
ОПЕРЕЖАЯ УГРОЗУ
RedCheck
Оценка соответствия
Контроль защищенности
Комплексное решение для мониторинга
защищенности IT-инфраструктуры предприятия
ALTEX
SOFT
www.altx-soft.ru

Информационные системы всё глубже проникают в нашу жизнь, мы все больше стали доверять им то, что имеет для нас значительную ценность: персональные данные, финансы и многое другое. На чем же основывается это доверие? На том, что разработчики уверяют нас, что их программы совершенны, что администраторы безопасности имеют должную квалификацию, а операторы информационных ресурсов не жалеют средств на закупку современных средств защиты?

Какова бы ни была квалификация сотрудников безопасности, человеческие возможности уже не позволяют самостоятельно обрабатывать массивы информации, связанной с безопасностью эксплуатируемых ими систем. Большие бюджеты, выделяемые на создание систем защиты, ещё не являются залогом безопасности. А использование таких привычных для пользователя средств как межсетевые экраны, антивирусы и IDS не устранит проблему полностью. Сегодня для эффективного противодействия существующим угрозам на передний план выходят автоматизированные средства, способные в реальном времени контролировать защищенность информационных систем и оперативно вырабатывать решения по устранению выявленных проблем и уязвимостей.

В современном мире информационных технологий средства анализа защищенности стали основным инструментом, позволяющим выявлять уязвимости систем, проверять настройки безопасности, выполнять оценку соответствия, осуществлять контроль целостности программ и данных. Кроме того, средства анализа защищенности представляют собой «энциклопедии» знаний в области информационной безопасности. Помимо сведений об уязвимостях и слабостях систем они содержат широкий спектр рекомендаций по их устранению, лучшие мировые практики соответствия политикам и стандартам безопасности и многое другое.

Средства анализа защищенности позволяют комплексно взглянуть на задачу обеспечения безопасности информационных активов и решать проблемы превентивными методами, предотвращая возможные атаки и каналы утечки информации до их реализации злоумышленниками.

RedCheck – современное средство анализа защищенности (сканер безопасности), позволяющее выявлять уязвимости операционных систем и приложений, потенциально опасные настройки, осуществлять оценку соответствия требованиям политик и стандартов, проводить инвентаризацию оборудования и программ, формировать детальные отчеты.

RedCheck - флагманский продукт компании **АЛТЭКС-СОФТ**, вобравший в себя многолетний опыт наших экспертов и передовые технологии SCAP. Сканер разработан с учетом потребностей отечественных компаний в области информационной безопасности и требований Российских регуляторов. Применение **RedCheck** позволяет решать широкий спектр задач: от поиска уязвимостей до оценки соответствия отечественным и международным стандартам безопасности, а также реализовать ряд мер, обязательных для информационных систем персональных данных (ИСПДн), государственных информационных систем (ГИС) и автоматизированных систем, обрабатывающих конфиденциальную информацию.

Создание сканера безопасности заняло чуть больше года, что по современным меркам считается довольно небольшим сроком для серьёзных законченных проектов корпоративного уровня. Это стало возможным благодаря использованию технологий, отработанных на десятках тысяч инсталляций Программ настройки и контроля семейства «Check», а также накопленному опыту формирования контента безопасности, аккумулированного в нашем репозитории OVALdb.

Сканер безопасности **RedCheck** постоянно совершенствуется, а база уязвимостей ежедневно актуализируется и регулярно пополняется новыми продуктами и платформами. Сегодня в базе **RedCheck** содержатся описания более 30 000 различных уязвимостей, критических обновлений ПО и смежного контента безопасности.

Отличительными особенностями сканера **RedCheck** являются простота в использовании, достоверность и «прозрачность» проверок, адаптивность, а так же сравнительно низкая стоимость.

> “RedCheck – мощное решение корпоративного уровня для автоматизации мониторинга защищенности по разумной цене.”

Средства анализа защищенности - эффективный иструмент управления безопасностью

Содержит ли установленное программное обеспечение уязвимости?

Насколько адекватна конфигурация системы актуальным угрозам?

Соответствует ли она принятым политикам и международным стандартам?

Выполнены ли требования Регуляторов?

И это далеко не все вопросы, на которые должен отвечать не только специалист ИБ, но и любой системный администратор. Для получения необходимой информации существуют в основном два подхода, имеющие свои плюсы и минусы.

1. Внешний аудит

Для того, чтобы получить ответы, организации справедливо заказывают аудит безопасности систем в сторонних специализированных компаниях. При этом бытует стереотип, нередко формируемый самими экспертами, в котором внешний аудит представляется продуктом деятельности неких хакеров-пентестеров, обладающих сакральными знаниями, неведомыми рядовому специалисту ИБ. Отчасти это так. Но в основном это всего лишь хорошо информированные специалисты, обладающие необходимым инструментарием и соответствующим опытом. Важно понимать, что заплатив немалые средства, Вы получаете разовую оценку состояния безопасности на определенный срез времени, и то, что сегодня были приняты меры по предотвращению уязвимостей совсем не гарантирует безопасность завтра.

2. Внутренний аудит с применением САЗ

В отличие от внешнего аудита, внутренний аудит представляет собой непрерывный процесс, реализуемый средствами организации. Сканеры безопасности (средства анализа защищенности) — мощные инструменты способные значительно упростить и автоматизировать этот процесс, решая при этом широкий спектр задач: идентифицировать и ранжировать уязвимости, осуществлять инвентаризацию программного и аппаратного обеспечения, давать объективную оценку соответствия политикам безопасности, контролировать целостность, документировать состояние систем и предлагать меры по повышению их безопасности. Современные сканеры сконцентрировали опыт и знание тысяч различных экспертов всего мира, банки знаний об уязвимостях (репозитории) носят глобальный международный статус.

Процесс мониторинга защищенности систем в динамично меняющемся IT-пространстве должен быть непрерывным и объективным, способным своевременно противостоять всем современным угрозам и вызовам.

Технические процедуры аудита СУИБ

Уровень развития современных средств анализа защищенности позволяет составить конкуренцию дорогостоящим экспертным оценкам, что дает возможность осуществлять эффективный контроль защищенности системы самостоятельно и непрерывно, в соответствии с принятыми в организации политиками и регламентами, при этом существенно снизив затраты на обеспечение ИБ.

