



Решение SecureKiosk для безопасной передачи данных между доменами

secure
Kiosk

Организация удобного и безопасного файлового обмена между сегментами разного уровня доверия является важной задачей для большинства современных организаций со зрелым уровнем цифровизации бизнес-процессов. Типичными вариантами обмена данными между доменами являются: общие файловые серверы, файловые шлюзы, ручной перенос файлов на USB-накопителях. Однако, сопряжение сетей разного уровня доверия без предварительных проверок и только с применением программных средств может привести к несанкционированному доступу к критическим сегментам. Например, использование USB-накопителей требует их детального учета, исключения использования нелегитимных носителей, рисков вирусного заражения и утечек данных. Соответственно, этот вариант нельзя считать эффективным ни с точки зрения рисков ИБ, ни с точки зрения удобства. Решить эту задачу позволяют специальные комплексы, которые объединяют в своем составе два компонента: интерфейс для взаимодействия с пользователем для приема и передачи данных и систему передачи данных. Такие комплексы позволяют осуществлять передачу данных в строгом соответствии с установленными политиками безопасности.

Примером такого комплекса является **SecureKiosk** - физический киоск, который предоставляет пользователям «единое окно» для обмена данными. Он обеспечивает прием и передачу данных от пользователя, соблюдение политик обмена в отношении данных и фактов их передачи. На практике это означает, что USB накопители не перемещаются в более доверенную зону и не подключаются к доверенным устройствам, возможна передача только проверенных файлов с этих носителей. Проверка файлов выполняется, в том числе, с использованием внешних СЗИ (антивирусы, «песочницы», системы предотвращения утечек). Передача данных выполняется только в соответствии с принятыми политиками обмена. Передаются только файлы определенных типов, именований, только в определенное время. Обмен данными между доменами может выполняться с использованием различных систем передачи данных. Примерами таких систем могут быть межсетевые экраны или решения для физически однонаправленной передачи InfoDiode.



119121, Россия, Москва, Ружейный переулок, 6с1.

Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru

www.infodiode.ru

Общие сведения о SecureKiosk

SecureKiosk предназначен для удобной и безопасной передачи файлов между сегментами сети (доменами) с различными требованиями политик безопасности.

В комплексном решении SecureKiosk можно выделить два ключевых компонента:

- Точки доступа SecureKiosk - киоски, предоставляющие пользователям простой и понятный интерфейс передачи данных в иные сегменты в случае когда в организации применяются USB-накопители.
- Система передачи данных - механизм передачи данных между доменами. Системой передачи данных могут являться средства межсетевого экранирования или однонаправленные шлюзы (InfoDiode).

Защита доверенного сегмента при использовании SecureKiosk реализуется на нескольких уровнях:

- Доступ к пользовательским интерфейсам SecureKiosk осуществляется только после многошаговой аутентификации, USB-накопители и файлы на них проверяются на возможное вирусное заражение или признаки компрометации, а все действия пользователя записываются в журнал.
- Все передаваемые файлы проходят контроль на соблюдение политик безопасности передачи. Разрешаются к передаче файлы: определенных типов, именований, размеров. Передача разрешается с учетом интенсивности и в регламентированное время. Необходимым является получение вердикта от профильных СЗИ.
- В зависимости от модели угроз и нарушителя возможно использование базового уровня защиты (передача с использованием МСЭ) и усиленного уровня защиты (передача с использованием физически однонаправленных шлюзов InfoDiode).
- Может выполняться видео- и аудио- фиксация фактов пользования SecureKiosk.

Такой подход обеспечивает эшелонированную защиту доверенного сегмента от значительного количества угроз безопасности, исключает перемещение USB-носителей в доверенную зону и повышает доверие к передаваемым файлам.

