



Код безопасности
ГК «Информзащита»

Сравнение Trust Access и SSEP

Выбираем программный межсетевой экран, который позволит наиболее оптимально решить задачи организации.

Введение

Выбор межсетевого экрана для использования в системах защиты информации организаций и предприятий обуславливается несколькими факторами. Наиболее важен ряд задач, для которых будет использоваться межсетевой экран, необходимо учесть также и архитектуру ИС предприятия и те важные объекты сети, которые необходимо защищать. Межсетевой экран (МЭ) – комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию, проходящих через него сетевых пакетов в соответствии с заданными правилами. Основной задачей МЭ является защита компьютерных сетей или отдельных узлов от несанкционированного доступа. В зависимости от охвата контролируемых потоков данных МЭ делятся на традиционные и персональные. Традиционный МЭ контролирует входящие и исходящие потоки данных между подключенными сетями. Персональный сетевой экран устанавливается на конкретный компьютер и обеспечивает защиту от несанкционированного доступа только этого компьютера. При этом персональный межсетевой экран может обеспечивать защиту как рабочего места пользователя, так и сервера. Поскольку потенциальные угрозы безопасности для рабочего места и сервера различны, то и

средство защиты не должно быть одним и тем же. Например, на рабочем месте пользователя основным источником угроз является подключение к сети Интернет: интернет-трафик может содержать спам, вирусы и т.д. Тогда как для сервера, который может и не иметь подключения к Интернету, на первый план выходит угроза несанкционированного доступа к данным со стороны внутренних нарушителей.

В линейке компании «Код Безопасности» присутствуют несколько продуктов, которые по своей технологической основе относятся к программным продуктам класса «межсетевой экран». Эти решения применимы как для защиты рабочего места пользователя – Securiry Studio Endpoint Protection (SSEP), так и для защиты других локальных ресурсов сети – TrustAccess. Причем надо отдельно отметить, что в SSEP персональный межсетевой экран является только частью защитного функционала. В SSEP, помимо персонального МЭ, входят также IDS и HIPS, антивирус и антиспам. Тогда как Trust Access – это решение для обеспечения высокого уровня защиты для значимых объектов информационной сети организации, а именно – серверов.

Security Studio Endpoint Protection – комплексная защита сетевого рабочего места

Рабочие места пользователей в большинстве организаций не изолированы: компьютеры объединены в локальную сеть и, как правило, имеют выход в Интернет. Традиционные средства защиты информации (СЗИ) от несанкционированного доступа (НСД), созданные на базе требований к автоматизированным системам, сконцентрированы на защите локальных конфиденциальных файловых ресурсов и не гарантируют защиту данных на сетевых рабочих местах.

Security Studio Endpoint Protection (SSEP) – система для защиты сетевых рабочих мест, используемых для обработки конфиденциальной информации и персональных данных.

Продукт позволяет решить следующие основные задачи:

- обеспечение безопасного доступа в локальную сеть и Интернет;

- защита от вирусов и программ-шпионов;
- защита от неизвестных угроз;
- безопасное использование сетевых ресурсов и защита от спама;
- защита от отключения вредоносным ПО.

Security Studio Endpoint Protection состоит из трех функциональных компонентов:

- межсетевой экран (SSEP Firewall);
- средство обнаружения вторжений (SSEP HIPS);
- антивирус (SSEP Antivirus).

Полученные сертификаты ФСТЭК на каждый компонент позволяют выполнить требования Федерального закона «О персональных данных» в части защиты информации в информационных системах с применением межсетевых экранов, антивирусов и средств обнаружения вторжений.

Помимо основного защитного функционала, SSEP располагает дополнительными средствами защиты рабочих станций от внешних угроз:



Для удобства использования продукта в корпоративной сети были разработаны средства администрирования SSEP: мастер развертывания и настройки сервера обновлений и Administration Center, позволяющий централизованно устанавливать и настраивать продукт на рабочих станциях.

