейс управления;
- управление учетными записями;
- управление ролями и правами доступа;
- управление компонентами сбора сетевого трафика;
- создание и экспорт отчетов;
- импорт и экспорт данных.

4.2.2.5.6. Контроль целостности программного обеспечения подсистемы.

4.2.2.5.7. Формирование и предоставление отчетов в форматах docx и pdf.

4.2.2.5.8. Формирование отчетов по расписанию.

4.2.2.5.9. Самодиагностика работы компонентов подсистемы и оповещение пользователя о неисправностях.

4.2.2.5.10. Сбор статистики работы с узлов с установленными компонентами подсистемы и ее передачи в системы внешнего мониторинга.

4.2.2.5.11. Автоматическое построение схемы сетевых связей узлов сети.

4.2.2.5.12. Управление компонентами сбора сетевого трафика (включение, выключение функции сбора).

4.2.2.5.13. Управление фильтрами сбора сетевого трафика (создание, изменение, удаление).

4.2.2.5.14. Поиск и просмотр сохраненной в системе информации по сетевым взаимодействиям по различным параметрам.

4.2.2.5.15. Предоставление возможности выгрузки данных о сессиях в файлы форматов csv и json.

4.2.2.5.16. Управление репутационными списками (создание, изменение, удаление).

4.2.2.5.17. Управление правилами обнаружения атак (создание, изменение, копирование, удаление, импорт).

4.2.2.5.18. Уведомление пользователей подсистемы о результатах анализа сетевого трафика и выявленных атаках на электронную почту

4.2.2.5.19. Поиск и просмотр сохраненной в системе информации по обнаруженным атакам по различным параметрам.

4.2.2.5.20. Возможность маркировка атаки как ложной.

4.2.2.5.21. Автоматическое обновление правил и репутационных списков.

4.2.2.5.22. Просмотр информации о хранилищах данных.

4.2.2.5.23. Просмотр данных из выбранного хранилища.

4.2.2.5.24. Импорт сетевого трафика в выбранное хранилище.

4.2.2.5.25. Выгрузка выбранной пользователем сессии из хранилища в формате pcap.

4.2.3. ***Требования к подсистеме управления уязвимостями***

4.2.3.1. *Требования к компоненту сбора данных*

4.2.3.1.1. Требования в части управления сбором данных

4.2.3.1.1.1. Компонент сбора данных должна обеспечивать возможность создания, изменения, удаления, запуска, остановки задач сбора данных, также поиска и сортировки задач по их атрибутам.

4.2.3.1.1.2. Компонент сбора данных должен обеспечивать возможность создания, изменения, удаления, а также поиска профилей, определяющих протоколы и способы сбора данных.

4.2.3.1.1.3. Компонент сбора данных должен обеспечивать возможность создания, изменения, удаления учётных записей, необходимых для авторизации на активах.

4.2.3.1.2. *Требования в части сбора данных об активах*

4.2.3.1.2.1. Компонент сбора данных должен обеспечивать выявление и идентификацию активов, включенных и подключенных к ЛВС на момент сканирования сети с использованием стека TCP/IP.

4.2.3.1.2.2. Компонент сбора данных должен обеспечивать активный сбор инвентаризационной и конфигурационной информации с помощью следующих протоколов и механизмов удалённого управления: DCE/RPC (WMI), LDAP, SSH, Telnet, ODBC API, ODBC API, SNMP, OPSEC, VMware API.

4.2.3.1.2.3. При сетевом сканировании компонент сбора данных должен решать следующие задачи:

– поиск активов (сетевых узлов ИС) в области, заданной пользователем по IP-адресам (подсетям), именам или внутрисистемным идентификаторам активов;

– ограничение или выбор числа портов и протоколов транспортного уровня, используемых при сканировании;

– сбор инвентаризационной информации (идентификацию доступных сетевых служб и ПО):

- обеспечивать идентификацию наименования и версии ОС семейства Microsoft Windows;
- обеспечивать идентификацию сетевых служб, использующих транспортные протоколы TCP и UDP;

– обеспечивать возможность подбора паролей для протоколов:

- электронной почты – SMTP, POP3;
- файловые службы – FTP;
- удалённого управления – RDP, SSH, Telnet, SNMP, VNC, Radmin, Symantec PCAnywhere, NetBios;
- баз данных – Microsoft SQL, Oracle DB, Sybase, DB2, MySQL, PostgreSQL;
- бизнес приложения – SAP DIAG, SAP RFC;
- сред виртуализации – VMware vSphere;
- IP-телефония – SIP.