Следует уточнить, что контроль защищенности «собственными силами» не всегда должен заменять аудит, проводимый сторонними организациями, в отдельных случаях внешний контроль регламентируется нормативными или иного рода документами. В последнем случае, можно говорить об усилении мер контроля с использованием собственных технических средств.

RedCheck – инструмент комплексного мониторинга безопасности информационных систем

RedCheck представляет собой простое и удобное решение для анализа защищенности и управления информационной безопасностью организации любого масштаба, обеспечивающее поиск и предотвращение уязвимостей, вызванных ошибками в коде, неверными настройками параметров безопасности, слабостью парольной защиты, несанкционированным изменением конфигураций, несвоевременной установкой критичных обновлений, нарушением принятых политик безопасности.

RedCheck позволяет:

- Повысить эффективность деятельности служб безопасности и IT-подразделений;
- Снизить издержки при управлении безопасностью;
- Обеспечить непрерывный мониторинг защищенности корпоративной сети.

Функциональные возможности

- *Аудит уязвимостей и критичных обновлений безопасности на основе контента в формате языка OVAL для современных программных платформ: Microsoft, Red Hat, POCA, Debian, Ubuntu, ORACLE, и др.;*
- *Аудит конфигураций безопасности на соответствие политикам, рекомендованным разработчиками ПО и экспертными организациями;*
- *Оценка соответствия политикам и стандартам, включая CIS, PCI DSS, СТО БР, ГОСТ Р ИСО/МЭК 27002;*
- *Проведение детальной инвентаризации программного и аппаратно-программного обеспечения сети организации;*
- *Контроль целостности на файловом уровне с использованием встроенных сертифицированных СЗИ;*
- *Анализ сетевой активности;*
- *Проверка сложности паролей;*
- *Детализированные и дифференциальные отчёты по каждому направлению аудита.*

SCAP и Репозиторий OVALdb компании АЛТЭКС-СОФТ

Ключевой особенностью сканера безопасности **RedCheck** является его работа с унифицированным SCAP-контентом (обновления, уязвимости, конфигурации, политики безопасности), получаемым из открытого репозитория OVALdb компании **АЛТЭКС-СОФТ**. Сегодня репозиторий содержит более 40 000 верифицированных проверок безопасности для различных программных и аппаратно-программных платформ, полученных из авторитетных экспертных российских и зарубежных источников.

RedCheck - первый отечественный сканер безопасности, соответствующий набору стандартов и спецификаций SCAP.

Security Content Automation Protocol (SCAP, протокол автоматизации управления контентом безопасности) включает в себя ряд открытых стандартов, поддерживаемых международным сообществом профессионалов в области информационной безопасности. Последняя версия (версия 1.2) SCAP состоит из одиннадцати компонентов протокола в пяти категориях:

Языки. Языки SCAP стандартизуют словари и выражения, описывающие политику безопасности, механизмы контроля и результаты оценки:

- *Расширяемый формат описания контрольного списка конфигураций (XCCDF, The Extensible Configuration Checklist Description Format);*

Открытый язык описания уязвимостей и проведения оценок (OVAL®, Open vulnerability and assessment language). Встроенный в программу **RedCheck** интерпретатор поддерживает последнюю на данный момент версию языка 5.10.1;

- *Открытый интерактивный язык описания контрольного списка (OCIL™, Open checklist interactive language).*

Формат отчетов. Форматы отчета SCAP представляют необходимые конструкции для выражения собранной информации в стандартизированных форматах.

Перечни. Перечни SCAP определяют стандартизованные спецификации, официальные перечни (словари), выраженные с использованием этих спецификаций. SCAP включает в себя следующие перечни:

- *Общий перечень платформ (CPE ™, Common platform enumeration);*
- *Общий перечень конфигураций (CCE ™, Common configuration enumeration);*
- *Общий перечень уязвимостей и рисков (CVE®, Common vulnerabilities and exposures*

Измерение и оценка систем. В SCAP данные процедуры выражаются в оценке определенных особенностей уязвимости (например, слабых мест программного обеспечения и проблем конфигурации безопасности) и определении количественного значения влияния уязвимости (метрики). Метрики SCAP в терминах системных технических требований описываются Общей системой оценки уязвимости (CVSS, Common vulnerability scoring system) и Общей системой оценки конфигурации (CCSS, Common configuration scoring system).

Целостность. Для обеспечения целостности информационного SCAP-контента используется спецификация (TMSAD, Trust Model for Security Automation Data).

SCAP призван автоматизировать процесс управления конфигурациями безопасности, унифицировать форматы представления и спецификации уязвимостей, стандартизовать признаки их выявления, а также обеспечить информационный обмен между производителями и пользователями средств защиты информации. Статус SCAP как международного проекта обеспечивает участие в нем широкого круга специалистов в области информационной безопасности. Протокол поддерживается ведущими мировыми вендорами, такими как Microsoft, Cisco, Symantec, Red Hat и др.

Компания **АЛТЭКС-СОФТ** также присоединилась к сообществу и получила официальный статус OVAL Adopter. Мы являемся первой в России компанией, создающей и поддерживающей Репозиторий определений на языке OVAL, в котором систематизирован информационный контент безопасности (SCAP-контент) для наиболее распространенных программных и аппаратно-программных средств, в том числе и для отечественных средств защиты. Компания «**АЛТЭКС-СОФТ**» неоднократно получала почетный статус Top Contributor и отмечалась на различных международных форумах как организация, вносящая заметный вклад в формирование контента уязвимостей и развитие протокола SCAP.

Наш открытый Web-ресурс OVALdb и решения, построенные на базе протокола SCAP, позволяют широкому кругу специалистов в области информационной безопасности воспользоваться и обменяться опытом и знаниями, наработанными международным сообществом SCAP.

