Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Сибирский государственный автомобильно-дорожный университет (СибАДИ)»

Институт Информационные системы, экономика и управление

Кафедра Информационная безопасность

Направление Информационная безопасность

Профиль Безопасность автоматизированных системы

**ПОЯСНИТЕЛЬНАЯ ЗАПИСКА**

**к курсовому проекту**

по дисциплине: «Защита информации от утечки по техническим каналам»

Тема работы «Анализ российского рынка средств обеспечения информационной безопасности беспроводных сетей»

Выполнил:

студент группы БИб-21Э1 Парфёнов Александр Романович

Курсовой проект сдан на проверку:

«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_2023 г.

Студент \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Парфёнов Александр Романович

(подпись студента)

Курсовой проект допущен к защите:

«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_2023 г.

Руководитель работы

доцент, канд. техн. наук \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.В. Пролубников

(подпись преподавателя)

Курсовой проект защищен с оценкой:

«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_2023 г.

Руководитель работы

доцент, канд. техн. наук \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.В. Пролубников

Омск 2023

Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Сибирский государственный автомобильно-дорожный университет (СибАДИ)»

Кафедра «Информационная безопасность»

УТВЕРЖДАЮ

Зав. кафедрой ИБ, д.п.н., проф.

\_\_\_\_\_\_\_\_\_\_\_\_\_ Д.А. Панков

«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 2023 г.

**ЗАДАНИЕ**

**к курсовой работе**

студенту группы БИб-21Э1 Парфёнову Александру Романовичу

1. Тема курсовому проекту: «Анализ российского рынка средств обеспечения информационной безопасности беспроводных сетей»
2. Содержание пояснительной записки:

* титульный лист;
* задание к курсовому проекту;
* содержание;
* введение;
* теоретический раздел;
* практический раздел;
* заключение;
* список использованных источников.

1. Срок сдачи работы: « » 2023 г.

Задание выдано « » 2023 г.

Руководитель работы: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.В. Пролубников

(подпись преподавателя)

Задание к исполнению принял « » 2023 г.

Студент \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.Р. Парфёнов

(подпись студента)

**Содержание**

[Введение 4](#_Toc153594124)

[1 ОСНОВНЫЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ БЕСПРОВОДНЫХ СЕТЕЙ 5](#_Toc153594125)

[1.1 Угрозы беспроводных технологий 5](#_Toc153594126)

[«Человек посередине» 6](#_Toc153594127)

[DDoS-атаки 6](#_Toc153594128)

[Ложная точка доступа 7](#_Toc153594129)

[Атаки на сетевое оборудование 7](#_Toc153594130)

[1.2 Стандарты беспроводных сетей 7](#_Toc153594131)

[1.3 Методы контроля безопасности 9](#_Toc153594132)

[2 УСТРОЙСТВА ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ БЕСПРОВОДНЫХ СЕТЕЙ НА РОССИЙСКОМ РЫНКЕ 11](#_Toc153594133)

[2.1 Обзор и сравнение межсетевых экранов отечественных производителей 11](#_Toc153594134)

[1.   Межсетевые экраны Diamond 12](#_Toc153594135)

[2. Межсетевые экраны DIONIS DPS 14](#_Toc153594136)

[3. Межсетевые экраны «Континент» 16](#_Toc153594137)

[4. Межсетевые экраны «Рубикон» 18](#_Toc153594138)

[5. Межсетевые экраны UserGate 20](#_Toc153594139)

[6. Межсетевые экраны Ideco 21](#_Toc153594140)

[Выводы 22](#_Toc153594141)

[2.2 (еще устройства с российского рынка) 23](#_Toc153594142)

[2.3 Программно-аппаратные комплексы защиты 23](#_Toc153594143)

[3 ………………(что-то типо сравнительной характеристики устройств) 23](#_Toc153594144)

[Заключение 24](#_Toc153594145)

[Список использованных источников 25](#_Toc153594146)

# **Введение**

В современном мире беспроводные сети стали неотъемлемой частью нашей повседневной жизни. Они позволяют нам подключаться к интернету, обмениваться данными и взаимодействовать с другими устройствами без необходимости использования проводов. Однако, с развитием беспроводных технологий возникают и новые угрозы безопасности.