4.2.3.1.2.4. При выполнении системного сканирования компонент сбора данных должен решать следующие задачи:

– подключение к выбранным активам, заданным пользователем по IP-адресам (подсетям), FQDN-именам или иным идентификаторам активов, используемым Системой;

– выбор способов (протоколов) подключения к активам и определения учётных записей, используемых для аутентификации;

– сбор идентификационной и конфигурационной информации:

- идентификационных данных об активах (IP-адрес, FQDN и другие);
- данных о составе аппаратного обеспечения (материнская плата, центральный процессор, сетевая карта и другие);
- данных о составе программного обеспечения (BIOS, ОС, общесистемное ПО и другие);
- данных о настройках ОС семейства Windows (локальные и доменные политики);
- данных о запущенных службах и задачах планировщика ОС.

4.2.3.1.2.5. Для поиска слабых паролей и пар логин/пароль компонент сбора данных должен обеспечивать:

– группировку инструкций по подбору паролей в выделенные редактируемые справочники;

– предусматривать предустановленные в Системе справочники;

– возможность создавать/изменять/удалять пользовательские справочники;

– возможность определять какой справочник будет использоваться при подборе попытке подбора пароля.

4.2.3.2. ***Требования к компоненту обработки данных***

4.2.3.2.1. *Функциональные требования к обработке активов*

4.2.3.2.1.1. Компонент обработки данных должен обеспечивать отображение инвентаризационной и информации об активе в виде карточки актива.

4.2.3.2.1.2. Компонент обработки данных должен обеспечивать управление карточками активов, включая:

– ручное добавление/изменение/удаление карточки актива;

– отображение даты и времени последнего обновления информации об активе;

– задание уровня значимости актива;

– задание статусов (сроков) актуальности данных.

4.2.3.2.1.3. Компонент обработки данных должен обеспечивать автоматическое создание карточек активов на основе информации, собранной в результате выполнения задач сбора данных.

4.2.3.2.1.4. Компонент обработки данных должен обеспечивать автоматическое изменение инвентаризационной и конфигурационной информации об активах в результате выполнения задач сбора данных.

4.2.3.2.1.5. Компонент обработки данных должен обеспечивать ведение истории изменения карточки актива с отображением истории изменения карточек активов с возможностью:

- просмотра состояния актива на заданный момент времени;
- сравнения конфигураций актива в два различных момента времени.

4.2.3.2.1.6. Компонент обработки данных должен обеспечивать управление списком активов, включая:

– поиск активов по их атрибутам;

– группировку активов в статические и динамически формируемые группы:

- членство в статических группах определяется пользователем;
- членство в динамических группах определяется Системой автоматически на основе информации об активе (IP-адресов, ОС и т.п.).

– построение иерархии групп активов.

4.2.3.2.1.7. Компонент обработки данных должен обеспечивать поддержку следующих механизмов фильтрации и сортировки активов:

– сортировка и фильтрация перечня активов по заданному набору атрибутов и их значениям;

– быстрое создание группы фильтрации путем одного клика на значениях основных атрибутов актива;

– возможность отображения активов, удовлетворяющих условиям заданного фильтра.

4.2.3.2.1.8. Компонент обработки данных должен обеспечивать поддержку работы с топологией сети, включая:

– построение и визуализация топологии сети на уровне L3 модели OSI на основе собранной Системой информации;

– возможность проверки сетевой доступности между активами на основе собранной Системой информации;

– возможность отображения активов, удовлетворяющих условиям заданного фильтра.

4.2.3.2.2. *Функциональные требования к обработке уязвимостей*

4.2.3.2.2.1. Компонент обработки данных должен обеспечивать следующие действия с уязвимостями:

- поиском и сортировкой уязвимостей по их атрибутам;
- автоматическое выявление уязвимостей;
- автоматическая ассоциация активов с уязвимостями;
- выделением важных (критических) уязвимостей;
- созданием/удалением информации (меток) к уязвимостям;
- контролем выполнения работ по устранению уязвимостей;
- демонстрацию карточек уязвимостей, содержащих справочную информацию в развёрнутом виде;
- возможность изменения статуса уязвимости;

– возможность контроля устранения уязвимостей;

– градацию уязвимостей в том числе выявление трендовых уязвимостей, то есть уязвимостей, которые активно используются в атаках злоумышленников в актуальный период времени (при условии постоянных обновлений базы знаний Системы);

– возможность проведения массовых операций над уязвимостями.