Ключевые преимущества

Сокращение расходов и объема работ по мониторингу защищенности сети

- *Программа оперативно выявляет проблемы несоответствия политикам безопасности, связанные с наличием уязвимостей, несвоевременной установкой критичных обновлений, несанкционированного изменения настроек параметров безопасности, установкой запрещенных программ, изменением состава аппаратных средств.*
- *Программа имеет понятный графический интерфейс, не предъявляет высоких требований к подготовке пользователя при установке и использовании.*
- *Планировщик заданий делает удобным применение программы при повседневном контроле безопасности корпоративной сети.*
- *Совмещение консоли управления и службы сканирования в одном серверном компоненте позволяет легко разворачивать программу при проведении однократных процедур аудита.*
- *Интеграция с сервером консолидации делает удобным процесс мониторинга защищенности распределённых сетей.*
- *Эффективная комбинация агентной и безагентной технологии сканирования сети, позволяющая существенно оптимизировать время проверок и обеспечить требуемый уровень безопасности.*
- *Возможность консолидации результатов сканирования в распределённых сетях.*

Достоверность и прозрачность результатов проверок

- *Контроль изменения конфигураций программного и аппаратного обеспечения сети с помощью дифференциальных отчетов.*
- *Аудит соответствия произвольным требованиям безопасности, а также возможность использования унифицированного SCAP-контента других вендоров: Microsoft, Red Hat, McAfee, eEye и др., при помощи встроенных полнофункциональных интерпретаторов OVAL и XCCDF.*
- *Возможность глубокого анализа результатов контроля, определения причин и способов выявления уязвимостей благодаря открытому описанию контента безопасности (уязвимостей, обновлений, конфигураций).*
- *Высокая достоверность результатов проверок благодаря верификации контента безопасности международным сообществом, поддерживающим SCAP.*
- *Возможность загрузки произвольного контента из репозитория OVALdb, принадлежащего компании **АЛТЭКС-СОФТ**, и других источников.*

Оптимизация бизнес-среды.

- *Получение сведений о защищенности информационной системы с необходимой периодичностью.*
- *Снижение требований к квалификации персонала, отвечающего за информационную безопасность.*
- *Применение эффективных и проверенных политик безопасности (Best practices).*
- *Сокращение объема используемых ресурсов благодаря невысоким требованиям **RedCheck** к аппаратному и программному обеспечению.*
- *Снижение генерируемого трафика и распределение нагрузки на хосты при сканировании с использованием агентной технологии.*
- *Пригодность для работы в изолированных сетях без доступа к сетям общего пользования (Интернет), реализован оффлайн режим обновления контента.*

Программа может быть условно представлена как 3-х уровневое приложение.

1-ый уровень развернут на доверенной части интернет-сайта компании **АЛТЭКС-СОФТ** и представляет собой репозиторий OVALdb, содержащий информационный контент безопасности и Web-службы, позволяющие синхронизировать необходимую информацию локальной БД **RedCheck** с OVALdb. Здесь же расположены средства активации и учета действующих лицензий.

2-ой уровень - консоль управления и служба сканирования **RedCheck**SVR развернутая на сервере компании (рис. 1) или ПЭВМ администратора безопасности (рис. 2). База данных признаков уязвимостей и смежного контента может быть установлена как на компьютере, где установлены консоль управления и служба сканирования **RedCheck**, так и на любом другом сервере, доступном по сети. База функционирует под управлением СУБД Microsoft SQL Server 2008 и последующих версий. Редакция СУБД (Express, Standard, Enterprise) не влияет на функциональные возможности программы.

К **3-му уровню** относятся сканируемые компьютеры и серверы, на которые устанавливается агент-служба программы **RedCheck**, предназначенная для удаленного сканирования службой **RedCheck**SVR. Функции аудита обновлений, аудита уязвимостей и инвентаризации для ОС семейства Microsoft Windows могут быть реализованы и без установки агента программы благодаря технологии сканирования – agentless. В случае безагентного сканирования требуется настроить соответствующий доступ к целевому хосту. Сканирование ЭВМ осуществляется на основе глобального пространства IP-адресов, находящихся как в одноранговой сети, так и в доменной сети, состоящей из одного или нескольких (возможно вложенных) доменов.

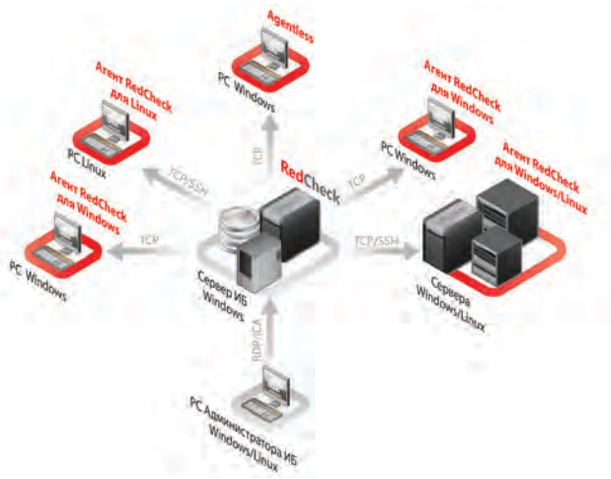


*Рис.1 Установка **RedCheck** на сервер безопасности организации*

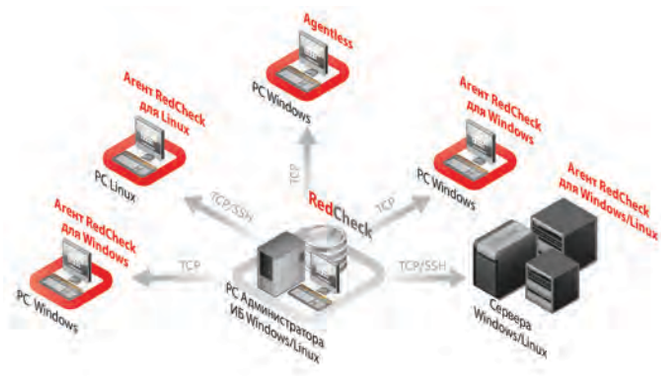


*Рис.2 Установка **RedCheck** на клиентское АРМ администратора безопасности*

Для работы в распределенных филиальных сетях предусмотрена система консолидации сканеров **RedCheck** на уровне отчетов о результатах проверок. В данном случае, в каждом филиале разворачиваются полнофункциональные версии **RedCheck** со своими базами данных контента безопасности, а в центральном офисе устанавливается ПК УИБ, разработки ООО «ЦБИ», предназначенный для обобщения, анализа и представления обобщенных отчетов безопасности в организации.