Стоит отметить и другие важные особенности SSEP:

- совместимость с средством защиты от несанкционированного доступа (СЗИ от НСД) Secret Net, что позволяет создать комплексную сертифицированную

защиту рабочих мест в информационных системах персональных данных (ИСПДн): Secret Net обеспечивает защиту от внутренних угроз, SSEP – защиту от внешних угроз;

- возможность выбора варианта поставки в зависимости от решаемых задач. Например, если в компании уже используется антивирус другого производителя, можно не приобретать антивирус, входящий в состав SSEP.

Распределенный межсетевой экран TrustAccess

Как правило, современные информационные системы, в том числе и информационные системы персональных данных, представляют собой клиент-серверные или многозвенные распределенные системы. Данные в таких системах обрабатываются не только локально на компьютерах, но и на серверах баз данных, в клиентских приложениях, использующих сетевые сервисы, в веб-приложениях и т. д. Традиционные СЗИ от НСД не гарантируют защиту данных при их передаче по сети. Для достижения защищенного сетевого взаимодействия обычно применяются средства межсетевого экранирования (межсетевые экраны) определенного класса защиты.

Сертифицированный распределенный межсетевой экран TrustAccess может применяться для защиты ИСПДн любого класса, в том числе и максимального класса К1. А его усиленная версия – TrustAccess-S

– предназначена специально для защиты сведений, составляющих гостайну. В отличие от обычной версии TrustAccess, которая имеет сертификат ФСТЭК России по классу МЭ 2 и уровню НДВ 4, усиленная версия сертифицирована уже по уровню НДВ 2 и позволяет обеспечить легитимную защиту АС класса 1Б (до грифа «совершенно секретно»).

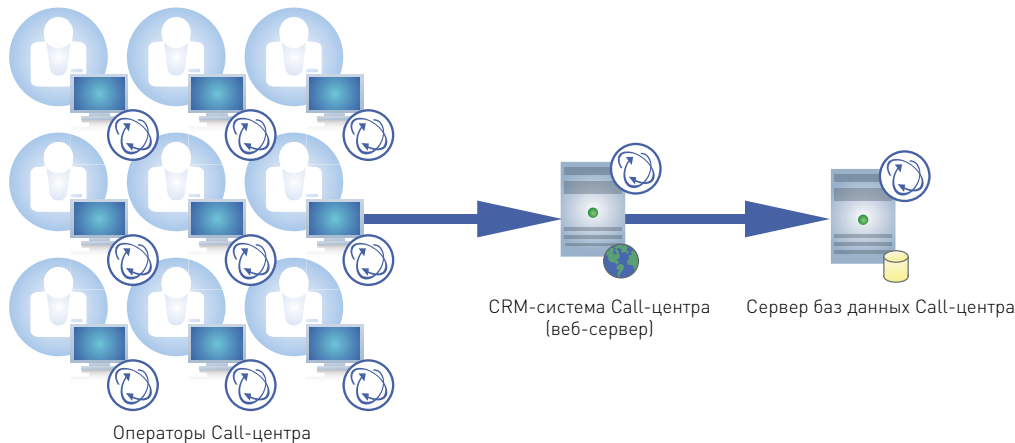
В отличие от традиционного МЭ, устанавливаемого на границе сетей/сегментов сети, компоненты TrustAccess функционируют непосредственно на защищаемых объектах, что позволяет разграничить доступ аутентифицированных абонентов к защищаемым информационным системам.

Ниже приведены некоторые сценарии применения TrustAccess для решения различных практических задач.

Сценарий 1. Защищенное межсетевое взаимодействие в клиент-серверных и многозвенных ИСПДн

На иллюстрации показан сценарий организации защиты персональных данных с помощью TrustAccess на примере Call-центра. Операторы

Call-центра принимают или совершают телефонные звонки и фиксируют результаты в CRM-системе, осуществляя при этом обработку персональных данных.