4.2.3.2.2.2. Компонент обработки данных должен обеспечивать представление ссылки на иные базы уязвимостей (по результатам сетевого и системного сканирования).

4.2.3.2.2.3. Компонент обработки данных должен обеспечивать представление сведений об уязвимостях в соответствии с таксономией CVSSv2 и CVSSv3.

4.2.3.2.3. Функциональные требования к контролю ключевых показателей процессов управления активами и уязвимостями

4.2.3.2.3.1. Компонент обработки данных должен обеспечивать отображение и управление контролем ключевых показателей процесса управление контролем ключевых показателей процесса в виде настраиваемых политик/правил, включая:

– активацию/деактивацию политики/правила;

– добавление/изменение/удаление политики/правила.

4.2.3.2.3.2. Компонент обработки данных должен реализовывать следующие политики/правила:

– для контроля сроков актуальности данных об активах, имеющие следующие возможности:

○ определение/изменение сроков актуальности и устаревания данных об активе;

○ определение перечня активов, на которые действует правило.

– для контроля устранения уязвимостей, имеющие следующие возможности:

○ определение/изменение действий с уязвимостью по результатам применения правила;

○ определение/изменение статус, который получает уязвимость при выполнении правила;

○ добавление/изменение/удаление фильтра уязвимостей, на которые действует правило;

○ определение перечня активов, на которые действует правило.

– для пометки критически важных уязвимостей, имеющих следующие возможности:

○ присвоение уникальной метки, по которой легко выявить помеченный актив;

○ добавление/изменение/удаление фильтра уязвимостей, на которые действует правило;

○ определение перечня активов, на которые действует правило.

4.2.3.2.3.3. Компонент обработки данных при активации политики/правила должен выполнять все настроенные в нём действия, при деактивации должно вернуть изменения состояния активов и уязвимостей в исходное (то которое было до активации политики/правила).

4.2.3.3. ***Требования к компоненту хранения***

4.2.3.3.1. Компонент хранения должен обеспечивать хранение выявленных в различные моменты времени сведений об активах и сведений об их уязвимостях.

4.2.3.4. ***Требования к компоненту управления***

4.2.3.4.1. *Функциональные требования к управлению доступом*

4.2.3.4.1.1. Компонент управления должен обеспечивать идентификацию, аутентификацию и авторизацию пользователей Системы на основе учётных записей.

4.2.3.4.1.2. Компонент управления должен обеспечивать реализацию ролевой модели управления доступом к функциям Системы.

4.2.3.4.1.3. Компонент управления должен обеспечивать возможность управления (создание/изменение) учётными записями пользователей Системы:

– идентификаторами и аутентификаторами;

– ролями (в том числе для отдельных площадок в иерархии);

– методами аутентификации (локальная база или LDAP-аутентификация).

4.2.3.4.1.4. Компонент управления должен обеспечивать поддержку интеграции с внешними системами аутентификации по протоколу LDAP.

4.2.3.4.1.5. Компонент управления должен обеспечивать возможность генерации пользовательских паролей.

4.2.3.4.1.6. Компонент управления должен обеспечивать возможность блокировки учётной записи.

4.2.3.4.1.7. Компонент управления должен обеспечивать журналирование действий пользователей с:

– активами;

– уязвимостями;

– функциями управления сбором данных;

– функциями управления подсистемой;

– входом/выходом в/из подсистемы.

4.2.3.4.1.8. Компонент управления должен обеспечивать возможность фильтрации журналов регистрации событий по пользователям и их действиям в подсистеме.

4.2.3.4.2. *Функциональные требования к управлению обновлениями*

4.2.3.4.2.1. Компонент управления должен обеспечивать получение обновлений ПО и базы знаний.

4.2.3.4.2.2. Компонент управления должен обеспечивать возможность распространения файлов обновлений ПО на отчуждаемых носителях информации.

4.2.3.4.2.3. Компонент управления должен обеспечивать возможность ручного запуска обновлений ПО и автоматического обновления базы знаний.

4.2.3.4.3. *Функциональные требования к пользовательскому интерфейсу*

4.2.3.4.3.1. Компонент управления должен обеспечивать доступ пользователям для:

– администрирования подсистемы с помощью: веб-интерфейса и/или графического интерфейса и/или интерфейса командной строки;

– выполнения основных функций подсистемы с помощью веб-интерфейса.

4.2.3.4.3.2. Компонент управления должен обеспечивать уведомление о изменения статусов основных системных сущностей (активов, задач сбора данных, состояния системы) с их отправкой на электронную почту или по POST-запросу.