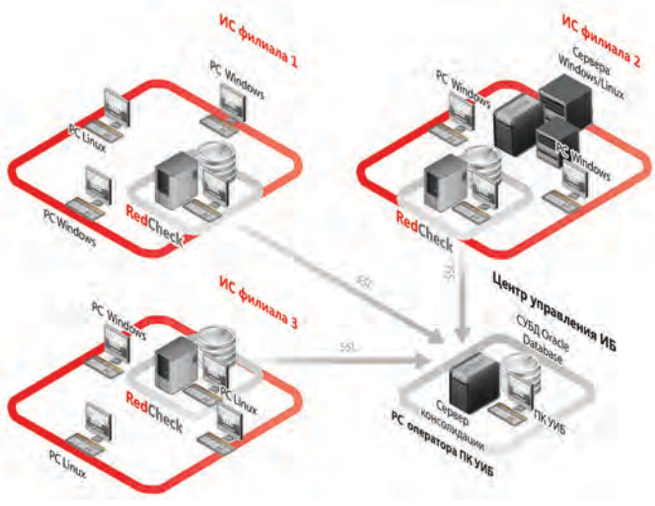


Рис.3 Консолидация результатов контроля с помощью ПК УИБ

В состав ПК УИБ входит:

- *Собственная база данных для хранения и накопления результатов сканирования;*
- *Сервер приложений, предназначенный для взаимодействия клиентских частей ПК с БД, а также для выполнения служебных задач;*
- *Клиентские приложения, выполняющие функции интерфейса пользователя ПК УИБ, интерфейсов взаимодействия ПК УИБ с **RedCheck** и другими сторонними СЗИ, такими как антивирусы, средствами регистрации событий и пр.*

Порядок взаимодействия RedCheck и ПК УИБ достаточно прост: в директивном порядке в центральном офисе формируются регламенты проверок, которые на местах реализуются в виде «заданий» для **RedCheck**, выполняемых с определенной периодичностью. Результаты сканирования, конвертированные особым образом, по защищенным каналам с помощью «коннекторов» ПК УИБ передаются в центральный офис для обработки.

Функционал **RedCheck**

В классификации средств анализа защищённости **RedCheck** является профессиональным сканером безопасности, в котором системные проверки дополнены возможностями сетевого сканирования. Кроме того, функциональность программы усилена средствами контроля соответствия, механизмами оценки защищенности СУБД, сертифицированными средствами контроля целостности и рядом других полезных функций, делающих **RedCheck** эффективным средством поиска уязвимостей и контроля соответствия. Программа создает "моментальный снимок" состояния защищенности системы, позволяет специалистам ИБ обнаруживать слабые места в системе защиты или выполнять оценку соответствия принятым в организации политикам безопасности.

Обнаружение уязвимостей

Сканер безопасности **RedCheck** выполняет централизованное и/или локальное сканирование хостов в сети на наличие уязвимостей операционных систем, специального и прикладного ПО. Аудит хостов может осуществляться в ручном или автоматическом режимах по сформированным в консоли управления заданиям. Сканирование выполняются либо с использованием постоянно работающих управляемых служб-агентов, либо на основе безагентной технологии (agentless). Проверки построены на сопоставлении состояния параметров системы сигнатурам уязвимостей, содержащихся в открытом репозитории OVALdb и описанных в формате SCAP. В базе данных **RedCheck** имеются описания уязвимостей для различных современных платформ и большого количества популярных прикладных программ, включая:

- *Все серверные и клиентские операционные системы Microsoft Windows, начиная с Windows XP/Server 2003;*
- *Серверные и клиентские операционные системы Red Hat, Ubuntu, Debian, POCA, CentOS;*
- *Офисные пакеты Microsoft, Adobe, OpenOffice для Linux-платформ;*
- *СУБД Microsoft SQL 2005/2008/2008R2/2012, Oracle database for Linux/Windows, Oracle MySQL;*
- *Браузеры Microsoft Explorer, Opera, Google Chrome;*
- *Фреймворки, средства виртуализации, языки программирования и многое другое.*

Контент уязвимостей ежедневно актуализируется и пополняется новыми платформами и продуктами. Проверка обновления контента происходит автоматически при каждом запуске программы.

Результаты сканирования сохраняются в разделе «История» и могут быть представлены в виде дифференциальных или общих отчетов. С помощью дифференциальных отчетов можно контролировать эффективность мер по предотвращению ранее выявленных уязвимостей и легко отслеживать вновь появившиеся уязвимости.

Аудит обновлений

По мере обнаружения уязвимостей каждый разработчик стремится как можно быстрее исправить ошибки в коде, выпустив обновления или новые сборки дистрибутивов. В свою очередь, задачей любого администратора является своевременно установить вышедшие обновления, тем самым ликвидировав потенциальные угрозы.

RedCheck быстро и точно укажет на недостающие в системе обновления. В отчете о результатах аудита пользователь найдет ссылки на источники, которые содержат требуемые обновления, а так же описание закрываемых уязвимостей. В базе сканера содержатся сведения об обновлениях серверных и клиентских операционных систем Microsoft, популярных Linux платформ, а также большого количества системных и прикладных программ.

Контроль конфигураций и оценка соответствия политикам безопасности

Наиболее простой и доступный способ взломать «оборону» - это найти системы, содержащие программное обеспечение, инсталлированное с настройками по умолчанию. Как правило, такие конфигурации предоставляют максимальную функциональность программ, но не гарантируют их безопасность. Подразумевается, что осуществление настроек безопасности и контроль их неизменности - обязанность специалиста ИБ или пользователя. Но сложность и многообразие программного обеспечения являются фактором, значительно усложняющим процесс корректной настройки «вручную», не только для новичков, но и для опытных специалистов. К сожалению, именно "человеческий фактор", а точнее, отсутствие должной квалификации и ответственности администраторов зачастую является главной угрозой безопасности информационных систем. Также стоит отметить еще один немаловажный момент - настройки безопасности должны быть разумными, сбалансированными и не мешать решению целевых задач системы.

Ответственные разработчики стараются подстраховать пользователей, предоставив им свои варианты настроек параметров безопасности, или же предлагают воспользоваться конфигурациями, разработанными экспертными организациями. Как правило, такие рекомендации представлены в виде Руководств по безопасности или конфигурационных файлов (шаблонов), которые можно применять с помощью локальных или групповых политик. Задачей системного администратора является адаптация и применение данных настроек безопасности, а также последующий контроль за их неизменностью.