SecureKiosk колонна

- Автономный киоск для безопасной передачи данных между доменами
- Экран 32" с разрешением 4K
- 1 порт USB Type A и 1 порт USB Type C
- Считыватель для SMART-карт и интеграция с СКУД организации
- Подключение к системе видеонаблюдения организации
- Проверка накопителя антивирусом
- Ограничения на передачу данных
- Интеграция с SIEM и LDAP



SecureKiosk настольный ПК

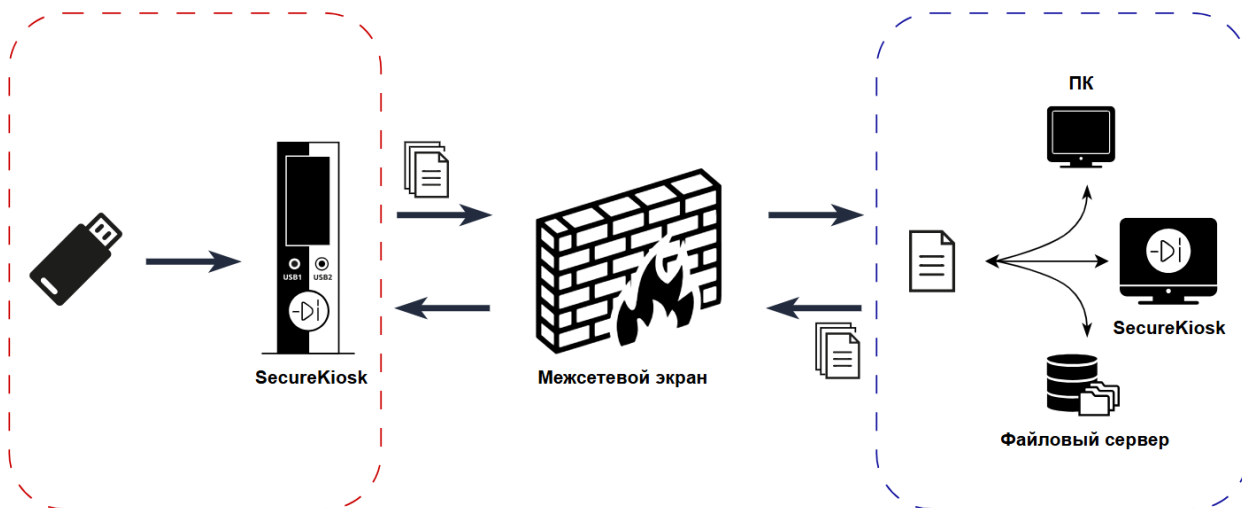
- Рабочее место сотрудника для безопасной передачи данных между доменами
- Экран 24" с разрешением FHD
- 1 порт USB Type A и 1 порт USB Type C
- Проверка накопителя антивирусом
- Ограничения на передачу данных
- Интеграция с SIEM и LDAP