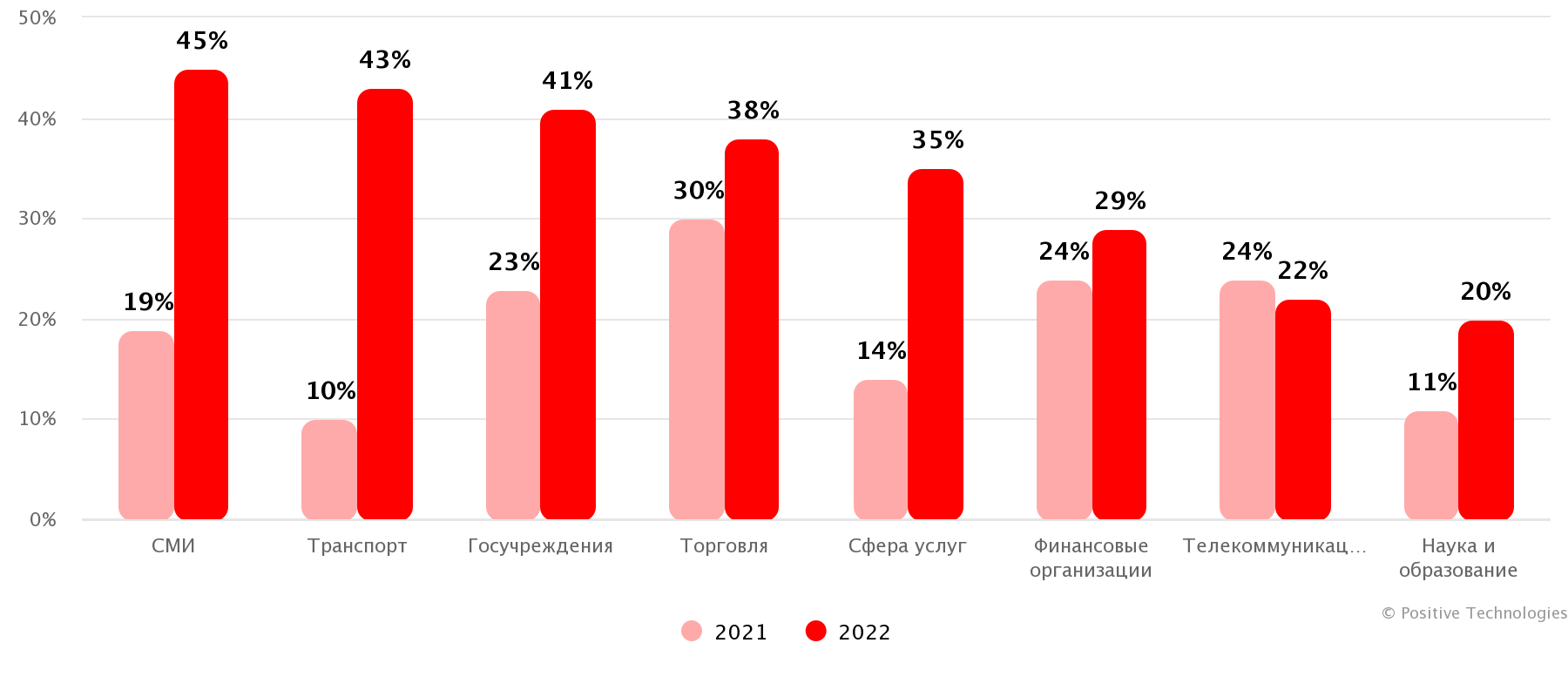
**Цель работы**: Проанализировать средства обеспечения информационной безопасности беспроводных сетей на Российском рынке.

Для достижения поставленной цели необходимо решить следующие **задачи**:

1. Собрать данные об основных средствах обеспечения безопасности беспроводных сетей.
2. Исследовать российские компании, разрабатывающие средства обеспечения информационной безопасности беспроводных сетей.
3. Выполнить сравнительный анализ устройств обеспечения безопасности сетей российского рынка.

# **ОСНОВНЫЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ БЕСПРОВОДНЫХ СЕТЕЙ**

Обеспечение информационной безопасности беспроводных сетей является важным аспектом в современном мире, где беспроводные технологии широко используются в различных сферах. Количество атак растет с каждым годом (Рисунок 1), поэтому необходимо предпринимать меры для их устранения.

*Рисунок 1. Доля инцидентов, связанных с атаками на веб-ресурсы в 2021 и 2022 годах*

# **1.1 Угрозы беспроводных технологий**

Существенные проблемы безопасности беспроводных сетей, несмотря на их существенные плюсы, является одним из основных их недостатков. В этом плане они намного уступают проводному соединению. Это связано с тем, что для взлома проводной сети злоумышленнику необходим непосредственный доступ к кабелю, получить который намного сложнее, чем перехватить радиосигнал при помощи специальных устройств. Кроме того, часто беспроводные сети работают даже без элементарной защиты паролем.

Получение доступа к локальной беспроводной сети дает злоумышленникам возможности похищения конфиденциальной информации и персональных данных, распространения вредоносного ПО, для других манипуляций.

Различают несколько основных видов атак, которые угрожают безопасности беспроводных компьютерных сетей:

* «человек посередине»;
* DDoS-атаки;
* ложная точка доступа;
* атаки на сетевое оборудование.

Каждый из этих типов может применяться хакерами в определенных условиях с разными целями.

### «Человек посередине»

«Человек посередине», или Man-in-the-Middle, относится числу наиболее распространенных типов атак. Этот способ чаще всего применяется для подключения к точкам доступа, не защищенным паролем. Поскольку сигнал в таких сетях транслируется без шифрования, злоумышленник может легко перехватывать его при помощи обычного ноутбука или компьютера с адаптером Wi-Fi. Однако возможно хакер может подключиться и к запаролированной сети при помощи специальной программы для взлома паролей методом подбора.

Атаки типа Man-in-the-Middle в свою очередь подразделяются на два вида — подслушивание и манипуляция.

«Подслушивание» называют еще пассивной атакой. Оно выполняется при помощи специального программного обеспечения, которое после получения доступа в локальную сеть отображает на компьютере злоумышленника весь трафик пользователя. Это может быть история посещения сайтов, вводимые логины и пароли, данные пластиковых карт и другая конфиденциальная информация.