4.2.3.4.3.3. Компонент управления должен обеспечивать уведомление о сбоях в работе сервисов и отображение состояния подсистемы в интерфейсе пользователя.

4.2.3.4.3.4. Компонент управления должен обеспечивать визуализацию и настройку статистических данных о результатах функционирования подсистемы:

– визуализации подлежат оперативные данные об активах, уязвимостях и состоянии работоспособности подсистемы в виде графиков, диаграмм и таблиц, закрепляемых за отдельными виджетами;

– настройка должна обеспечивать:

o возможность создания пользовательских виджетов, с указанием необходимых источников данных и их типов визуализации (график, диаграмма, таблица);

o возможность настройки периодичности обновления виджетов.

4.2.3.4.3.5. Компонент управления должен обеспечивать возможность настройки, построения, отправки и экспорта отчётов, за счёт:

– наличия предустановленных форм отчётов;

– возможности создания пользовательских форм отчётов с помощью конструктора отчётов, позволяющего:

o задать последовательность объектов отчёта (текста, изображений, актуальной информации из виджетов);

o задать тип визуализации данных (диаграммы, графики, гистограммы);

o настроить внешний вид отчёта (колонтитулы, легенду, подписи к объектам отчёта).

– возможность выпуска отчётов вручную или по расписанию, в том числе с отправкой на заданный адрес электронной почти;

– возможность экспорта отчётов в один из следующих форматов: PDF, XLSX.

4.2.4. *Требования к подсистеме многоуровневой защиты от вредоносного контента*

4.2.4.1. *Общие требования*

4.2.4.1.1. При работе с веб-интерфейсом подсистемы все передаваемые данные должны защищаться при помощи HTTPS с использованием SSL-сертификата. SSL-сертификат может быть, как самоподписанным, так и выданным официальным центром сертификации.

4.2.4.1.2. Подсистема должна выполнять ведение базы знаний по загруженным объектам и вердиктам.

4.2.4.1.3. Подсистема должна поддерживать следующие варианты загрузки объектов для анализа:

– анализ файлов, загружаемых вручную пользователями в подсистему, в том числе и анонимно;

– анализ файлов, отправляемых пользователями на выделенный почтовый адрес подсистемы;

– выявление и анализ файлов, прикрепленных к электронным письмам, посредством направления копий писем на подсистему;

– выявление и анализ файлов, передаваемых в Web-трафике посредством интеграции с системами защиты;

– 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).

4.2.4.1.4. 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).

4.2.4.1.5. Подсистема должна иметь возможность блокировки писем электронной почты при интеграции с почтовым сервером Microsoft Exchange.

4.2.4.1.6. Подсистема должна уметь извлекать файлы из архивов, в том числе, защищенных паролем (при его наличии), следующих форматов:

– application/x-rar (RAR);
– application/x-7z-compressed (7z);
– application/zip (ZIP);
– application/x-tar (Tar).

4.2.4.1.7. Подсистема должна распаковывать вложенные архивы до второго уровня.

4.2.4.1.8. Подсистема должна обеспечивать распаковку сжатых файлов следующих форматов:

– .gz (gzip);
– .Z (compress);
– .bz2 (bzip2);
– .lz, .lzma (LZMA);
– .xz (LZMA2);
– Zip;
– Rar;
– Arj;
– 7zip

4.2.4.1.9. Подсистема должна иметь встроенный механизм Anti-Evasion для защиты от техник обхода песочниц.

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

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

4.2.4.2. *Требования к компоненту статического анализа*

4.2.4.2.1. Компонент должен осуществлять предварительную комплексную и многопоточную проверку файлов на наличие ВПО с использованием множественных антивирусных ядер на наборе нескольких антивирусных решений.
4.2.4.2.2. Компонент должен позволять дополнять (при наличии соответствующих лицензий) набор антивирусных движков несколькими решениями.
4.2.4.2.3. Компонент должен проводить статический анализ файлов на наличие ВПО с использованием базы предустановленных разработчиком правил.
4.2.4.2.4. По завершению статического анализа, компонент должен возвращать следующую информацию:

– итоговый вердикт антивирусной проверки (высокая опасность, подозрительный, чистый);
– итоговый результат проверки (обнаружено опасное ПО, обнаружено потенциально опасное ПО, угроз не обнаружено);
– тип вредоносного ПО для каждого из антивирусных решений;
– вердикт каждого из антивирусных решений (опасный, потенциально опасный, угроз не обнаружено), с применением которого проводилось сканирование;
– версию антивирусных решений, с применением которых проводилось сканирование;
– дату обновления антивирусных баз.