Уровни защиты SecureKiosk

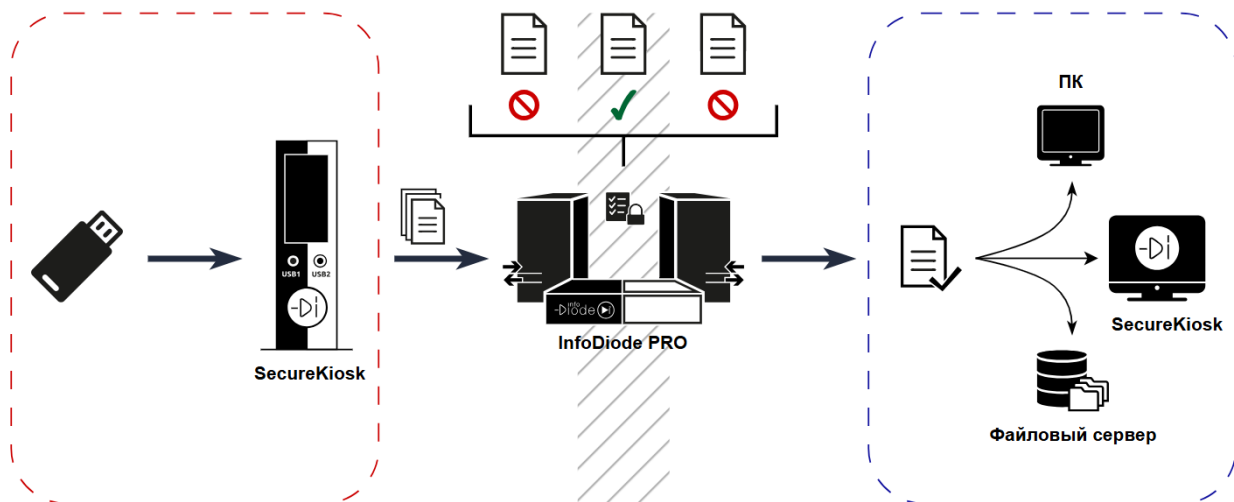
Базовый уровень защиты

В случае если в качестве системы передачи данных для SecureKiosk используются средства межсетевого экранирования, такой уровень защиты называется базовым. Он прост в реализации, хотя и не лишен недостатков за счет возможности эксплуатации злоумышленником двунаправленного канала для организации атаки на инфраструктуру организации и отсутствия детальных проверок файлов на системе передачи данных (МСЭ). Часто именно этот вариант используется как первый шаг к организации управляемого обмена данными.



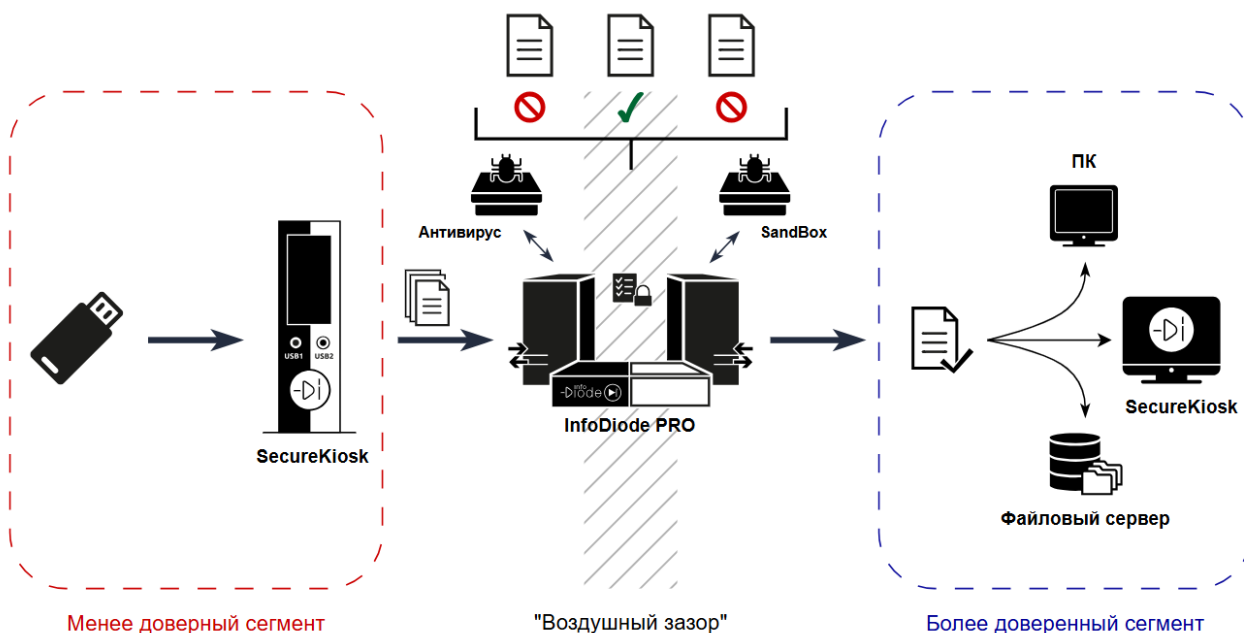
Усиленный уровень защиты

Усиленный уровень защиты предполагает, что в качестве системы передачи данных для SecureKiosk используется односторонний шлюз (InfoDiode), реализующий передачу данных с применением принципа «воздушного зазора». При таком сценарии передача сопровождается дополнительным контролем безопасности и проверками политик междоменного обмена. Использование «воздушного зазора» позволяет нейтрализовать множество удаленных атак на инфраструктуру организации даже в случае компрометации киоска данных и его политик. В случае применения усиленного уровня защиты на практике реализуется концепция «нулевого доверия» на четырех уровнях безопасности – нет доверия к пользователю, носителю информации, передаваемым файлам, сетевым соединениям.