Атаки типа «Манипуляция» называют активными. В этом случая хакер получает возможность не только кражи персональных данных пользователя, но и манипуляции его устройством через беспроводную сеть. Например, при помощи специального ПО на компьютер пользователя может быть отправлена от имени точки доступа команда переадресации браузера на определенную страницу в интернете. На этой страницы компьютер заражается вирусами или другими вредоносным программным обеспечением.

### DDoS-атаки

Еще одним распространенным типом угроз, которые необходимо учитывать в стандартах безопасности беспроводных сетей, являются DDoS-атаки, или отказ в обслуживании. Целью злоумышленников является нарушение работы локальной сети, при котором ее невозможно полноценно использовать. Атака может производится на программном и на аппаратном уровне. В первом случае хакеры используют существующие уязвимости в программном обеспечении. Атака на аппаратном уровне выполняется за счет переполнения системы запросами, что приводит к исчерпанию ее ресурсов (дискового пространства, процессорного времени, пропускной способности и т. д.).

DDoS-атаки на программном уровне чаще всего выполняются за счет уязвимостей в протоколе. Они могут приводить к полной потере работоспособности подключенного к сети устройства. Например, может зависать компьютер, изменяются конфигурации операционной системы, или она получает повреждения.

При атаках на аппаратном уровне злоумышленник стремится добиться неработоспособности канала связи. Это достигается за счет направления массивных потоков бессмысленных данных, перегружающих канал, или созданием мощных помех. Помехи создаются при помощи специальных генераторов электромагнитного излучения.

### Ложная точка доступа

Этот тип атак применяется злоумышленниками в местах, где действует общественная точка доступа, например, в кафе, в транспорте и т. д. Хакер через смартфон или ноутбук создает незапаролированную точку доступа, которая маскируется под легальную. Пользователи при попытке подключения к общественному Wi-Fi, видят в списке доступных сетей ложную точку доступа и подключаются к ней. В результате злоумышленник перехватывает весь передаваемый трафик, включая конфиденциальные данные.

Часто нарушители, использующие ложные точки, могут подавлять сигнал легальной точки доступа при помощи специального оборудования. Это значительно увеличивает количество подключений жертв.

### Атаки на сетевое оборудование

Точки доступа и другое сетевое оборудование с неправильно выстроенной конфигурацией и недостаточно эффективной защитой часто становится каналом для проникновения хакеров в локальную беспроводную сеть. Более того, беспроводные сети в конечном итоге, как правило, коммутируются с проводными. Поэтому взлом сетевого оборудования создает угрозу безопасности и проводных сетей.

# **1.2 Стандарты беспроводных сетей**

**Беспроводные компьютерные сети —** это технология, позволяющая создавать вычислительные сети, полностью соответствующие стандартам для обычных проводных сетей (например, Ethernet), без использования кабельной проводки. В качестве носителя информации в таких сетях выступают радиоволны СВЧ-диапазона.  
  
**Беспроводные технологии —** подкласс информационных технологий, служат для передачи информации на расстояние между двумя и более точками, не требуя связи их проводами. Для передачи информации может использоваться инфракрасное излучение, радиоволны, оптическое или лазерное излучение.  
  
В настоящее время существует множество беспроводных технологий, наиболее часто известных пользователям по их маркетинговым названиям, таким как Wi-Fi, WiMAX, Bluetooth. Каждая технология обладает определёнными характеристиками, которые определяют её область применения. (<https://it-wr.ru/support/spravochnik/technology/standarty-besprovodnyh-setej>)

Существуют различные подходы к классификации беспроводных технологий.

**Наиболее распространенные стандарты беспроводных сетей**

Стандарты беспроводных сетей - это наборы технических спецификаций и правил, которые определяют, как устройства должны взаимодействовать в радиоволновой среде для обеспечения беспроводной связи.

Эти стандарты определяют как физический, так и логический уровни связи, что включает в себя методы модуляции, спектральное распределение сигнала, протоколы управления доступом к среде, а также форматы данных и протоколы для передачи информации.

Стандарты беспроводных сетей служат основой для различных беспроводных технологий и применяются в разных сферах, включая беспроводные локальные сети (Wi-Fi), мобильную связь (3G, 4G, 5G), беспроводные сенсорные сети, беспилотные авиационные системы (дроны) и многие другие области.

Эти стандарты разрабатываются различными стандартизационными организациями, такими как IEEE (Институт инженеров по электротехнике и электронике), 3GPP (3rd Generation Partnership Project), Bluetooth SIG (Special Interest Group), и другими.

Стандарты беспроводных сетей обеспечивают совместимость и интероперабельность между различными устройствами и сетями, позволяя им успешно взаимодействовать и обмениваться данными.

Давайте рассмотрим некоторые из наиболее распространенных стандартов беспроводных сетей и их значение.