4.2.4.3. *Требования к компоненту поведенческого анализа*
4.2.4.3.1. Компонент должен обеспечивать запуск и анализ поведения в изолированной среде файлов следующих форматов:

– PE (исполняемые);
– скрипты (vbs, bat, ps);
– Microsoft Office (rtf, doc/docx, xls/xlsx, ppt/pptx);
– Adobe Acrobat (pdf);
– архивы (rar, 7z, zip, tar).

4.2.4.3.2. Компонент должен поддерживать следующие операционные системы для анализа файлов в изолированной среде:

– Microsoft Windows 7 x64/x86;
– Microsoft Windows 8.1 x64;
– Microsoft Windows 10 x64;
– OS из семейства Linux

4.2.4.3.3. Компонент должен автоматически масштабировать количество виртуальных машин для анализа файлов в зависимости от выделенных ресурсов на этапе развертывания.
4.2.4.3.4. Компонент должен анализировать на основе заданных правил поведения следующие действия:

– создание файлов (артефактов);
– запуск процессов;
– выполнение интернет-запросов;
– изменения в системном реестре.

4.2.4.3.5. По завершению динамического анализа компонент должен возвращать следующую информацию:

– журнал событий в изолированной среде (в исходном и нормализованном виде);
– созданные артефакты;
– копия сетевого трафика;
– видеозапись поведения файла.

4.2.4.3.6. Компонент должен выстраивать граф поведения семплов в изолированной среде после проведения поведенческого анализа и отображать его в графическом интерфейсе.

4.2.4.3.7. Компонент должен выстраивать дерево выпавших в процессе поведенческого анализа артефактов.
4.2.4.3.8. Компонент должен обеспечить передачу артефактов, выпавших в процессе динамического анализа, в подсистему статического анализа для их репутационной и антивирусной проверки.
4.2.4.3.9. Компонент должен собирать дампы памяти процессов при поведенческом анализе и проводить постобработку этих дампов статическим методом анализа с использованием предустановленных разработчиком правил.
4.2.4.3.10. Компонент должен производить видеозапись рабочего стола ОС изолированной среды при запуске исполняемого файла, а также действий, производимых этим файлом.

4.2.4.4. *Требования к компоненту хранения*

4.2.4.4.1. Компонент должен обеспечивать хранение следующих данных:
- проверяемых файлов;
- метаданных проверяемых файлов;
- значений хэш-функций проверяемых файлов;
- даты и времени сканирования;
- информации об антивирусах, которые производили проверку (имя, версию ядра, версию антивирусной базы, результат сканирования).
- артефактов, выпавших из семпла;
- сессионных трасс;
- TCP дампов;
- дампов памяти процессов.

4.2.4.4.2. Компонент должен позволять выполнять следующие действия с отсканированными файлами:
- скачивать;
- просматривать историю сканирований и статистику ретроспективного анализа.

4.2.4.4.3. Компонент должен позволять выполнять поиск файла в хранилище отсканированных файлов.
4.2.4.4.4. Компонент должен обеспечивать возможность ограничения объема и ротации данных в хранилище.

4.2.4.5. *Требования к компоненту управления*

4.2.4.5.1. Компонент должен обеспечивать аутентификацию обслуживающего персонала на основании имени учетной записи и пароля.
4.2.4.5.2. Компонент должен обеспечивать функцию разграничения доступа обслуживающего персонала к настройкам системы.
4.2.4.5.3. Компонент должен обеспечивать возможность автоматического обновления баз антивирусных решений и образов виртуальных машин.
4.2.4.5.4. Компонент должен обеспечивать возможность автоматического обновления программного обеспечения подсистемы.
4.2.4.5.5. Компонент должен обеспечивать возможность добавления, изменения, отключения, удаления источников для сканирования.
4.2.4.5.6. Компонент должен отслеживать состояние всех подсистем, входящих в состав подсистемы.
4.2.4.5.7. Компонент должен информировать о текущем статусе работоспособности подсистемы через веб-интерфейс.
4.2.4.5.8. Компонент должен предоставлять возможность выбора типов файлов, для которых необходимо проводить динамический анализ.
4.2.4.5.9. Компонент должен обеспечивать возможность задания словаря паролей для анализа архивов, защищенных паролем.

