# Требования Н2 – реализация средствами ОПО и СПО

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Требование ТЗ | СПО/ОПО | Предложения по реализации, выбор ПО для реализации СПО |
| 1. | 3.2.3.1 Строгую идентификацию и аутентификацию субъектов и объектов доступа. | СПО аутентификации и управления пользователями |  |
| 2. | 3.2.3.2 Журналирование событий и действий всех субъектов доступа. |  | Журналирование обеспечивается средствами ОС.  Необходимо будет сделать настройки журналирования, устраивающие Заказчика.  Сбор журналов - OSSEC |
| 3. | 3.2.3.3 Возможность взаимодействия с сетевыми сегментами Заказчика, в т.ч. с использованием КОП. |  |  |
| 4. | 3.2.3.4 Накопление данных ОО ПТК «Н-2» и организацию обмена данными с виртуальными компьютерами Заказчика с использованием файловых серверов во внешнем и внутреннем контурах виртуализации. |  | FTP сервер в среде виртуализации.  Обеспечивается средствами ОС.  FTP клиент – FileZilla  Bigs |
| 5. | 3.2.3.5 Ролевое разграничение доступа на файловых серверах внешнего и внутреннего контуров виртуализации. | СПО аутентификации и управления пользователями |  |
| 6. | 3.2.3.6 Автоматическое создание телекоммуникационных сегментов специального назначения с использованием программно-технических средств ОО ПТК «Н-2», для проведения анализа разрабатываемых СпПС. | СПО создания и обновления образов  СПО ведения узлов сети. | Развертывание виртуальных сетей в среде виртуализации. Управление виртуальными машинами.  VirtualBOX + Vagrant  Xen/KVM + ConVirt |
| 7. | 3.2.3.7 Возможность совместной разработки программного кода с использованием систем контроля версий (Git), систем непрерывной интеграции (Jenkins), систем управления проектами (Redmine), сред разработки (IDEA, Eclipse, Visual Studio). | СПО анализа СпПС | Git, Jenkins, Redmine, IDEA, Eclipse, Visual Studio,  Дизассемблер IDA Pro  Необходимо уточнить по поводу платного ПО. |
| 8. | 3.2.3.8 Возможность администрирования собственной сетевой и вычислительной инфраструктуры. | ?????? |  |
| 9. | 3.2.3.9 Безопасность процесса обработки технологической информации о функционировании разрабатываемых СпПС. | ?????? |  |
| 10. | 3.2.3.10 Возможность проведения автоматизированного анализа разрабатываемых средств СпПС. | СПО анализа СпПС | Дизассемблер IDA Pro  ?????? |
| 11. | 3.2.3.11 Возможность проведения анализа обрабатываемой технологической информации о функционировании разрабатываемых СпПС. | СПО анализа СпПС | Дизассемблер IDA Pro  ?????? |
| 12. | 3.2.3.12 Возможность установки АВС на сервера и АРМ разработки с обеспечением корректной совместной работы СПО и АВС. | АВС Касперский  АВС Dr.Web |  |
| 13. | 3.2.3.13 Обновление ОПО через сетевые сегменты Заказчика, подключение к ОО ПТК «Н-2». | СПО взаимодействия с ИВС | ?????? |
| 14. | 3.2.3.14 Возможность взаимодействия с виртуальными компьютерами Заказчика на основе платформы RabbitMQ. |  | RabbitMQ – управление очередью сообщений.  Не понятна суть взаимодействия виртуалок через RabbiMQ.  Передача информации между подкомплексами из региона в центр |
| 15. | 3.2.3.15 Обнаружение вторжений уровня компьютеров на основе системы OSSEC. | СПО выявления аномалий сетевых взаимодействий | OSSEC  Анализ ПО, которое в песочнице |
| 16. | 3.2.3.16 Обнаружение вторжений уровня сетей на основе системы Suricata. | СПО выявления аномалий сетевых взаимодействий | Suricata  Должна стоять на виртуальных сетевых интерфейсах, на которых проводится исследование. |
| 17. | 3.2.3.17 Мониторинг событий на основе системы Zabbix. |  |  |