Сценарии использования SecureKiosk

Основной сценарий — передача файлов в более доверенный сегмент



Такой сценарий использования SecureKiosk включает в себя следующие этапы:

1. Пользователь подходит к SecureKiosk и первично аутентифицируется на нем с помощью PIN-кода или SMART-карты.
2. Пользователь вставляет USB-накопитель в порт SecureKiosk, после чего накопитель проходит проверки целостности, наличия в черных/белых списках, вирусного заражения и др.
3. Пользователь проходит аутентификацию на InfoDiode PRO с помощью логина/пароля или SMART-карты для получения доступа к папкам получателя.
4. Пользователь выбирает папку получателя и файлы, которые необходимо передать, после чего запускает процесс передачи файлов.
5. Файлы передаются с USB-накопителя на прокси-сервер InfoDiode PRO, где проходят контроль на соблюдение политик безопасности передачи файлов по физически однонаправленному каналу.
6. При наличии подключенных к InfoDiode PRO профильных СЗИ осуществляется передача файлов в эти СЗИ, чтобы получить их решение о возможности передачи файлов в другой домен.
7. Успешно прошедшие все проверки безопасности файлы по физически однонаправленному каналу передаются в другой сегмент, где могут быть дополнительно проверены. Только после этого получатель сможет забрать переданные файлы, используя для этого другой киоск или штатно используемый ПК в доверенном сегменте.

Файлы, не прошедшие проверки безопасности, остаются в сегменте-источнике. Центр мониторинга информационной безопасности получает уведомления о выявлении нарушений политик безопасности как от SecureKiosk, так и от InfoDiode PRO. При выявлении угрозы безопасности высокой критичности SecureKiosk может автоматически блокироваться.

Данный сценарий SecureKiosk может применяться, например, для передачи файлов подрядчиков, контрагентов в технологический сегмент организации или передачи дистрибутивов программного обеспечения, обновлений или файлов конфигураций из сегмента разработки и тестирования в технологические сети. В качестве киоска могут быть использованы оба варианта исполнения: колонна, настольный ПК.



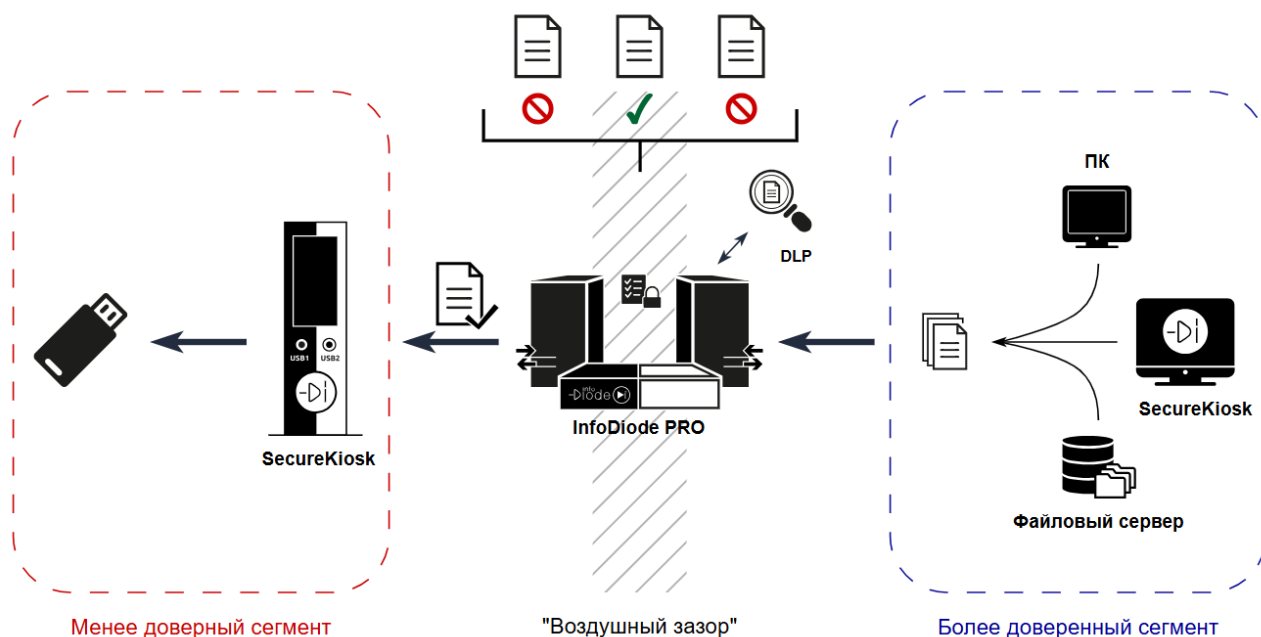
119121, Россия, Москва, Ружейный переулок, 6с1.

Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru

www.infodiode.ru

Сценарии использования SecureKiosk

Основной сценарий — получение файлов из более доверенного сегмента



Такой сценарий использования SecureKiosk включает в себя следующие этапы:

1. Отправитель аутентифицируется на InfoDiode PRO в более доверенном сегменте и передает файлы в менее доверенный сегмент.
2. Файлы проходят на InfoDiode PRO контроль за соблюдением политик безопасности передачи, осуществляется передача файлов в профильные СЗИ, например DLP-системы (при их наличии), чтобы получить их решение о возможности передачи файлов в другой домен.
3. Успешно прошедшие все проверки безопасности файлы по физически однонаправленному каналу передаются в другой сегмент, где могут быть дополнительно проверены. После этого переданные файлы ожидают получателя.
4. Получатель подходит к SecureKiosk и первично аутентифицируется на нем с помощью PIN-кода или SMART-карты.
5. Получатель подключает USB-накопитель к порту SecureKiosk, после чего накопитель проходит проверки целостности, наличия в черных/белых списках, вирусного заражения и др.
6. Получатель проходит дополнительную аутентификацию на InfoDiode PRO с помощью логина/пароля или SMART-карты для получения доступа к строго определенным ему папкам.
7. Получатель выбирает файлы, которые необходимо скачать, после чего запускает процесс передачи файлов на USB-накопитель.
8. После завершения передачи получатель извлекает USB-накопитель со скачанными файлами. При этом файлы на самом SecureKiosk, равно как во всей системе передачи, удаляются и недоступны другим пользователям и при последующих подключениях.

Файлы, не прошедшие проверки безопасности, остаются в сегменте-источнике. Центр мониторинга информационной безопасности получает уведомления о выявлении нарушений политик безопасности как от SecureKiosk, так и от InfoDiode PRO. При выявлении угрозы безопасности высокой критичности SecureKiosk может автоматически блокироваться.

Данный сценарий SecureKiosk может применяться, например, для выдачи документов или справок из корпоративной сети на удаленном объекте или выдачи медицинской документации по запросам пациентов. SecureKiosk в подходящем форм-факторе (колонна или настольный ПК) может использоваться на обеих сторонах системы передачи данных.