TrustAccess, установленный на рабочие места операторов Call-центра, позволит предоставить доступ к CRM-системе только операторам Call-центра. Пользователям корпоративной компьютерной сети, работа которых не связана с обработкой персо-

нальных данных, доступ в CRM-системе запрещается. TrustAccess, установленный на серверы CRM-системы и СУБД, предоставляет доступ к базам данных только веб-серверу с CRM-системой Call-центра.

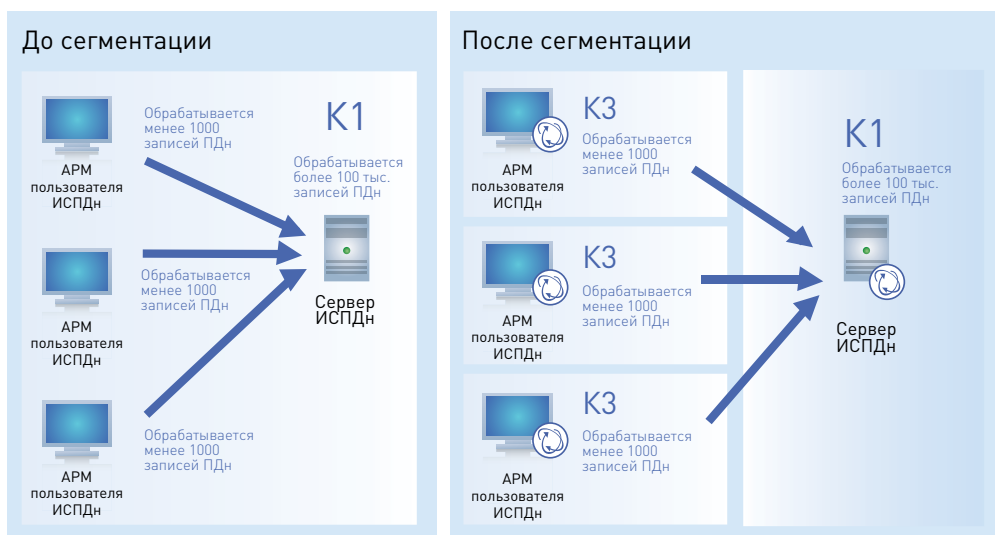
Сценарий 2. Снижение класса ИСПДн

TrustAccess может использоваться для снижения класса ИСПДн путем сегментирования с целью сэкономить на защите. Сегментирование ИСПДн посредством сертифицированных межсетевых экранов является легитимным способом снижения класса ИСПДн – согласно приказу 58 ФСТЭК «При разделении информационной системы при помощи межсетевых экранов на отдельные части системы для указанных частей системы может устанавливаться

более низкий класс, чем для информационной системы в целом».

TrustAccess, установленный на сегментированные участки сети, позволяет снизить класс защищенности сегментированных участков и, соответственно, сэкономить на защите.

На иллюстрации продемонстрирован пример сегментирования ИСПДн с помощью TrustAccess.



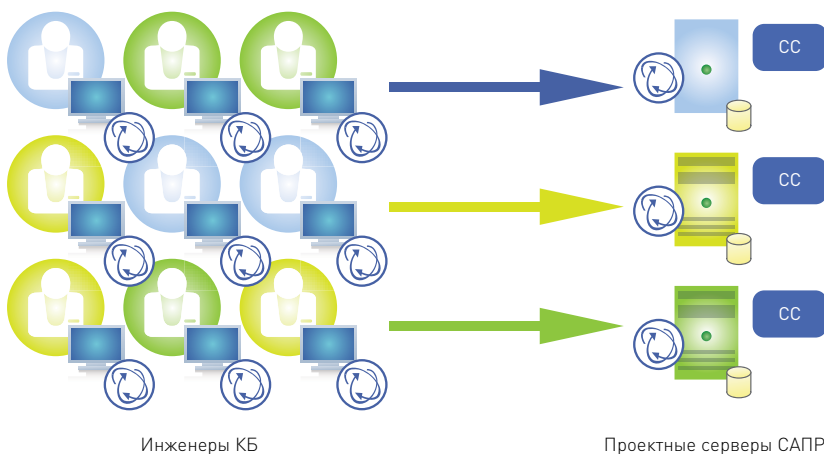
Поскольку на сервере ИСПДн обрабатывается более 100 тыс. записей персональных данных второй категории (ФИО, место работы, семейное положение), то вся ИСПДн классифицируется как К1. Разбив с помощью межсетевого экрана всю ИСПДн на отдель-