4.2.4.5.10. Компонент должен обеспечивать возможность пересылки пользователем заблокированного письма адресату.
4.2.4.5.11. Компонент должен обеспечивать возможность просмотра результатов поведенческого анализа файлов в виде диаграммы.
4.2.4.5.12. Компонент должен обеспечивать возможность просмотра артефактов, созданных при поведенческом анализе файлов.
4.2.4.5.13. Компонент должен обеспечивать возможность просмотра видеозаписи поведения файла в ходе поведенческого анализа.
4.2.4.5.14. Компонент должен обеспечивать возможность сохранения на компьютер пользователя результатов поведенческого анализа файлов:

- журнал событий в изолированной среде (в исходном и нормализованном виде);
- созданные артефакты;
- копия сетевого трафика;

4.2.4.5.15. Компонент должен обеспечивать возможность формирования и копирования ссылки на страницу с результатами проверки файлов.
4.2.4.5.16. Компонент должен обеспечивать возможность вывода на печать результатов проверки файлов.
4.2.4.5.17. Компонент должен обеспечивать возможность скачивать файлы из хранилища.
4.2.4.5.18. Компонент должен помещать любые файлы, скачиваемые пользователем из хранилища просканированных файлов, в ZIP-архивы с паролем infected.
4.2.4.5.19. Компонент должен поддерживать следующие методы сжатия:

- application/gzip (Gzip);
- application/x-compress (Z);
- application/x-bzip2 (Bzip2);
- application/x-xz (XZ).

4.2.4.5.20. Компонент должен обеспечивать возможность просмотра сведений о файле, содержащимся в хранилище.

## 4.3. Требования к видам обеспечения

### 4.3.1. *Требования к техническому обеспечению*

#### 4.3.1.1. *Требования к техническому обеспечению подсистемы мониторинга событий информационной безопасности*

Подсистема мониторинга событий информационной безопасности должна быть реализована на базе одного виртуального или физического сервера, характеристики предоставляются *Исполнителем, в пакете документов на тендер.*
Сервер или вычислительные мощности для него предоставляются *Заказчиком*.

#### 4.3.1.2. *Требования к техническому обеспечению подсистемы анализа сетевого трафика и выявления атак*

Подсистема анализа сетевого трафика и выявления атак должна быть реализована на базе одного виртуального или физического сервера, характеристики предоставляются *Исполнителем, в пакете документов на тендер*.
Сервер или вычислительные мощности для него предоставляются *Заказчиком.*

#### 4.3.1.3. *Требования к техническому обеспечению подсистемы управления уязвимостями*

Подсистема управления уязвимостями должна быть реализована на базе единого аппаратного (или виртуального) сервера с подсистемой мониторинга событий информационной безопасности.

#### 4.3.1.4. *Требования к техническому обеспечению подсистемы многоуровневой защиты от вредоносного контента*

Подсистема многоуровневой защиты от вредоносного контента должна быть реализована на базе одного или нескольких физических серверов, суммарно обеспечивающего характеристики предоставляются *Исполнителем, в пакете документов на тендер.*
Сервер предоставляется *Заказчиком.*

4.3.2. ***Требования к программному обеспечению***

4.3.2.1. *Требования к программному обеспечению подсистемы мониторинга событий информационной безопасности*

Подсистема мониторинга событий информационной безопасности должна быть реализована на базе одного виртуального или физического сервера.
Операционная система сервера –определяется *Исполнителем*.
В случае использования виртуальной инфраструктуры – должна применяться среда виртуализации VMWare.
Работа с графическим интерфейсом пользователя Подсистемы должна осуществляться на автоматизированном рабочем месте (АРМ) пользователя с помощью Web-браузера.
Подсистема должна поддерживать работу пользователя с использованием графического интерфейса через Web-браузеры:

- Google Chrome версии 49 или выше;
- Mozilla Firefox версии 45 или выше.

Операционная система и среда виртуализации предоставляется *Заказчиком*.

4.3.2.2. *Требования к программному обеспечению подсистемы анализа сетевого трафика и выявления атак*

Подсистема анализа сетевого трафика и выявления атак должна быть реализована на базе одного виртуального или физического сервера.
Операционная система сервера – определяется *Исполнителем*.
В случае использования виртуальной инфраструктуры – должна применяться среда виртуализации VMWare.
Работа с графическим интерфейсом пользователя Подсистемы должна осуществляться на автоматизированном рабочем месте (АРМ) пользователя с помощью Web-браузера.
Подсистема должна поддерживать работу пользователя с использованием графического интерфейса через Web-браузеры:

- Google Chrome версии 49 или выше;
- Mozilla Firefox версии 45 или выше.

Операционная система и среда виртуализации предоставляется *Заказчиком*.