Аудит защищенности СУБД

RedCheck является эффективным инструментом управления безопасностью СУБД. Помимо известных уязвимостей(CVE) и неустановленных критичных обновлений, сканер способен выполнять проверки хранимых процедур и настроек безопасности популярных СУБД Microsoft SQL Server 2005/2008/2012, в том числе касающихся:

- *Сетевого взаимодействия СУБД;*
- *Систем аутентификации;*
- *Механизмов разграничения доступа;*
- *Прав и привилегий пользователей.*

Инвентаризация сети

Сканер позволяет получать информацию об операционных системах, пакетах обновлений и исправлениях, установленном ПО, запущенных процессах, общих папках, аппаратном обеспечении и многом другом. Глубокая детализация отчетов позволяет отслеживать даже самые незначительные изменения в составе программного и аппаратного обеспечения.

RedCheck позволяет создать «опись» аппаратно-программного обеспечения сети без установки агента программы для компьютеров, работающих на платформе Microsoft. Для инвентаризации компьютеров под управлением Linux необходима установка специального пакета, входящего в состав дистрибутива.

Фиксация и контроль целостности

С помощью программы может быть реализован контроль целостности программного обеспечения, включая средства защиты информации. Фиксация и контроль целостности исполняемых файлов, библиотек, реестра, а так же произвольных файлов осуществляется методом контрольного суммирования по Уровню 3 (ГОСТ 28147-89) с использованием сертифицированного СЗИ «ФИКС-библиотека 1.0» (Сертификат ФСТЭК России № 677), входящего в состав сканера.

В RedCheck предусмотрена блокировка запуска на случай обнаружения фактов нарушения целостности исполняемых файлов и служебных библиотек, что позволяет использовать сканер в информационных системах, к которым предъявляются повышенные требования безопасности (ГИС, ИСПДн, АС, банковские системы), без применения каких-либо дополнительных средств контроля целостности.

Сканирование портов

Поддержка утилиты Nmap позволила реализовать в **RedCheck** ряд возможностей сетевого сканера. Этот функционал дополняет и повышает общую эффективность проверок. Сканирование портов дает возможность определить такую доступную информацию об исследуемых хостах как: открытые порты, протоколы работы портов, сетевые сервисы и т.д.

Получение всей информации происходит при минимальном уровне привилегий. В зависимости от необходимой полноты сканирования и временных ограничений можно использовать один из нескольких профилей: от быстрого сканирования до полного глубокого исследования.

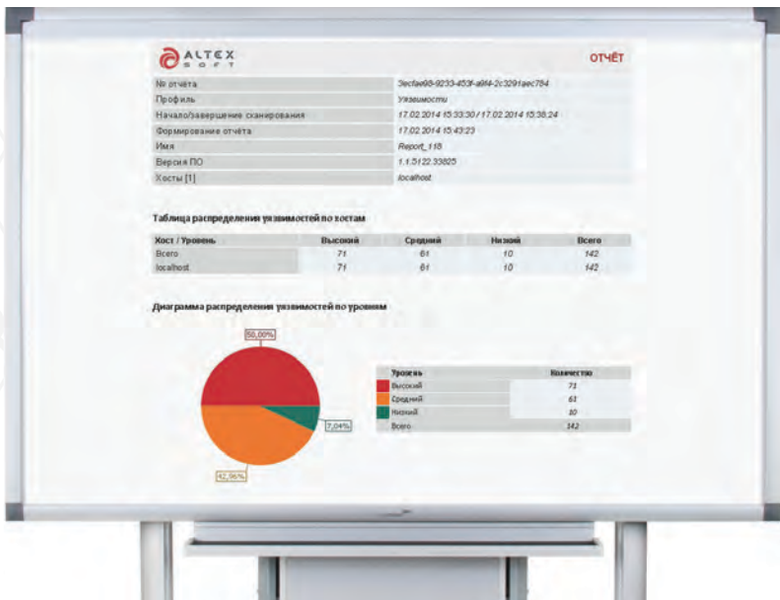
Проверка сложности паролей

С помощью программы **RedCheck** администратор безопасности может проверить стойкость паролей, а также некоторые уязвимости, связанные с механизмами аутентификации операционных систем и СУБД.

RedCheck подбор паролей «по словарю» и парольным хэшам, что, прежде всего, востребовано при проверке механизмов аутентификации СУБД. Данный функционал доступен для Microsoft SQL Server, Postgre SQL и Oracle SQL.

Документирование результатов проверок

Результаты сканирования сохраняются в «истории» проверок, но могут быть экспортированы в формат PDF. Отчеты предоставляются либо в простом, либо в дифференциальном виде, что дает возможность легко отслеживать любые изменения, будь то появившиеся уязвимости, несанкционированно установленное ПО или «железо». Для быстрого поиска необходимых событий в программе реализованы фильтры, позволяющие выполнять выборку по дате, временному интервалу, типу проверок, статусу, наименованию или номеру хоста. Формирование отчетов в формате PDF дает возможность экспортировать их в любой текстовый формат, поддерживаемый Adobe Acrobat или аналогичными программами.