* **Wi-Fi (802.11).**Этот стандарт является основой для беспроводной связи в домах, офисах, общественных местах и даже на улицах. Стандарт 802.11 предлагает различные версии, такие как 802.11n, 802.11ac и 802.11ax, которые предоставляют разные скорости передачи данных и характеристики. Wi-Fi позволяет мобильным устройствам подключаться к Интернету и локальным сетям с высокой скоростью и без необходимости использования проводов.
* **Bluetooth.** Стандарт Bluetooth предназначен для ближней беспроводной связи между устройствами. Это позволяет смартфонам и другим устройствам обмениваться данными, управлять аксессуарами, такими как наушники или гарнитура, и даже управлять умными домашними устройствами. Bluetooth также используется для передачи аудио-сигнала на беспроводные наушники и гарнитуры.
* **3G, 4G, 5G**. Эти стандарты относятся к мобильной связи и предназначены для передачи данных по мобильным сетям. 3G (третье поколение) был первым, кто предложил высокоскоростной доступ к Интернету с мобильных устройств. 4G (четвертое поколение) значительно увеличило скорость передачи данных, что позволило потоковое воспроизведение видео и другие приложения высокой пропускной способности. 5G (пятое поколение) обещает еще более высокую скорость и низкую задержку, что сделает возможным впечатляющие новые приложения, такие как расширенная реальность (AR) и многие другие.
* **NFC (Near Field Communication).** NFC - это стандарт для ближней беспроводной связи, который позволяет устройствам обмениваться данными на краткое расстояние, обычно менее 4 см. Этот стандарт активно используется для бесконтактных платежей, передачи данных между устройствами и других задач, где важна близкая связь.

(https://electricalschool.info/spravochnik/poleznoe/2917-standarty-besprovodnyh-setey.html)

# **1.3 Методы контроля безопасности**

1. Шифрование данных:

WPA3 (Wi-Fi Protected Access 3): Это последний стандарт протокола безопасности для Wi-Fi, который предоставляет более сильное шифрование данных по сравнению с предыдущим стандартом WPA2.(Больше инфы + ссылка)

VPN (Virtual Private Network): Использование VPN может обеспечить шифрование данных в беспроводной сети, что делает их более защищенными от несанкционированного доступа. (Больше инфы + ссылка)

1. Аутентификация:

802.1X (Extensible Authentication Protocol): Этот протокол обеспечивает механизм аутентификации пользователей в беспроводных сетях, предоставляя контроль доступа к сети на основе учетных данных. (Больше инфы + ссылка)

MAC-фильтрация: Позволяет разрешать или блокировать доступ к беспроводной сети на основе физического адреса устройства. (Больше инфы + ссылка)

1. Средства мониторинга и обнаружения угроз:

Intrusion Detection Systems (IDS) и Intrusion Prevention Systems (IPS): Эти системы могут мониторить беспроводную сеть на наличие аномальной активности и принимать меры для предотвращения атак. (Больше инфы + ссылка)

Wi-Fi анализаторы: Позволяют обнаруживать и анализировать активность в беспроводной сети, включая несанкционированные устройства и подключения. (Больше инфы + ссылка)

1. Физическая безопасность:

Ограничение доступа к оборудованию: Физическое обеспечение безопасности маршрутизаторов, точек доступа и другого оборудования, чтобы предотвратить несанкционированный доступ. (Больше инфы + ссылка)

Географическое ограничение сети (Geofencing): Ограничение доступа к сети на основе физического местоположения устройства. (Больше инфы + ссылка)

1. Обновления и патчи:

Регулярные обновления программного обеспечения: Обновление маршрутизаторов, точек доступа и другого оборудования с целью устранения уязвимостей и обеспечения безопасности. (Больше инфы + ссылка)

1. Обучение пользователей:

Создание политик безопасности: Разработка и внедрение правил безопасности для пользователей беспроводных сетей, включая регулярные смены паролей и использование сложных паролей. (Больше инфы + ссылка)

1. Физическая безопасность сети:

Разделение сетей (VLANs): Создание виртуальных локальных сетей для разделения трафика и повышения безопасности сети. (Больше инфы + ссылка)

1. Фильтрация MAC-адресов:

Ограничьте доступ к беспроводной сети, разрешая только определенным устройствам, чьи MAC-адреса заранее известны. (Больше инфы + ссылка)

1. VPN (Virtual Private Network):

Использование VPN для шифрования трафика между устройством и точкой доступа может усилить безопасность, особенно при использовании открытых Wi-Fi сетей. (Больше инфы + ссылка)

1. Firewall:

Настройте брандмауэр для контроля трафика между беспроводными устройствами и сетью. (Больше инфы + ссылка)

# **2 УСТРОЙСТВА ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ БЕСПРОВОДНЫХ СЕТЕЙ НА РОССИЙСКОМ РЫНКЕ**

# **2.1 Обзор и сравнение межсетевых экранов отечественных производителей**

(https://habr.com/ru/articles/726662/)

Не так давно на рынке средств ИБ появились межсетевые экраны нового поколения (Next-Generation Firewall, NGFW), которые кроме основных функций брандмауэра имеют еще и дополнительные функции, такие как:

* контроль приложений;
* DPI (Deep Packet Inspection, проверка пакетов на уровне приложений);
* IPS (предотвращение вторжений);
* веб‑фильтрация (контроль URL‑адресов, к которым обращаются пользователи);
* аутентификация пользователей.

В связи с развитием программы импортозамещения и уходом некоторых зарубежных компаний из нашей страны, на рынке появились отечественные модели МЭ, которые соответствуют всем современным критериям качества.

При выборе МЭ для своей компании следует рассмотреть также такие факторы, как наличие сертификатов ФСТЭК, ФСБ и Минобороны РФ. Ведь для выполнения некоторых задач (к примеру, для работы с государственными системами или на объектах критической информационной инфраструктуры — КИИ) важно установить именно сертифицированный межсетевой экран.