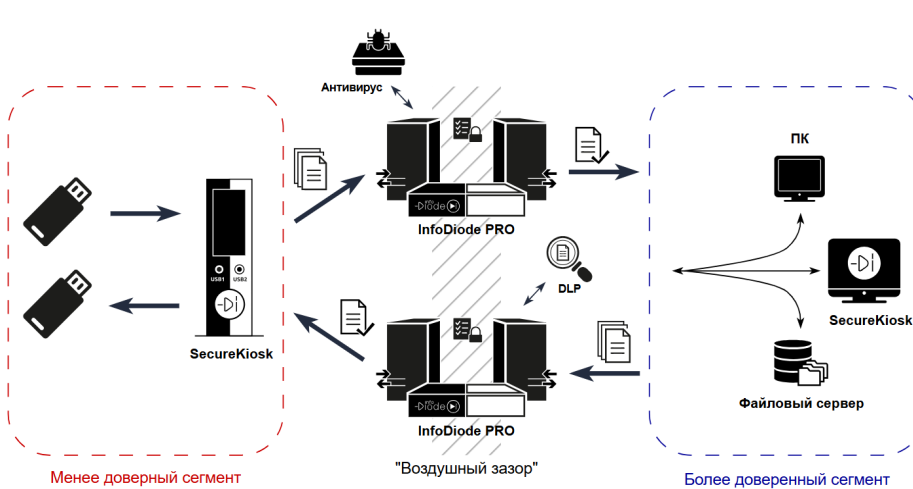
119121, Россия, Москва, Ружейный переулок, 6с1.

Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru

www.infodiode.ru

Сценарии использования SecureKiosk

Дополнительные сценарии



SecureKiosk может применяться для одновременной передачи и приема данных через единое устройство.

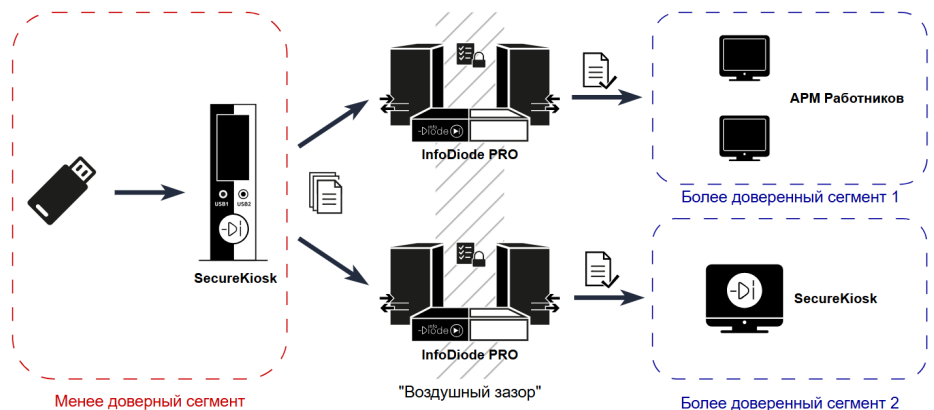
Примером такого обмена может выступать обмен документацией между клиентами и/или подрядчиками и работниками организации.

Использование двух разнонаправленных InfoDiode PRO за счет разрыва двунаправленных сетевых протоколов гарантирует невозможность проведения удаленных атак даже в случае компрометации SecureKiosk.

SecureKiosk может применяться для передачи данных в несколько сетевых сегментов с различным уровнем доверия.

Примером может выступать единое устройство, через которое возможна передача документов в корпоративный сегмент на АРМ работников, а также доставка обновлений от подрядчиков в технологическую сеть.

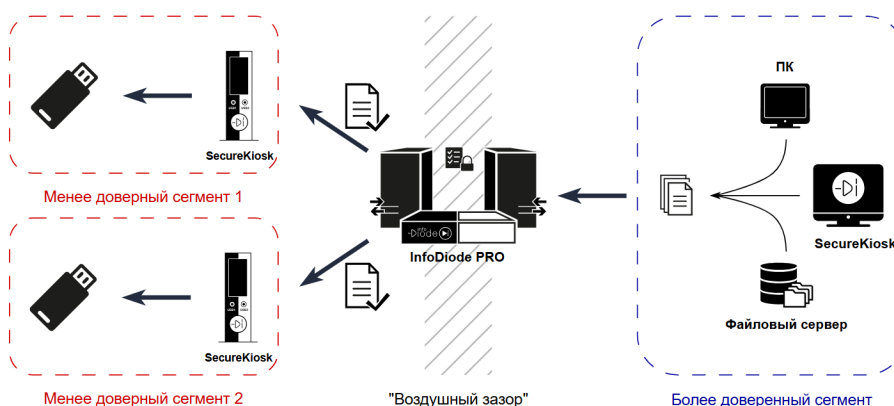
Использование двух InfoDiode PRO за счет «воздушного зазора» гарантирует невозможность сопряжения сетей двух более доверенных сегментов.