4.3.2.3. *Требования к программному обеспечению подсистемы управления уязвимостями*

Подсистема управления уязвимостями должна быть реализована на базе единого аппаратного (или виртуального) сервера с подсистемой мониторинга событий информационной безопасности.

4.3.2.4. *Требования к программному обеспечению подсистемы многоуровневой защиты от вредоносного контента*

Подсистема многоуровневой защиты от вредоносного контента должна быть реализована на базе одного или нескольких физических серверов.
Подсистема должна функционировать под управлением операционной системы Linux Server.
Работа с графическим интерфейсом пользователя Подсистемы должна осуществляться на автоматизированном рабочем месте (АРМ) пользователя с помощью Web-браузера.
Подсистема должна поддерживать работу пользователя с использованием графического интерфейса через Web-браузеры:

- Google Chrome версии 49 или выше;
- Mozilla Firefox версии 45 или выше.

Операционная система предоставляется *Заказчиком*.

## 4.4. Общие технические требования к Системе

4.4.1. *Требования к показателям назначения*

Система должна обеспечивать следующие показатели назначения:

– Поддержка мониторинга и выявления уязвимостей для ИТ-активов не менее чем - 1500 шт.;

– Срок хранения событий – не менее 30 дней;

– Анализ сетевого трафика и выявление атак в каналах передачи данных с пропускной способностью не менее, чем 100Мбит/с;

– архивное хранение копий исходного сетевого трафика для расследования инцидентов до 5 суток;

– хранение результатов обработки сетевого трафика до 7 суток;

– обеспечение поведенческого анализа не менее, чем для 1300 почтовых ящиков пользователей;

– обеспечение статического и динамического анализа для выявления вредоносных объектов не менее, чем для одного файлового хранилища;

– срок хранения артефактов – не менее 30 дней;

– количество образов виртуальных машин для поведенческого анализа – не менее 4;

– гарантийные обязательства не менее, чем в течение 1 года с момента покупки.

4.4.2. *Требования к защите информации от несанкционированного доступа*

4.4.2.1. В Системе должны быть реализованы следующие встроенные меры по защите информации от несанкционированного доступа:

- идентификация, авторизация и аутентификация пользователей Системы;
- разграничение доступа к функциям Системы на основе ролей;
- регистрация действий пользователей Системы.

4.4.2.2. Безопасность Системы должна обеспечиваться в соответствии с мерами защиты, определёнными для информационных систем Заказчика.

4.4.2.3. Меры защиты Системы должны реализовываться встроенными и (или) наложенными средствами (механизмами).

4.4.3. *Требования к обеспечению регистрации событий безопасности*

4.4.3.1. Средства Системы должны предусматривать возможность регистрации и хранения событий взаимодействия пользователей со средствами Системы.

4.4.3.2. Средства Системы должны предоставлять возможности чтения записанных событий в человекочитаемом формате.

4.4.4. *Требования по сохранности информации при авариях*

4.4.4.1. Система должна обеспечивать сохранность конфигурационных файлов и данных в случаях аварийных ситуаций либо несанкционированных воздействий на элементы Системы.

4.4.5. *Требования к патентной чистоте*

4.4.5.1. Все компоненты Системы должны иметь действующие лицензии от производителей ПО.

# 5. Состав и содержание работ по созданию Системы

Состав и содержание работ приведены ниже в ***таблице 1***.

**Таблица 1 — Состав и содержание работ**

| Наименование стадии | Наименование этапа | Состав и результаты выполнения работ | Организация исполнитель |
|---|---|---|---|
| Ввод в действие | Подготовка объекта защиты к вводу Системы в действие | Разработка документа:<br>- план подготовки объекта к вводу Системы в действие | Заказчик, Подрядная организация |
| | Комплектация Системы поставляемыми изделиями | Поставка, по результатам подготавливается:<br>- акт приёма-передачи оборудования и программного обеспечения | Подрядная организация |
| | Подготовка персонала | Обучение персонала Системы | Заказчик, Подрядная организация |
| | Пусконаладочные работы | Установка и настройка программно-аппаратного комплекса (ПАК) Системы, по результатам подготавливается:<br>- акт выполнения пусконаладочных работ. | Подрядная организация |
| | Проведение предварительных испытаний | Проведение предварительных испытаний, по результатам подготавливается:<br>- программа и методика предварительных испытаний;<br>- протокол предварительных испытаний;<br>- акт приема Системы в опытную эксплуатацию;<br>- акт устранения замечаний и неисправностей (при необходимости). | Заказчик, Подрядная организация |
| | Проведение опытной эксплуатации | Проведение опытной эксплуатации, по результатам подготавливается:<br>- рабочий журнал опытной эксплуатации;<br>- акт о завершении опытной эксплуатации;<br>- акт устранения замечаний и неисправностей (при необходимости). | Заказчик, Подрядная организация |
| | Проведение приемочных испытаний | Проведение приёмочных испытаний, по результатам подготавливается:<br>- программа и методика приёмочных испытаний;<br>- протокол приемочных испытаний;<br>- акт устранения замечаний и неисправностей (при необходимости)<br>- акт приема Системы в постоянную эксплуатацию. | Заказчик, Подрядная организация |
| Сопровождение Системы | Гарантийное и послегарантийное обслуживание | — | Подрядная организация |

