ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ (ТЕХНИЧЕСКОЕ ЗАДАНИЕ) ПО ВНЕДРЕНИЮ СИСТЕМЫ АНАЛИЛА ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ КОМПАНИИ

## **Общие требования к функциям системы**

### 1.1. Комплексная система защиты (далее - Система) должна позволять получать объективную оценку состояния защищенности как всей информационной системы, так и отдельных подразделений, узлов и приложений. Иметь механизмы тестирования на проникновение, с поддержкой анализа различных операционных систем, коммуникационного оборудования, СУБД и Web-приложений

### 1.2. Функциональные компоненты Системы должны поддерживать развертывание как на физическом, так и на виртуальном оборудовании.

### 1.3. Система не должна требовать установки программного агента на ИС. Для сканирования ИС должны использоваться встроенные механизмы удаленного доступа, такие как WMI, SSH и Telnet.

### 1.4. Интерфейс Системы должен быть выполнен на русском языке. Отчеты, формируемые системой, должны также выводиться на русском языке.

### 1.5. Система должна иметь открытый API-интерфейс для интеграции со сторонними системами с использованием языка XML:

* с системами управления заявками (Service Desk, Help Desk);
* с системой управления событиями информационной безопасности (SIEM) и системой управления рисками (Risk management);
* со службой каталогов Microsoft Active Directory.

1.6. В комплект Системы должны входить следующие программные продукты:

- система тестирования защищенности;

## **Требования к архитектуре системы тестирования защищенности.**

## В состав системы тестирования защищенности должны входить:

* серверные модули;
* консоль управления (клиентская часть).

## Серверный модуль должен обеспечивать управление специализированными сетевыми сканерами, сбор данных, их обработку, сохранение в БД и выпуск отчетов.

## Консоль управления должна предоставлять графический интерфейс для администраторов, операторов и пользователей комплекса с учетом назначенных ролей.

## Система должна обеспечивать хранение результатов сканирования для дальнейшего анализа и отслеживать изменения в контролируемой системе путем сравнения текущего состояния узла с данными журналов и эталонными результатами.

## Система должна поддерживать тестирование защищенности не менее 100 узлов.

## Система должна состоять из следующих подсистем:

* контроля защищенности;
* обновления;
* управления.

## **Требования** **к подсистеме контроля защищенности**

### 2.6.1. Подсистема контроля защищенности должна обеспечивать выполнение следующих основных функций:

* идентификацию узлов, инвентаризацию аппаратного и программного обеспечения;
* выявление уязвимостей и ошибок конфигурирования с предоставлением краткого описания и методов устранения;
* сбор сведений о конфигурационных параметрах операционных систем, служб, СУБД, прикладных систем и средств защиты информации (перечень наименований и версий приведен в Таблица 1);
* сканирование компонентов ИС в области поиска, заданной пользователем по IP-адресам, NetBIOS- и DNS-именам.

Таблица 1. Перечень анализируемого программного обеспечения[[1]](#footnote-1)

| **Наименование** | **Версии** |
| --- | --- |
| **Операционные системы семейства Microsoft Windows** | |
| Microsoft Windows | 2000 Professional |
| Microsoft Windows | XP Professional |
| Microsoft Windows | Vista |
| Microsoft Windows | 7 |
| Microsoft Windows | 8 |
| Microsoft Windows | 8.1 |
| Microsoft Windows | 10 |
| Microsoft Windows | 2003 Server |
| Microsoft Windows | 2008 Server |
| Microsoft Windows | 2008 R2 Server |
| Microsoft Windows | 2012 Server |
| Microsoft Windows | 2012 R2 Server |
| Microsoft Windows | 2016 Server |
| Microsoft Windows | 2019 Server |
| **Операционные системы семейства Unix и GNU/Linux** | |
| Oracle Solaris | 9, 10, 11 |
| HP-UX | 11.31 |
| CentOS | 5-7 |
| RedHat Linux | 5-8 |
| SUSE Enterprise Server | 10-12, 15 |
| Ubuntu | 10.04-18.04 |
| **Операционные системы телекоммуникационного оборудования** | |
| Cisco IOS | 12.х-15х |
| Juniper JunOS | 3.x—16.x |
| Cisco Nexus | 4.x—9.x |
| Fortinet FortiOS | 4.3.x—4.3.20 |
| **Службы ОС Microsoft, СУБД и прикладных систем** | |
| Microsoft Internet Information Services | 5-10  Windows 2008 Server  Windows 2008 R2 Server |
| Microsoft Sharepoint Server | 2003, 2007, 2010, 2013, 2016 |
| Microsoft Exchange Server | 2003, 2007, 2010, 2013, 2016 |
| Microsoft Office | 2003, 2007, 2010, 2013, 2016 |
| Microsoft SQL Server | 2000,2005,2008R2,2012, 2014,2016,2017 |
| Oracle DB | 8.1, 9.0, 9.2, 10.0, 10.1, 10.2, 11.1, 11.2, 12.1, 12.2 |
| SAP R/3 | 4.6B, 4.6C, 4.6D |
| SAP NetWeaver ABAP | 6.4 и выше |
| SAP NetWeaver JAVA | 7.0 и выше |
| **Средства защиты информации** | |
| Cisco PIX | 4.0—8.2.x |
| Cisco ASA | 6.x—9.9 |
| Cisco IPS | 4.0—7.4 |
| CSP VPN Gate (C-Терра) | 3.1 |
| Checkpoint Firewall (для платформы Checkpoint SecurePlatform) | R7.0 |
| Checkpoint Security Management (для платформы Checkpoint SecurePlatform) | R7.0 |
| InfoTeCS ViPNet Custom | 3.6.0-1412, 4.2.0-1286 |

### 2.6.2. В подсистеме контроля защищенности должны быть реализованы следующие механизмы:

* сетевого сканирования;
* системного сканирования.