ные сегменты, рабочие станции можно классифицировать как ИСПДн класса К3, поскольку на каждой рабочей станции обрабатывается одновременно не более 1000 записей ПДн.

Сценарий 3. Защита сведений, составляющих государственную тайну

На рисунке показано, как с помощью усиленной версии TrustAccess-S можно разграничить сетевой доступ к серверам, обрабатывающим сведения,

составляющие государственную тайну, на основе групп пользователей.



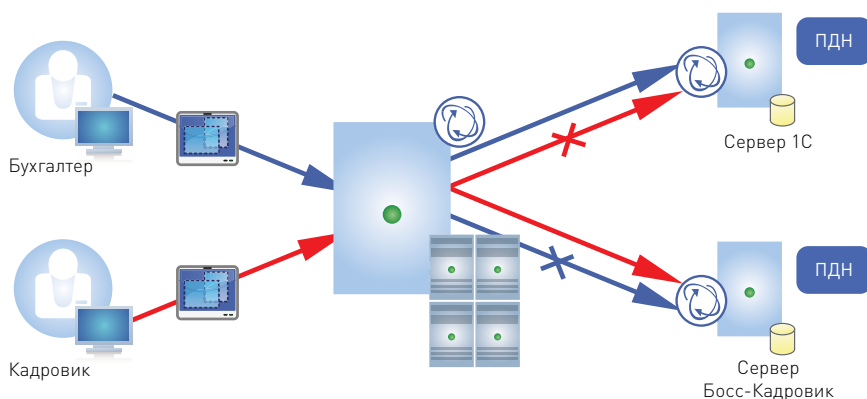
В зависимости от того, над каким проектом работает инженер, он получает доступ к тем или иным серверам (сетевым сервисам).

Сценарий 4. Защита терминальных соединений

Для оптимизации IT-инфраструктуры в некоторых современных компаниях применяются решения на основе терминальных служб. В этом случае разные пользователи получают доступ к обрабатываемым данным с одного физического компьютера и с одного IP-адреса – сервера терминальных служб. Как правило, традиционные межсетевые экраны оказываются неэффективны в условиях терминальных соединений.

На иллюстрации продемонстрировано как TrustAccess, установленный на защищаемые серверы, позволяет обеспечить защиту терминальных соединений и разграничить доступ к данным на уровне пользователей, работающих на одном физическом компьютере.

Таким образом, бухгалтер получит доступ только серверу 1С, а сотрудник отдела кадров – к кадровой системе даже при терминальном соединении.