В этой статье [мы рассмотрим следующие межсетевые экраны](https://global-it.ru/) отечественных брендов: Diamond, DIONIS DPS, «Континент», «Рубикон», UserGate и Ideco.

Надо отметить, что модельный ряд у некоторых производителей отечественных МЭ достаточно большой, он включает, как программные межсетевые экраны, так и аппаратные МЭ. В нашем обзоре мы будем рассматривать российские межсетевые экраны для среднего бизнеса и корпоративного сектора. В таблицах сравнения будут участвовать только аппаратные межсетевые экраны.

Итак, я выбрал следующие параметры для сравнения:

* Количество пользователей максимальное;
* Трафик EMIX (Enterprise Mix, усредненный корпоративный трафик) в режиме МЭ;
* Трафик EMIX в режиме контентной фильтрации;
* Трафик EMIX в режиме контроля приложений;
* Трафик EMIX в режиме предотвращения вторжений;
* Трафик EMIX в режиме NGFW (IPS, контент‑фильтр, контроль приложений, межсетевой экран).

Также в таблицах будут указаны базовые технические характеристики аппаратных МЭ (процессор, оперативная память, хранилище, сетевые адаптеры, источник питания, форм-фактор, размеры и масса изделия). В обзоре мы обязательно укажем наличие сертификатов ФСТЭК, ФСБ и Минобороны РФ.

Надо отметить, что не все производители предоставляют такую подробную техническую информацию в открытом доступе, но мы постарались собрать и проанализировать наиболее полные данные о российских межсетевых экранах.

### 1.   Межсетевые экраны Diamond



МЭ Diamond серии 7000

Для начала рассмотрим межсетевые экраны Diamond от российского производителя ООО «ТСС». Компания разрабатывает [МЭ семейства Diamond](http://diamond-fw.ru/) с целью комплексного обеспечения информационной безопасности. Данные МЭ позволяют решать задачи шифрования высокоскоростных каналов связи, межсетевого экранирования, а также обнаружения и предотвращения вторжений. Межсетевые экраны от ООО «ТСС» имеют сертификаты ФСТЭК и ФСБ.

Основные функции многофункционального комплекса сетевой защиты Diamond VPN/FW (МКСЗ «Diamond VPN/FW»):

* криптографическая защита каналов передачи данных (L2overVPN/L3overVPN) с применением отечественных криптографических алгоритмов;
* межсетевое экранирование в режиме коммутатора (прозрачный режим) и в режиме маршрутизатора;
* система обнаружения и предотвращения вторжений (СОВ/СПВ).

МЭ Diamond имеют аппаратное исполнение, могут быть интегрированы в любую сетевую инфраструктуру предприятия. Аппаратные межсетевые экраны «Diamond VPN/FW» разбиты на серии с похожими техническими характеристиками в зависимости от архитектуры процессора и скорости выполнения функций средств защиты. Производитель выпускает серии с номерами 1-7 на аппаратной платформе с архитектурой процессора x86. Также есть еще и специализированные серии под номером 0 и 10. В нашей таблице сравнения мы будем рассматривать серии 4-7, которые предназначены для обеспечения безопасности предприятий среднего и корпоративного бизнеса. Надо отметить, что МЭ 3-7 и 10 серии имеют стоечное исполнение.

Какие же преимущества есть у межсетевых экранов Diamond:

* высокая скорость шифрования;
* низкая вносимая задержка до 2 мс;
* высокая надежность компонентов и их резервирование;
* максимальная плотность портов (6-я и 7-я серии);
* четыре дополнительных модуля расширения (6-я и 7-я серии);
* высокая доступность и масштабируемость.

Обеспечение защиты информации в каналах связи от неправомерного доступа и модифицирования производится с помощью Dcrypt (СКЗИ «Dcrypt 1.0 v2»), которое является сертифицированным СКЗИ.

МЭ Diamond VPN/FW поддерживают возможность фильтрации сетевого трафика по основным полям сетевого пакета, производят фильтрацию по доменным именам, по расписанию, логирование правил фильтрации, синхронизацию правил фильтрации с другими устройствами. Производителем заявлена возможность агрегации правил фильтрации в группы и создание правил фильтрации с абстракциями различной сложности.

Устройства из 2-7 серий «Dimond VPN/FW» поддерживают встроенный механизм обнаружения и предотвращения вторжений. В результате чего сетевые пакеты подвергаются глубокому анализу с целью выявить различного рода аномалии в сетевом трафике.

«Dimond VPN/FW» является отказоустойчивым решением и позволяет обеспечить непрерывность бизнеса при различных сценариях. МКСЗ «Diamond VPN/FW» позволяет осуществлять маркировку, приоритезацию и шейпинг сетевого трафика по различным критериям. Также устройства «Dimond VPN/FW» могут работать в режиме маршрутизатора, коммутатора и поддерживают большое количество дополнительных функций и механизмов, которые упрощают сетевое администрирование. Ниже в табл. 1 приведено сравнение моделей МЭ Dimond VPN/FW 4-7 серий.

Таблица 1. Cравнение моделей МЭ Dimond VPN/FW 4-7 серий.