| 18. | 3.2.3.18 Создание и обновление образов программного обеспечения. | СПО создания и обновления образов |  |
| 18.1 | 3.2.3.18.1 Создание образов ОС с установленными приложениями в виде загрузочного носителя | СПО создания и обновления образов | Создание образов ОС Clonezilla Server |
| 18.2 | 3.2.3.18.2 Создание локального репозитария пакетов ОПО и баз АВС во внешнем контуре виртуализации. | СПО создания и обновления образов | Облако касперского и Dr.WEB.  Сервер обновлений - Spacewalk |
| 18.3 | 3.2.3.18.3 Ведение шаблонов виртуальных компьютеров с заданным набором сервисов, в т.ч. настройки параметров (размеров дискового пространства, ОЗУ, количества ядер). | СПО создания и обновления образов | Средство управления виртуальными машинами  VirtualBOX + Vagrant |
| 18.4 | 3.2.3.18.4 Перенос образов ОС, обновлений пакетов ОПО, баз АВС и шаблонов виртуальных компьютеров в системный репозитарий внутреннего контура виртуализации. | СПО создания и обновления образов |  |
| 18.5 | 3.2.3.18.5 Использование образов ОС из системного репозитария внутреннего контура для создания загрузочных носителей. | СПО создания и обновления образов |  |
| 18.6 | 3.2.3.18.6 Обновление ОПО внутреннего контура виртуализации с использованием пакетов системного репозитария внутреннего контура виртуализации. | СПО создания и обновления образов |  |
| 18.7 | 3.2.3.18.7 Редактирование параметров шаблонов виртуальных компьютеров. | СПО создания и обновления образов | Средство управления виртуальными машинами  VirtualBOX + Vagrant |
| 18.8 | 3.2.3.18.8 Использование шаблонов виртуальных компьютеров из системного репозитария внутреннего контура для установки на аппаратные средства. | СПО создания и обновления образов | Средство управления виртуальными машинами  VirtualBOX + Vagrant |
| 19. | 3.2.3.19 Защищенное соединение между узлами сетевой инфраструктуры. | СПО защищенного соединения | OpenVPN Server + OpenVPN Client  ПО Аладдин - JaCarta ГОСТ для Linux |
| 20. | 3.2.3.20 Ведение узлов специальной транспортной инфраструктуры.  - реестр узлов  - доступность, расположение, пропускная способность узлов  - мониторинг состояния узлов | СПО ведения узлов сети | Реестр внешних узлов для доставки ПО в точку к потребителю  Remmina  Реализация интерфейса для утилит командной строки telnet, ping, ssh, tracert |
| 21. | 3.2.3.21 Резервное копирование данных.  - автоматизированное создание резервных копий по расписанию.  - создание резервных копий разных уровней: полное, дифференциальное, инкрементное и консолидация.  - разбиение резервной копии на тома с возможностью распределенного хранения томов. | СПО резервного копирования | Резервная копия ОС Clonezilla Server  Резервное копирование папок файловой системы Rsync  Резервное копирование виртуальных машин функция Snapshot для Virtualbox |
| 22. | 3.2.3.22 Взаимодействия с ИВС.  - перенаправление портов  - изменение IP  - модификация сетевого трафика | СПО взаимодействия с ИВС | Выбор ПО для NAT  IPTables + визуальный клиент |
| 23. | 3.2.3.23 Обмен сообщениями электронной почты. | СПО обмена электронной почтой | E-mail сервер + клиенты  Сервер - hMail  Клиент Thunderbird |
| 24. | 3.2.3.24 Передачу текстовых сообщений и файлов между пользователями в режиме реального времени и в режиме отложенной передачи. | СПО мгновенного обмена сообщениями | Сервер OpenFire  Клиент Ignite Realtime Spark, Pidgin |
| 25. | 3.2.3.25 Анализ электронных журналов событий аудита информационной безопасности. | СПО анализа электронных журналов событий аудита информационной безопасности | OSSEC, Zabbix |