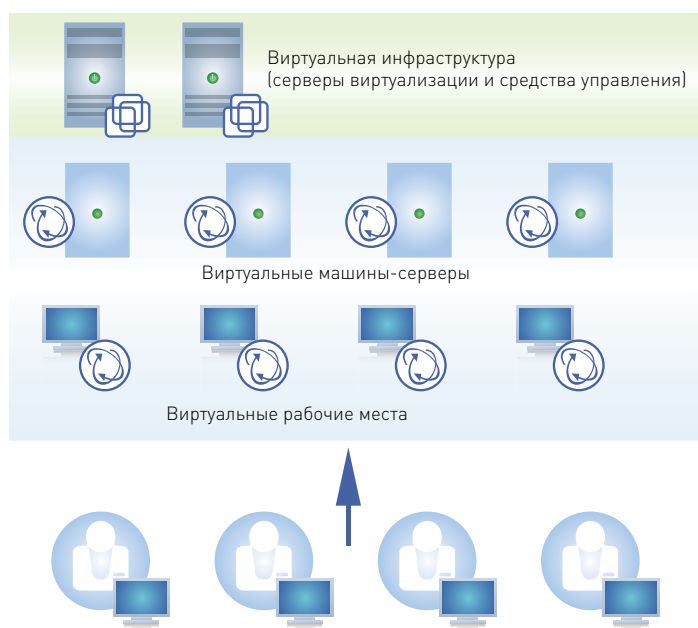


Сценарий 5. Защита виртуальных машин

Виртуализация – одна из наиболее перспективных технологий корпоративного сектора, внедрение которой позволяет снизить капитальные и эксплуатационные затраты. Безопасность информации, обрабатываемой в виртуальной среде, один из ключевых вопросов при внедрении технологии виртуализации.

TrustAccess, установленный на виртуальные машины, позволяет защитить как виртуальные

машины – сервера, так и виртуальные рабочие места. При этом виртуальные машины будут защищены от сетевых атак как со стороны внешних физических машин, так и со стороны виртуальных машин. Отдельно следует отметить, что механизмы защиты TrustAccess нечувствительны к подмене MAC- или IP-адресов, на которых обычно базируются такого рода атаки.



SSEP или TrustAccess: что же выбрать?

- В зависимости от решаемой задачи

Итак, выбор межсетевого экрана зависит в первую очередь от задач, которые планируется решить с помощью данного продукта. Если необходимо обеспечить защиту сетевых серверов, обрабатывающих сведения ограниченного доступа, то следует исполь-

зовать TrustAccess; а если комплексную защиту сетевых рабочих мест – SSEP.

В таблице показано, какой именно стоит выбрать продукт в зависимости от решаемой задачи:

Вариант использования	Security Studio Endpoint Protection 6	Trust Access 1.1
Фильтрация Интернет-трафика	✓	
Проактивная защита (HIPS/IDS)	✓	
Разграничение доступа к сетевым ресурсам в условиях терминальной среды	✓	✓
Разграничение сетевого доступа пользователей к серверу		✓
Защищенное межсетевое взаимодействие в клиент-серверных и многозвенных системах		✓
Межсетевое экранирование в виртуальной среде		✓
Защита конфиденциальных данных	✓	✓
Защита персональных данных	✓	✓
Возможность снижения класса ИСПДн		✓
Защита сведений, составляющих государственную тайну		✓
Сертификаты ФСТЭК России		
МЭ4/НДВ4	✓	
МЭ2/НДВ4		✓
МЭ2/НДВ2		✓
HIPS ТУ/НДВ4	✓	
Antivirus ТУ/НДВ4	✓	
Сертификаты совместимости		
VMware Ready		✓
Совместимо с Windows 7		✓

Из таблицы видно, что продукты решают совершенно разные задачи.

* С помощью Administration Center.

Сравнительная характеристика функциональных возможностей Security Studio Endpoint Protection 6 и Trust Access 1.1

В таблице приведена подробная сравнительная характеристика функциональных возможностей обоих продуктов.

Функции межсетевого экрана	Security Studio Endpoint Protection 6	Trust Access 1.1
Настройка правил фильтрации		
Настройка режима (политики) безопасности	√	√
Настройка правил для пакетов	√	√
Типовые наборы правил фильтрации	√	√
Контроль активности ICMP	√	√
Настройка аварийных правил для пакетов. Механизм защиты от сетевых сбоев		√
Настройка правил для прикладных протоколов		√
Расписание применения правил	√*	√
Программирование реакции при срабатывании правил		√
Режим обучения	√	
Настройка правил для приложений	√	
Аутентификация		
Аутентификация пользователей. Поддержка правил для пакетов на основе ID-отправителя		√
Аутентификация компьютеров. Поддержка правил для пакетов на основе ID-отправителя		√
Группы пользователей. Поддержка групп пользователей в правилах	√*	√
Сетевая защита		
Защита сетевых пакетов от модификации		√
Защита сетевых пакетов от перехвата		√
Защита сетевых пакетов от replay атак		√
Система обнаружения сетевых атак (IDS)	√	
Система предотвращения вторжений на хост (HIPS)	√	
Централизованное управление клиентскими компьютерами		
Парольная защита администрирования	√	√