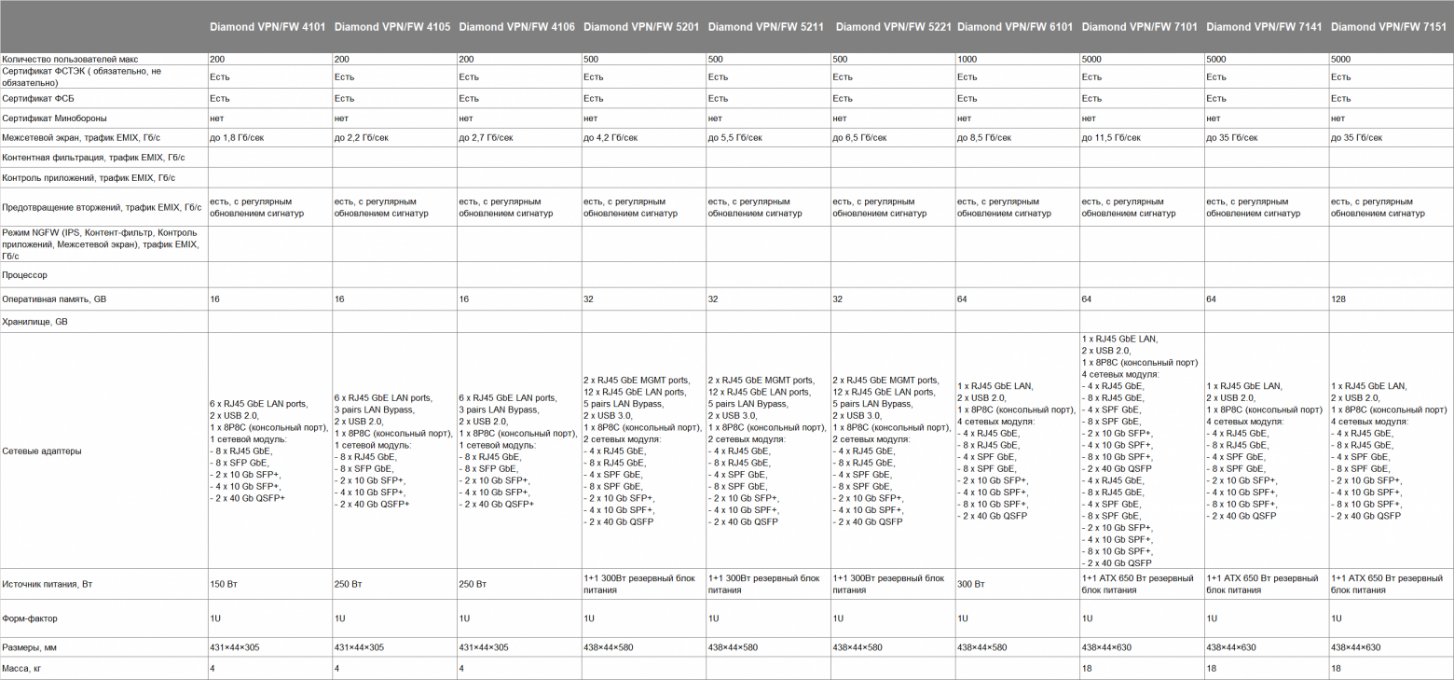


Таблица 1

### 2. Межсетевые экраны DIONIS DPS



МЭ dionis серии 5000

Следующей позицией в нашем обзоре российских межсетевых экранов будут [МЭ DIONIS DPS](https://dionis-dps.ru/) производства компании Фактор-ТС. Cразу отметим, что эти межсетевые экраны сертифицированы ФСБ, ФСТЭК. Dionis DPS является межсетевым экраном и криптошлюзом и предназначен для работы с персональными данными в корпоративном секторе и государственных организациях. Также данный МЭ имеет встроенную систему обнаружения и предотвращения вторжений IPS/IDS базе Snort, которая сертифицирована ФСБ. Система может работать в следующих режимах:

* в режиме только обнаружения атаки;
* в режиме обнаружения и предотвращения атаки.

Производитель предусмотрел в системе возможность поддержки создания собственных правил анализа трафика и запись дампов трафика, распознанного как атака. Управлять такой системой, а также получать статистику атак возможно через портал управления безопасностью Dionis-SMP. Ниже отметим базовые возможности сертифицированных межсетевых экранов Dionis DPS:

* работа в режиме межсетевого экрана и маршрутизатора;
* возможность организации криптографически защищенных VPN;
* работа в режиме межсетевого экрана и криптошлюза (класс защищенности КС1, КС3, сертификат ФСБ);
* работа в режиме МЭ (сертификация ФСТЭК, МЭ2/МЭ4), контроль сессий, NAT/PAT;
* работа в режиме системы обнаружения и предотвращения вторжений IDS/IPS (сертификация ФСТЭК СОВ2/СОВ4) с возможностью централизованного управления;
* поддержка QoS, управление качеством сервисов, ограничение и гарантирование полосы пропускания, PROXY, DHCP, NTP‑сервер;
* высокая надежность и отказоустойчивость;
* поддержка средств мониторинга и диагностики, оповещения администратора сети.