# 6. Требования к проведению работ

## 6.1. Общие требования к контролю и приёмке Системы

Испытания Системы проводятся для определения её соответствия требованиям настоящего ТЗ, оценки полноты и качества реализации функций Системы, выявления и устранения недостатков в функционировании Системы.

Для проведения проверки выполнения заданных функций и приёмки Системы в постоянную эксплуатацию должны быть осуществлены:

– предварительные испытания Системы на работоспособность и соответствие ТЗ;

– опытная эксплуатация Системы в комплексе со смежными системами в целях проверки их совместимости и работоспособности Системы в составе ИТ-инфраструктуры Заказчика;

– приёмочные испытания Системы по результатам опытной эксплуатации с последующей передачей Системы в постоянную эксплуатацию.

## 6.2. Предварительные испытания

Предварительные испытания проверяют реализацию функций Системы и работоспособность в целом. Предварительные испытания Системы проводятся в соответствии с программой и методикой предварительных испытаний. Программа и методика испытаний разрабатывается *Исполнителем* и согласовывается с *Заказчиком*.

В состав комиссии по проведению испытаний должны входить представители Заказчика и Исполнителя. Результаты отражаются в протоколе предварительных испытаний.

По результатам предварительных испытаний должно быть принято решение о работоспособности Системы и возможности приёмки в опытную эксплуатацию, а также сформирован перечень необходимых доработок с указанием сроков их выполнения. Решение оформляется актом приёмки в опытную эксплуатацию с указанием сроков проведения опытной эксплуатации.

## 6.3. Опытная эксплуатация

На этапе опытной эксплуатации должны быть определены готовность персонала к работе с Системой и при необходимости скорректированы основные процедуры и документация. Во время опытной эксплуатации ведётся рабочий журнал, в который заносятся сведения о продолжительности функционирования Системы, отказах, сбоях, затруднениях в работе. В опытной эксплуатации участвуют представители Заказчика и Исполнителя, которые имитируют реальную работу Системы в условиях постоянной эксплуатации.

По результатам опытной эксплуатации оформляется акт о завершении опытной эксплуатации, которым определяется возможность допуска Системы к приёмочным испытаниям.

## 6.4. Приёмочные испытания

На этапе приёмочных испытаний должна быть выполнена оценка результатов опытной эксплуатации, и принято решение о приёмке Системы в постоянную эксплуатацию. Приёмочные испытания Системы проводятся в соответствии с программой и методикой приёмочных испытаний. Программа и методика испытаний *разрабатывается Исполнителем* и *согласовывается с Заказчиком*.

В состав комиссии по проведению испытаний должны входить представители *Заказчика* и *Исполнителя*. Результаты отражаются в протоколе приёмочных испытаний.

По результатам приёмочных испытаний должно быть принято решение о соответствии Системы требованиям ТЗ и возможности приёмки в постоянную эксплуатацию, а также сформирован перечень выявленных недостатков с указанием сроков их устранения. Решение оформляется актом приёмки в постоянную эксплуатацию.

# 7. Требования к составу и содержанию работ по подготовке объектов автоматизации к вводу Системы в действие

При подготовке объектов Заказчика к вводу Системы в действие должны быть выполнены следующие работы:

- настройка оборудования гарантированного электропитания;
- настройка оборудования для обеспечения сетевой доступности ПАК Системы;
- настройка оборудования фильтрации;
- настройка оборудования зеркалирования трафика;
- создание учетных записей, используемых Системой.

Заказчик должен предоставить техническое обеспечение, необходимое для размещения ПАК Системы.

Заказчик должен обеспечить сетевое взаимодействие ПАК Системы с использованием сети передачи данных.

Работы по подготовке объекта автоматизации к вводу Системы в действие выполняются специалистами Заказчика.