Функции межсетевого экрана	Security Studio Endpoint Protection 6	Trust Access 1.1
Гранулярность удаленной настройки до уровня шаблона правил	√	√
Журнал сетевой активности	√	√
Гранулярность удаленной настройки до уровня правила на сервере		√
Развертывание клиентской части через Active Directory	√	√
Автоматическое обновление баз и модулей программ на компьютерах	√	
Собственный инструмент для централизованного развертывания клиентской части (SSEP Administration Center)	√	
Сертификаты		
Сертификат межсетевого экрана по ФСТЭК (МЭ4/НДВ4)	√	
Сертификат межсетевого экрана по ФСТЭК (МЭ2/НДВ4)		√
Сертификат межсетевого экрана по ФСТЭК (МЭ2/НДВ2)		√
HIPS (ТУ/НДВ4)	√	
Antivirus (ТУ/НДВ4)	√	
Подтверждение совместимости		
Сертификация ПО в Microsoft		√
Сертификация ПО в VMware (VMware Ready)		√
Поддерживаемые платформы		
Windows 2000	√	√
Windows XP	√	√
Windows 2003	√	√
Windows Vista	√	√
Windows 2003 R2		√
Windows 7		√
Windows 2008		√
Windows 2008 R2		√

- В зависимости от вида защищаемой информации ограниченного доступа

В данный момент наиболее актуальной проблемой для большинства российских компаний является защита персональных данных или иных сведений ограниченного доступа.

В таблице показано, какой именно стоит выбрать продукт в зависимости от вида информации, которую необходимо защитить:

Виды защищаемой информации	Security Studio Endpoint Protection 6	Trust Access 1.1
Персональные данные		
К1	√*	√
К2	√	√
К3	√	√
Сведения, составляющие государственную тайну		
Секретно		√
Совершенно секретно		√
Конфиденциальная информация (ДСП)	√	√

В следующей таблице показано, какие именно классы требований к системе защиты персональных данных (на основании приказа ФСТЭК 58) можно закрыть с помощью соответствующего продукта:

Классы требований защиты ПДн	Security Studio Endpoint Protection 6	Trust Access 1.1
Подсистема межсетевого экранирования	√	√
Подсистема управления доступом		√
Подсистема регистрации и учета	√	√
Подсистема антивирусной защиты	√	
Подсистема обнаружения вторжений	√	
Подсистема контроля целостности СЗИ		√

Как видно из таблицы, помимо требований к подсистеме межсетевого экранирования, продукты позволяют выполнить еще и другие классы требований. Например, TrustAccess позволяет выполнить требо-

вания к подсистемам управления доступом, а также регистрации и учета, что может быть крайне полезным в условиях отсутствия сертифицированных традиционных СЗИ от НСД.

* Может применяться для защиты ИСПДн К1 с ограничением: при подключении к сетям общего пользования в ИСПДн К1 необходимо использовать АПКШ «Континент» на периметре организации. В этом случае SSEP МЭ обеспечивает защиту от сотрудников, которые не имеют прав доступа к ИСПДн.

Коротко о SSEP

Security Studio Endpoint Protection (SSEP) – сертифицированное комплексное программное решение, обеспечивающее полную защиту автоматизированного рабочего места от внешних угроз в соответствии с требованиями ФСТЭК в области защиты персональных данных.