В нашей таблице сравнения рассмотрим МЭ серии DIONIS DPS 3000 и DIONIS DPS 4000, которые предназначены для среднего бизнеса и позволяют подключать до 200 и 400 пользователей соответственно. С помощью модульной системы и поддержки интерфейсов SFP+ (10G) эти модели возможно интегрировать в существующие высокопроизводительные сети. На базе моделей Dionis-DPS серии 3000/4000 (в качестве маршрутизаторов) есть возможность построения небольшого ядра сети предприятия. Маршрутизаторы Dionis-DPS работают под управлением операционной системы Dionis NX 2.0

Также в нашем сравнении будем рассматривать и старшие модели DIONIS DPS 5000, DIONOIS DPS 6000, DIONIS DPS 7000, основное предназначение которых — работа в центрах обработки данных и ключевых высокопроизводительных узлах сети крупных компаний. Максимальное количество пользователей для старших моделей — 1000, 1500 и 2000 соответственно. С помощью резервирования источника питания в сочетании с отказоустойчивым кластером возможно обеспечить высокий уровень надежности ядра сети крупной организации.

Компания Фактор-ТС производит и младшие модели МЭ DIONIS DPS 1000 и DIONIS DPS 2000, которые предназначены для использования в компаниях малого бизнеса. Несмотря на небольшое количество пользователей, которых можно подключить к данным моделям (DIONIS DPS 2000 — 100 пользователей), МЭ DIONIS DPS 1000 и DIONIS DPS 2000 поддерживают основной функционал средних и старших моделей, а именно: функции маршрутизатора, детектора атак, криптошлюза. В таблице сравнения мы не будем рассматривать младшие модели DIONIS DPS.

Таблица 2. Cравнение моделей МЭ DIONIS DPS 3000, 4000, 5000, 6000, 7000.



Таблица 2

### 3. Межсетевые экраны «Континент»



МЭ Континент 3, серия 1000F

В данном разделе нашей статьи рассмотрим продукцию компании «Код безопасности», которая уже 30 лет работает на российском рынке и имеет огромный опыт по внедрению средств ИБ.[Аппаратные межсетевые экраны](https://kontinent-ipc.ru/) этой компании представлены двумя линейками — Континент 3 и Континент 4. В каждой линейке идет подразделение на МЭ базовой производительности, средней производительности, высокой производительности. В линейке Континент 3 есть еще МЭ для крупных ЦОДов, а в Континент 4 — модели с виртуальным исполнением. В нашем обзоре мы рассмотрим наиболее производительные модели только аппаратных межсетевых экранов в линейках Континент 3 и Континент 4.

Надо отметить, что продукция Континент имеет сертификаты ФСТЭК, а линейка МЭ Континент 3 имеет также сертификаты ФСБ и Минобороны России.

Основной функционал Континент 3:

* криптографическая защита трафика на канальном уровне (L2 VPN‑сеть);
* защита трафика на сетевом уровне (L3 VPN‑сеть);
* маршрутизация трафика;
* режим работы МЭ;
* высокая отказоустойчивость серверов управления;
* анализ сетевого трафика, обнаружение и предотвращение атак;
* мониторинг всех компонентов;
* защита удаленного подключения.

МЭ Континент 3 рекомендуются для защиты государственных информационных систем, финансовых систем, критической информационной инфраструктуры (КИИ), защиты информации в здравоохранении, обеспечения безопасности персональных данных. С помощью моделей МЭ Континент 3 можно построить защищенную корпоративную сеть по алгоритмам ГОСТ, обеспечить защиту внешнего периметра корпоративной сети, обеспечить безопасность каналов связи между ЦОД, а также защититься от сетевых вторжений.

Континент 4 представляет собой целый комплекс защитных средств в одном устройстве: межсетевой экран, криптошлюз, криптокоммутатор, детектор атак, центр управления сетью, причем всеми этими компонентами можно управлять из консоли.

Основной функционал Континент 4:

* централизованная защита периметра корпоративной сети;
* сегментация внутренней сети;
* предотвращение сетевых вторжений;
* url‑фильтрация, контроль приложений;
* безопасность удаленного доступа.

Модели МЭ Континент 4 рекомендованы для защиты внешнего периметра корпоративной сети, обеспечения безопасности персональных данных, создания VPN ГОСТ вместе с обычной VPN-сетью, для обеспечения безопасности государственных информационных систем. С помощью моделей МЭ Континент 4 можно спроектировать защищенную корпоративную сеть передачи данных по алгоритмам ГОСТ, обеспечить защиту каналов связи между ЦОД и защиту магистральных каналов связи, наладить безопасную видеоконференцсвязь в компании.  Континент 4 имеет функцию защиты от сетевых вторжений и служит для безопасного удаленного подключения к корпоративной сети.

Для таблицы сравнения МЭ были выбраны следующие модели: Континент 3.9 IPC-R50, Континент 3.9 IPC-R550, Континент 3.9 IPC-R1000, Континент 3.9 IPC-3000NF2, Континент 4 IPC-R50, Континент 4  IPC-R550, Континент 4 IPC-R1000, Континент 4 IPC-3000NF2.

Таблица 3. Cравнение некоторых моделей МЭ Континент 3 и Континент 4.