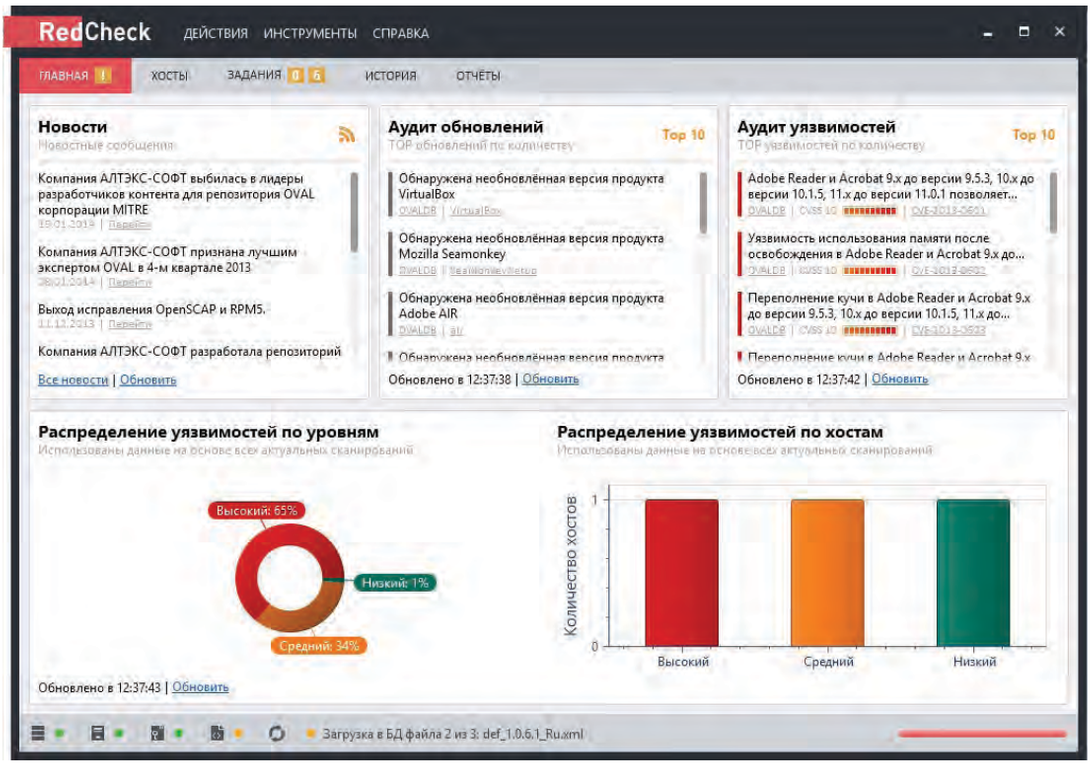
Работа с программой

Интерфейс программы

RedCheck имеет функциональный интерфейс, который прост в обращении и не требует специальной подготовки.

Интерфейс консоли управления состоит из следующих элементов:

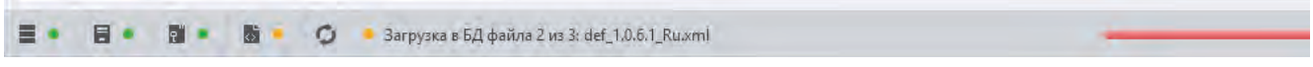
- *Пункты меню (Действия, Инструменты, Справка);*
- *Вкладки (Главная, Хосты, Задания, История, Отчеты);*
- *Статусная панель.*



Интерфейс «главной» вкладки консоли управления RedCheck

Через Пункты меню осуществляется управление всей программой: формируются пулы сканируемых хостов, создаются задания, осуществляется настройка режимов работы, управление обновлениями и контентом безопасности, доступ к справочной информации и многое другое.

Во Вкладках (центральное меню) размещены элементы управления процессами сканирования, в частности, представлена текущая информация (история) о результатах проверок, объектах сканирования, сформированных заданиях, отчетах о результатах аудита.



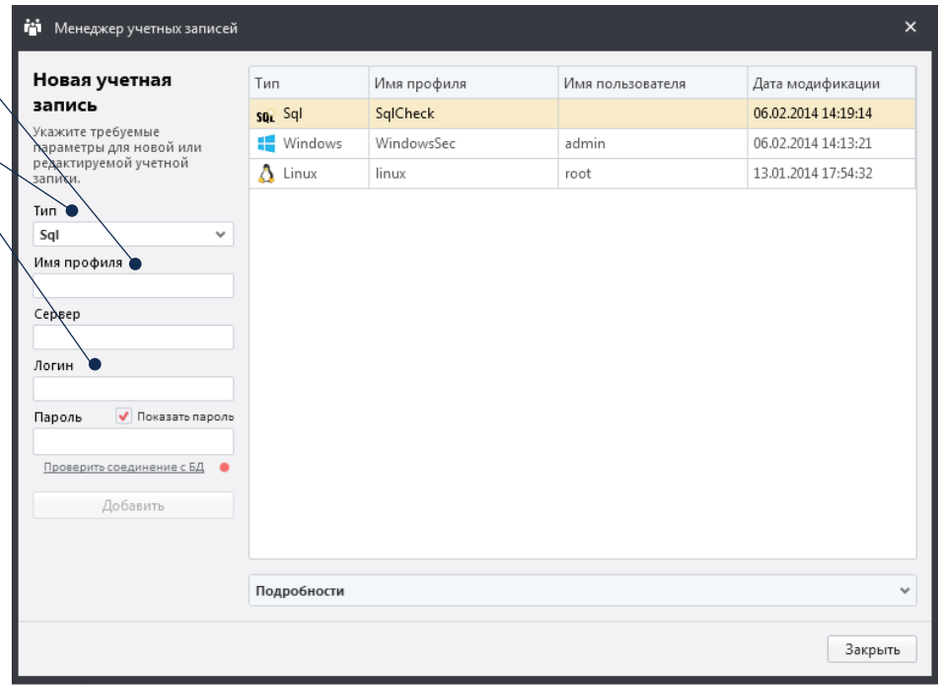
В статусной панели (нижняя панель) отображается важная информация о работе **RedCheck**: соединения консоли с базой данных и службой сканирования, активация лицензии, статус обновлений и пр.

Порядок работы

Провести оценку защищенности компьютера или корпоративной сети при помощи сканера безопасности **RedCheck** можно всего за несколько шагов:

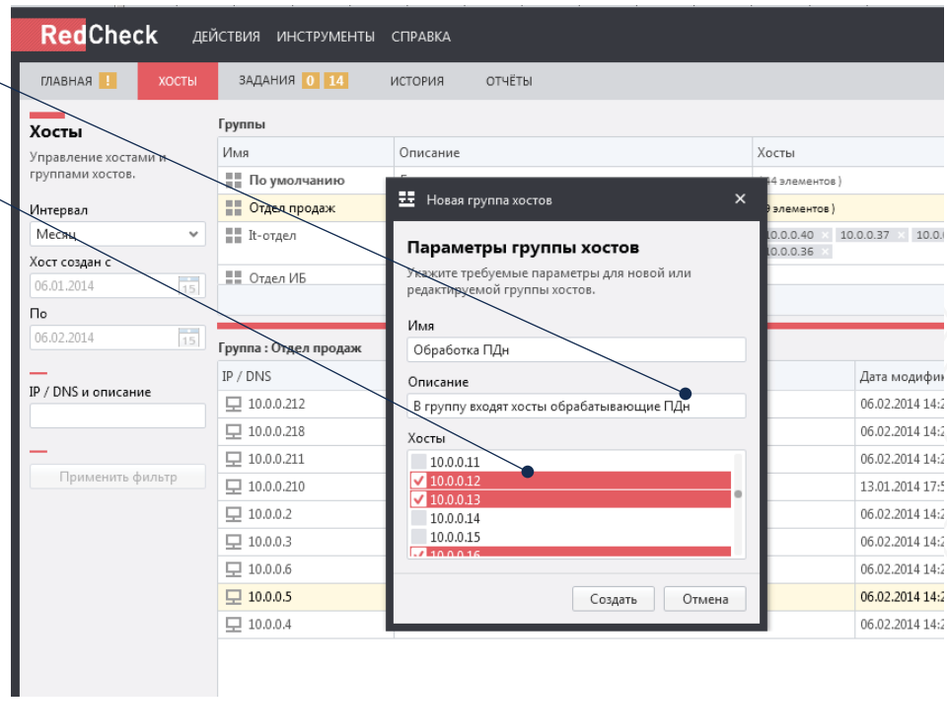
1. Добавить учетную запись, от имени которой будет осуществляться сканирование.

- *Задать произвольное название профиля.*
- *Выбрать нужный тип учетной записи.*
- *Указать учетные данные.*



2. Создать пул сканируемых хостов.

- *Задать IP-адреса и\или DNS имена хостов.*
- *Поместить заданные хосты в группу (при необходимости).*

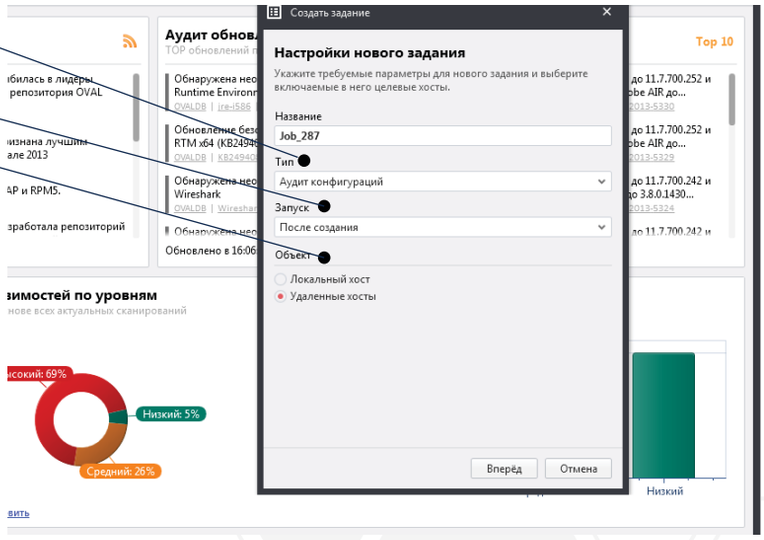


Функция «Импорт хостов» позволяет быстро импортировать хосты из Active Directory или получить список доступных хостов с помощью сетевого сканирования.

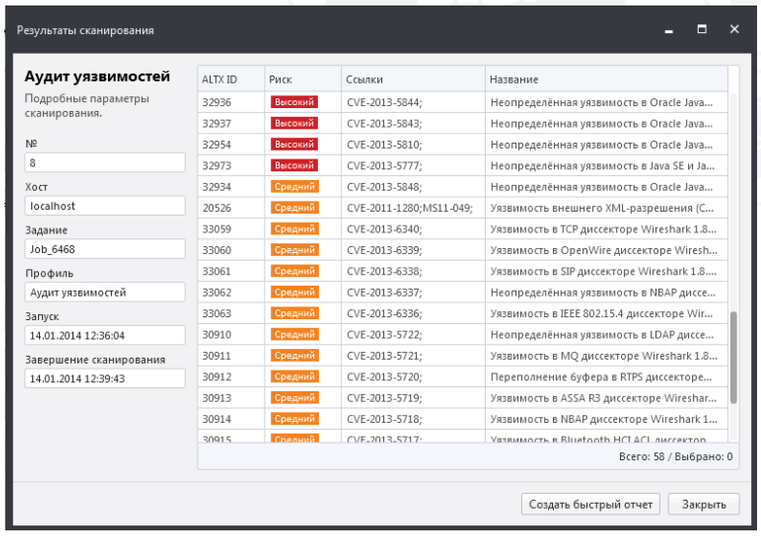
3. При необходимости установить и проверить соединение с агентами программы RedCheck (Windows/Linux).

4. Сформировать задание.

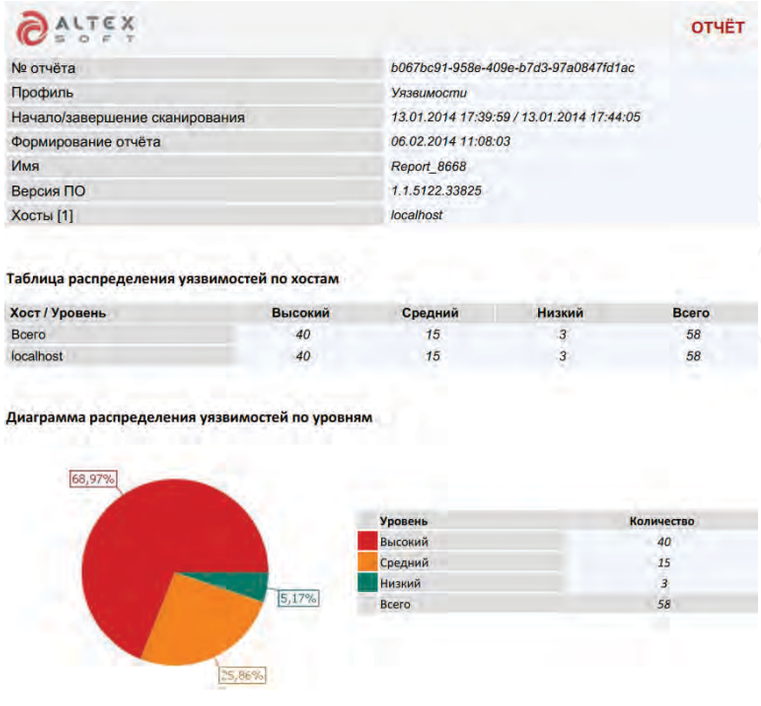
- *Выбрать необходимый тип проверок.*
- *Определить сценарий сканирования (сразу после создания, по расписанию).*
- *Определить объекты проверок.*



5. Просмотр полученных результатов выполняется на вкладке «История».