SecureKiosk может применяться для передачи данных на несколько физически удаленных объектов через единый центр контроля передачи данных.

Примером такого обмена может выступать выдача документов и справок работникам на различные удаленные объекты — предприятия, заводы и т.д.

Использование InfoDiode PRO за счет «воздушного зазора» гарантирует невозможность удаленных атак на корпоративный сегмент даже в случае компрометации SecureKiosk, а также обеспечивает единые политики контроля для всех передаваемых данных.



119121, Россия, Москва, Ружейный переулок, 6с1.

Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru

www.infodiode.ru

Технические характеристики SecureKiosk

Характеристики	AMTSK-1000-TWR	AMTSK-1000-DT	AMTSK-1000-TWR-L	AMTSK-1000-DT-L
Варианты исполнения	Колонна	Настольный ПК/ Моноблок	Колонна	Настольный ПК/ Моноблок
Уровень защиты	Усиленный	Усиленный	Базовый	Базовый
Экран	32", 2160x3840, сенсорный	24", 1920x1080	32", 2160x3840, сенсорный	24", 1920x1080
Проверки носителя	Целостность файловой системы, белый список, антивирус	Целостность файловой системы, белый список, антивирус	Целостность файловой системы, белый список, антивирус	Целостность файловой системы, белый список, антивирус
Проверки при передаче данных	Антивирус, DLP, Sandbox, именование, интенсивность, размер, тип, регламентное время передачи	Антивирус, DLP, Sandbox, именование, интенсивность, размер, тип, регламентное время передачи	размер, тип, именование, регламентное время передачи	размер, тип, именование, регламентное время передачи
Система передачи данных (не входит в комплект поставки)	междоменное решение InfoDiode (физически однонаправленный канал)	междоменное решение InfoDiode (физически однонаправленный канал)	межсетевой экран	межсетевой экран
Скорость передачи данных	300 Mbps	300 Mbps	1 Gbps	1 Gbps
Порты для подключения носителей информации	1x USB type A, 1x USB type C	1x USB type A, 1x USB type C	1x USB type A, 1x USB type C	1x USB type A, 1x USB type C
Температура	от +10 до +35	от +10 до +35	от +10 до +35	от +10 до +35
Рабочая влажность воздуха	5 – 95 %	5 – 95 %	5 – 95 %	5 – 95 %
Электропитание	100 – 240 В (AC)	100 – 240 В (AC)	100 – 240 В (AC)	100 – 240 В (AC)
Размеры, ШxВxГ, мм	580x1920x135	541x324x55	580x1920x135	541x324x55
Вес, кг	75 (без монтажного основания)	7,5	75 (без монтажного основания)	7,5

Спецификации для заказа SecureKiosk*

Код продукта	Описание
AMTSK-1000-TWR	Автономный киоск (колонна) для передачи данных между доменами в составе междоменного решения InfoDiode
AMTSK-1000-DT	Рабочее место сотрудника (настольный ПК/моноблок) для передачи данных между доменами в составе междоменного решения InfoDiode
AMTSK-1000-TWR-L	Автономный киоск (колонна) для передачи данных между доменами средствами межсетевого экранирования (лицензии на операционную систему и антивирус не входят в комплект поставки)
AMTSK-1000-DT-L	Рабочее место сотрудника (настольный ПК/моноблок) для передачи данных между доменами в условиях организации передачи средствами межсетевого экранирования (лицензии на операционную систему и антивирус не входят в комплект поставки)

* Цены на указанные в таблице продукты предоставляются по запросу, при обращении на InfoDiode@amt.ru



119121, Россия, Москва, Ружейный переулок, 6с1.
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru

www.infodiode.ru