### 2.6.3. Механизм сетевого сканирования:

* должен обеспечить идентификацию сетевых служб, использующих TCP или UDP в качестве протокола транспортного уровня;
* должен идентифицировать уязвимости сетевых служб, описанные в базе данных Common Vulnerabilities and Exposures, и обеспечивать оценку степени риска на основе правил Common Vulnerability Scoring System version 2;
* при сканировании веб-приложений должен использовать эвристические методы анализа, позволяющие обнаруживать уязвимости в соответствии с таксономиями Web Application Security Consortium Threat Classification version 2 и Open Web Application Security Project TOP 10.
* должен поддерживать подбор паролей для протоколов электронной почты (SMTP, POP3), служб передачи файлов (SMB, FTP, HTTP), протоколов удаленного управления (Telnet, SNMP, SSH, VNC) и баз данных (Microsoft SQL, Oracle, SAP, SAP DIAG);
* должен осуществлять идентификацию наименований и версий ОС семейства Microsoft Windows;

2.8. **Требования к подсистеме обновления**

2.8.1. Подсистема обновления должна получать обновления с глобального сервера обновления через сеть Интернет или автономно с использованием внешнего накопителя.

2.8.2. Подсистема обновления должна обеспечивать возможность хранения полученных обновлений.

2.8.3. Подсистема обновления должна осуществлять оповещение компонентов системы контроля (анализа) защищенности информации о доступности новых обновлений и предоставлять возможность получения обновлений.

2.9. **Требования к подсистеме управления**

### 2.9.1. Подсистема управления должна позволять:

* задавать параметры сканирования;
* запускать сканирование, в том числе по заданному расписанию и с учетом запрещенных интервалов;
* просматривать результаты сканирования;
* формировать справочники запрещенного и разрешенного к установке ПО, паролей, идентификаторов внешних устройств, которым разрешено подключение, и т. п.;
* формировать шаблоны, задающие параметры генерации отчетов;
* генерировать отчеты по заданному шаблону, в том числе — автоматически, после завершения сканирования, запущенного по расписанию;
* отправлять отчеты уполномоченным сотрудникам, в том числе — автоматически, после завершения сканирования, запущенного по расписанию;
* сравнивать текущее состояние узла с данными журналов и эталонными результатами;
* формировать отчеты о результатах сканирования на русском языке.

### 2.9.2. Подсистема управления должна поддерживать следующие шаблоны отчетов:

* отчет об уязвимостях;
* дифференциальный отчет;
* сравнительный аналитический отчет;
* динамический аналитический отчет;

### 2.9.3. Подсистема должна идентифицировать пользователя по индивидуальному идентификатору:

* при запуске графического интерфейса;
* при запуске операции по сканированию указанного пользователем компонента ИС;
* при формировании шаблонов по настройке программного обеспечения;
* при изменении требований, соответствие которым оценивается в ходе системного сканирования.

### 2.9.4. Подсистема должна проверять подлинность пользователя при запуске пользовательского интерфейса.

### 2.9.5. Подсистема должна регистрировать следующие события:

* вход пользователя в интерфейс пользователя и выход из интерфейса пользователя;
* запуск и прерывание операций по сканированию компонентов ИС.

**5. Требования к сертификации ПО**

5.1. Комплексная система защиты и должна быть сертифицирована на соответствие требованиям по безопасности информации в установленном порядке.

5.2. Комплексная система защиты должна соответствовать требованиям СТ РК ГОСТ Р ИСО/МЭК 15408-3-2006. Оценочный уровень доверия 4.

**6. Требования к потенциальному поставщику**

6.1. В целях исключения возможности приобретения контрафактного программного обеспечения, потенциальный поставщик должен предоставить авторизационное письмо на право поставки от производителя предлагаемого программного обеспечения.

6.2. Поставщик должен иметь подтвержденную техническую квалификацию своих специалистов по поставляемому продукту уровня не ниже Certified Specialist (CS) по каждому поставляемому программному продукту.

6.3. Поставщик должен предоставить гарантию от производителей сроком не менее одного года.

6.4. В течение гарантийного срока все затраты (в т. ч. транспортные, таможенные расходы) по устранению неисправности несет Поставщик.

6.5. Техническая поддержка со стороны Поставщика в рамках гарантийных обязательств должна обеспечивать условия 8\*5\*NBD сроком на один год, удаленную диагностику, замену, консультационную поддержку по телефону.

6.6. Поставщик должен предоставить на все устанавливаемое программное обеспечение сертификаты соответствия, действующие на территории РК.

1. Перечень может быть расширен. [↑](#footnote-ref-1)