Результаты сканирования могут быть представлены в виде простых или дифференциальных отчетов в формате PDF, а затем, при необходимости, с помощью любого pdf-редактора конвертированы в произвольный графический или текстовый формат.



Представление результатов сканирования в редактируемых форматах.

RedCheck при реализации и оценке эффективности мер защиты информации в ГИС[1,3] и ИСПДн[2]

Сканнер безопасности **RedCheck** сертифицирован на соответствие требованиям безопасности информации в системе сертификации № РОСС RU.0001.01БИ00 (ФСТЭК России). Сертификат подтверждает соответствие заявленным в ТУ 643.83252182.RC01-01 функциям безопасности и требованиям Руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» – по 4 уровню контроля.

RedCheck является эффективным инструментом операторов персональных данных и государственных информационных ресурсов при реализации мероприятий по контролю (анализу) защищенности информационных ресурсов. Программа может использоваться в составе АС до класса защищенности 1Г и информационных системах персональных данных (ИСПДн) и государственных информационных системах (ГИС) до 1 класса (уровня) защищенности включительно.

Сопоставление требуемых мер защиты и реализованных функций безопасности RedCheck

Условное обозначение меры	Меры защиты информации в информационных системах	Функции RedCheck	ИСПДн	ГИС
ОПС.2	Контроль за установкой компонентов программного обеспечения	Инвентаризация ПО	+	+
РСБ.3	Сбор, запись и хранение информации о событиях безопасности	История/Отчеты	+	+
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них	История/Отчеты	+	+
АН3.1	Выявление, анализ уязвимостей информационной системы	Аудит уязвимостей	+	+
АН3.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	Аудит обновлений	+	+
АН3.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации	Аудит конфигурации	+	+
АН3.4	Контроль состава технических средств, программного обеспечения и средств защиты информации	Инвентаризация ПО и аппаратных средств	+	+
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации	Фиксация и контроль	+	+
ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций	Фиксация и контроль, Аудит конфигурации	+	+
УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты данных	Аудит конфигурации	+	-
УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных	История/Отчеты	+	+

[1] Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (Приказ ФСТЭК России от 11 февраля 2013 г. N 17).

[3] Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (Приказ ФСТЭК России от 18 февраля 2013 г. N 21).

[2] Меры защиты информации в государственных информационных системах (Методический документ ФСТЭК России от 11 февраля 2014 г).

Лицензирование

Программа лицензируется по количеству сканируемых IP-адресов с одной консоли управления **RedCheck.** В последующем, лицензия может быть продлена по запросу. В течение действия лицензии пользователю предоставляется техническая поддержка, доступ к актуальному контенту безопасности и обновлениям программ для данной версии.

RedCheck может поставляется в электронном или коробочном варианте. Сертифицированная версия программы поставляется только в коробочном варианте, в который помимо лицензии и эксплуатационной документации, входит Медиа-комплект в составе: верифицированный дистрибутив, заверенная копия Сертификата и сопроводительная документация, маркированная голографическим Знаком соответствия ФСТЭК России.

Демоверсия

Прежде чем приобрести **RedCheck,** вы можете бесплатно протестировать все функциональные возможности продукта. Для получения демонстрационной версии необходимо оставить запрос на сайте **www.redcheck.ru**.

Демоверсия идентична коммерческой версии программы, но имеет ограничения по количеству одновременно сканируемых IP-адресов – не более 5 IP и сроку действия лицензии (возможность получения актуального контента безопасности) – 3 месяца. Демоверсию RedCheck Вы можете полноценно использовать в течение указанного выше срока не только в тестовом режиме, но и для мониторинга защищенности собственной корпоративной сети.

Как приобрести

RedCheck можно приобрести в нашем интернет-магазине **www.altx-store.ru** или через партнерскую сеть нашего официального дистрибьютора компанию **Axoft**.

Axoft официальный дистрибьютор RedCheck

Созданная в 2004 году, компания **Axoft** является одним из лидеров на рынке дистрибуции программного обеспечения в России и странах СНГ. Партнерская сеть **Axoft** насчитывает свыше 6000 компаний, в числе которых реселлеры ПО, системные интеграторы, разработчики программных решений, Интернет-магазины и консалтинговые компании. Офисы «**Аксофт**» действуют в 33 регионах России и странах Ближнего Зарубежья. Продуктовый портфель компании состоит из программного обеспечения более 1000 российских и иностранных производителей различного направления и масштаба.

Партнером АЛТЭКС-СОФТ быть выгодно и удобно

Благодаря развитой партнерской сети продукты **АЛТЭКС-СОФТ** доступны в любом регионе России и ближнего зарубежья. Нашими клиентами являются органы государственной власти и управления, крупные коммерческие структуры и компании малого бизнеса. Партнерская программа **АЛТЭКС-СОФТ** ориентирована на компании, работающие в области безопасности и информационных технологий, занимающихся поставкой, внедрением и сопровождением различных решений конечным пользователям. Гибкие программы сотрудничества обеспечивают разнообразные варианты партнерства и индивидуальные условия поставок средств защиты информации. Компания **АЛТЭКС-СОФТ** предоставляет партнеру презентационные и маркетинговые материалы, лицензии на продукты для внутреннего тестирования, и организует демонстрации заказчикам, оказывает помощь в подготовке проектной и конкурсной документации. Мы активно содействуем партнерам в реализации наших продуктов: проводим совместное планирование бизнеса, даем рекомендации по организации продаж, организуем акции и семинары. Для партнеров организована специальная линия технической поддержки. Целевые рассылки, партнерский сайт, печатные и электронные материалы помогут партнерам оставаться в курсе наших достижений и актуальных тенденций на рынке информационной безопасности.

ЗАО «АЛТЭКС-СОФТ»

141067, Московская обл., г. Королев, мкрн. Болшево, ул. Маяковского, д.10А

Тел.: +7 (495) 543-31-01, +7 (498) 601-49-38

Факс: +7 (498) 720-89-14

E-mail: info@altx-soft.ru, sales@altx-soft.ru