SSEP обеспечивает защиту компьютера с применением меж сетевого экрана, антивируса и средства обнаружения вторжений. Решение обеспечивает безопасную и комфортную работу с сетью Интернет, предотвращая любые попытки проникновения на компьютер вредоносного ПО и блокируя нежелательный трафик.

Основные возможности SSEP

- Безопасный доступ в сеть
- Защита от известных вирусов и программ-шпионов
- Защита от неизвестных угроз
- Безопасное использование сетевых ресурсов и защита от спама

Сертификаты

Продукт имеет следующие сертификаты: SSEP Personal Firewall – МЭ4, НДВ4; SSEP HIPS – ТУ, НДВ4; SSEP Antivirus – ТУ, НДВ4. Согласно сертификатам, данный продукт является средством защиты, которое может использоваться в автоматизированных системах до класса защищенности 1Г включительно и в системах обработки персональных данных до класса К1 включительно.

Решение может использоваться совместно с СЗИ от НСД Secret Net для обеспечения комплексной защиты автоматизированного рабочего места.

SSEP вошел в список рекомендуемых продуктов информационно-аналитического центра Anti-Malware.ru.

Коротко о TrustAccess

TrustAccess – распределенный межсетевой экран с централизованным управлением, агенты которого функционируют непосредственно на защищаемых компьютерах (серверах и рабочих станциях).

Основные возможности TrustAccess

TrustAccess имеет широкий функционал защиты сетевых соединений, который включает аутентификацию участников сетевых соединений, защиту трафика от подмены пакетов, гибкие настройки правил фильтрации и т.п. TrustAccess можно применять для защиты множества типов данных ограничен-

ного доступа (от защиты персональных данных до защиты гостайны). Защита TrustAccess эффективна в современных конфигурациях информационных систем. Например, в условиях терминальной или виртуальной среды.

Сертификаты

Продукт прошел сертификацию во ФСТЭК по уровню МЭ 2 и НДВ 4, что позволяет использовать его для защиты АС до класса 1Г включительно и для защиты ИСПДн до класса К1 включительно. Усиленная версия TrustAccess-S имеет сертификат ФСТЭК по уровню МЭ 2 и НДВ 2, что позволяет использовать ее также для защиты АС до класса 1Б включительно.

TrustAccess получил статус VMware Ready и был внесен в каталог партнерских продуктов VMware.

TrustAccess обладает статусами совместимости Microsoft Works with Windows Server 2008 R2 и Microsoft Works with Windows 7.



Код безопасности

ГК «Информзащита»

Почтовый адрес: 127018, Россия, Москва, а/я 55.

Адрес офиса в Москве: ул. Образцова, д. 38.

Адрес офиса в Санкт-Петербурге: Свердловская наб., д. 44.

Тел.: +7 (495) 980-2345 (многоканальный).

Факс: +7 (495) 980-2345.

E-mail: info@securitycode.ru

Запрос дополнительной информации о продуктах: info@securitycode.ru

По вопросам стоимости и покупки продуктов sales@securitycode.ru

По вопросам партнерства и сотрудничества info@securitycode.ru

Вы можете узнать подробную информацию о продуктах на сайте

www.securitycode.ru

О компании «Код Безопасности»

Компания «Код Безопасности» – российский разработчик программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям международных и отраслевых стандартов. Продукты «Кода Безопасности» применяются во всех областях информационной безопасности, таких как защита конфиденциальной информации, персональных данных, коммерческой и государственной тайны, а также среды виртуализации. «Код Безопасности» стремится предоставить клиентам качественные решения для любых задач информационной безопасности, как традиционных, так и появляющихся в процессе развития высоких технологий.

«Код Безопасности» входит в группу компаний «Информзащита», которая уже около 15 лет является лидером российского рынка информационной безопасности.

ООО «Код Безопасности» ведет свою деятельность на основании лицензий ФСТЭК России и ФСБ России.