| 26. | 3.2.3.26 Выявление аномалий сетевых взаимодействий. | СПО выявления аномалий сетевых взаимодействий | Wireshark, tcpdump  Отчет кварц |
| 27. | 3.2.3.27 Контроль целостности программного кода.  - контроль целостности ОС  - контроль целостности ОПО\СПО (файлы)  - контроль целостности BIOS | СПО контроля целостности | OSSEC HIDS анализ логов, контроль целостности для Linux, Mac, Windows  Open Source Tripwire мониторинг целостности файловых систем.  Контроль целостности BIOS??? |
| 28. | 3.2.3.28 Анализ СпПС. | СПО анализа СпПС |  |
| 28.1 | 3.2.3.28.1 Дизассемблирование кода СпПС. | СПО анализа СпПС | Дизассемблер IDA Pro |
| 28.2 | 3.2.3.28.2 Удаленную отладку кода СпПС на различных платформах. | СПО анализа СпПС |  |
| 28.3 | 3.2.3.28.3 Декомпилирование кода СпПС. | СПО анализа СпПС | Дизассемблер IDA Pro |
| 28.4 | 3.2.3.28.4 Анализ трафика СпПС. | СПО анализа СпПС | wireshark, tcpdump |
| 28.5 | 3.2.3.28.5 Возможность применения облачных антивирусных технологий для выявления СпПС. | СПО анализа СпПС |  |
| 28.6 | 3.2.3.28.6 Автоматическую классификацию СпПС на основе их характеристик. | СПО анализа СпПС |  |
| 28.7 | 3.2.3.28.7 Автоматизированное создание защищенной среды исполнения кода СпПС. | СПО анализа СпПС |  |
| 28.8 | 3.2.3.28.8 Ведение реестра СпПС. | СПО анализа СпПС | Git + Bitbucket, Github |
| 28.9 | 3.2.3.28.9 Предоставление программного интерфейса для создания расширений (плагинов) специального анализа кода СпПС. | СПО анализа СпПС |  |
| 28.10 | 3.2.3.28.10 Автоматическое выявление характеристик СпПС (в т.ч. процессы, файлы, ключи реестра, URL, IP-адреса, EMAIL-адреса, DNS-имена, признаки сетевого трафика, признаки программного кода, признаки обрабатываемых данных). | СПО анализа СпПС | Средство сравнения до и после установки ПО  Аналог Install Monitor |
| 29. | 3.2.3.29 Аутентификацию и управление правами пользователей. | СПО аутентификации и управления пользователями | FreeIPA |
| 29.1 | 3.2.3.29.1 Ведение учетных записей пользователей и дополнительных атрибутов. | СПО аутентификации и управления пользователями | LDAP - 389 Directory Server |
| 29.2 | 3.2.3.29.2 Однократную аутентификацию пользователей в различных сегментах и сервисах ОО ПТК «Н-2». | СПО аутентификации и управления пользователями | MIT’s Kerberos 5 |
| 29.3 | 3.2.3.29.3 Ведение прав пользователей на доступ к узлам специальной транспортной инфраструктуры (сегменты, серверы, протоколы, операции установки и удаления ПО) с использованием ролей. | СПО аутентификации и управления пользователями | LDAP - 389 Directory Server |
| 29.4 | 3.2.3.29.4 Контроль параметров оборудования АРМ разработчика (сведения о подключенном USB-токене, контрольная сумма загрузочного образа ОС, сведения об аппаратных компонентах АРМ) при аутентификации в ОО ПТК «Н-2». | СПО аутентификации и управления пользователями | DogTag |
| 29.5 | 3.2.3.29.5 Реализацию технологии единого входа для связок GlassFish-Java-Oracle, Apache-PHP-Postgresql, IIS-.NET-MSSQL. | СПО аутентификации и управления пользователями | MIT’s Kerberos 5 |
| 30. | 3.2.3.30 Контролируемый вывод документов на печать и файлов на МНИ. | СПО печати и вывода данных на МНИ | Прикладная разработка |
| 31. | 3.2.3.31 Информационный обмен между пользователями, СПО ОО ПТК «Н-2» и виртуальными компьютерами Заказчика. | СПО информационного обмена | Прикладная разработка |
| 32. | 3.2.3.32 Распределенное индексирование данных. | СПО распределенного индексирования данных | Прикладная разработка |
| 33. | 3.2.3.33 Поиска данных. | СПО поиска данных | Прикладная разработка |