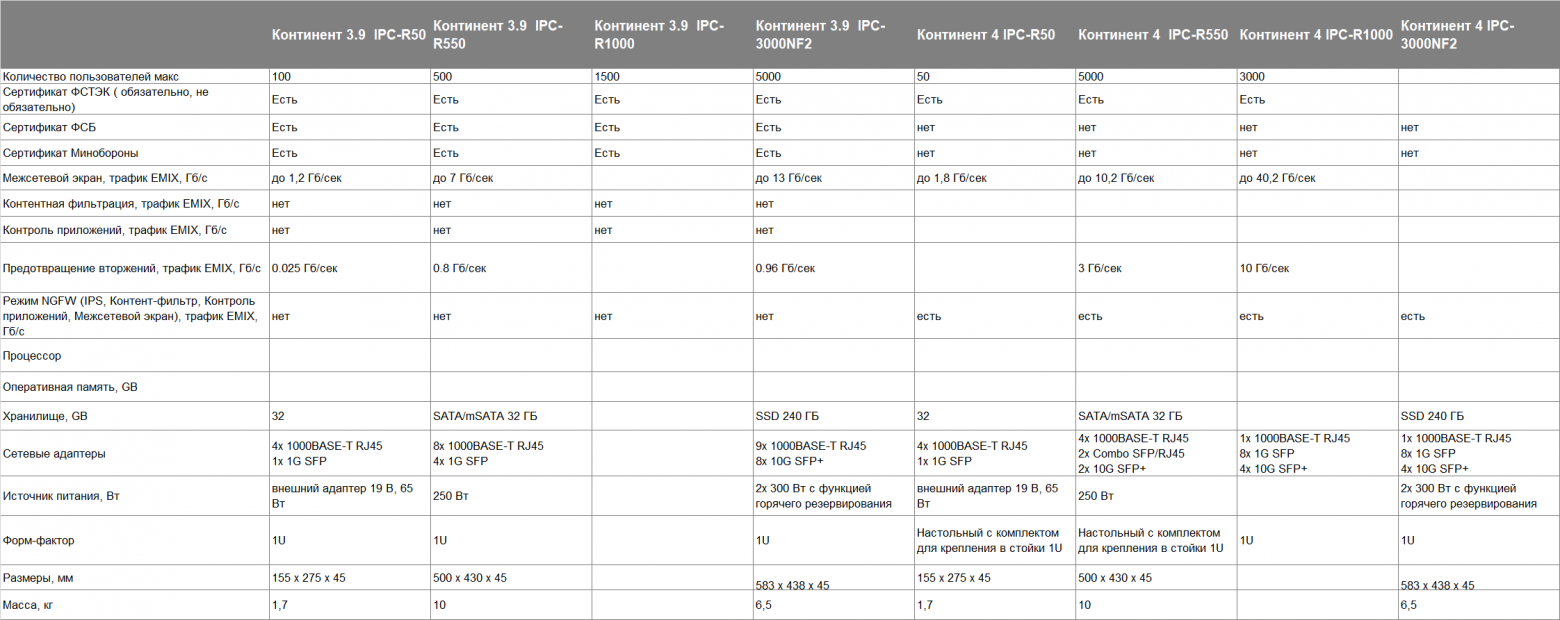


Таблица 3

### 4. Межсетевые экраны «Рубикон»



МЭ Рубикон К

Еще одно российское решение на рынке МЭ — [межсетевые экраны Рубикон](https://rubicon-k.ru/) от компании «Эшелон». Основное назначение программно-аппаратных комплексов (ПАК) «Рубикон» — это организация эффективной защиты периметра сети компаний в соответствии с требованиями регуляторов. ПАК Рубикон — это межсетевые экраны с дополнительными функциями маршрутизации и системы обнаружения вторжений.

Линейка продуктов Рубикон включает в себя следующие модели:

1. Рубикон — предназначен для военных систем и для работы с государственной тайной.
2. Рубикон А — предназначен для работы с ГИС, ИСПДн, ИИС, в которых обрабатывается информация, составляющая гос. тайну.
3. Рубикон К — предназначен для защиты ГИС и АИС, в которых ведется обработка конфиденциальной информации и персональных данных.

ПАК Рубикон кроме выполнения функций межсетевого экрана также оснащен системой обнаружения вторжений IDS/IPS, может выполнять функции маршрутизации.

Основные технические особенности ПАК Рубикон:

* Скорость маршрутизации и производительность межсетевых экранов до 9 Гб/c;
* Наличие отказоустойчивого кластера, что дает возможность организовать непрерывный доступ к корпоративной сети;
* Запись всех событий ИБ в сети и оповещение администратора;
* Возможность построения VPN туннелей с использованием протоколов IPSec, OpenVPN и GRE;
* Поддержка протоколов динамической маршрутизации (RIP, BGP, OSPF), наличие статической маршрутизации;
* Интеграция с внешними системами анализа и управления событиями информационной безопасности;
* Web‑интерфейс управления с ролевой моделью доступа.

Варианты исполнения МЭ Рубикон следующие:

* Рубикон Мини;
* Рубикон Защищенный 4 порта;
* Рубикон Защищенный 10 портов;
* Рубикон 1U;
* Рубикон Высокопроизводительный;
* Рубикон Мультипортовый.

Модели Рубикон Мини рассчитаны на подключение до 100 пользователей максимально, Рубикон 1U позволяет подключать до 200 пользователей, а модели Рубикон Высокопроизводительный — до 400 и Рубикон Мультипортовый — до 5000. Линейка Рубикон сертифицирована ФСТЭК и Минобороны РФ. Также необходимо отметить наличие криптошлюза в моделях Рубикон, который позволяет построить криптографические туннели для защиты передачи данных. В таблице сравнения мы проанализировали все модели Рубикон.

Таблица 4. Cравнение моделей МЭ Рубикон.

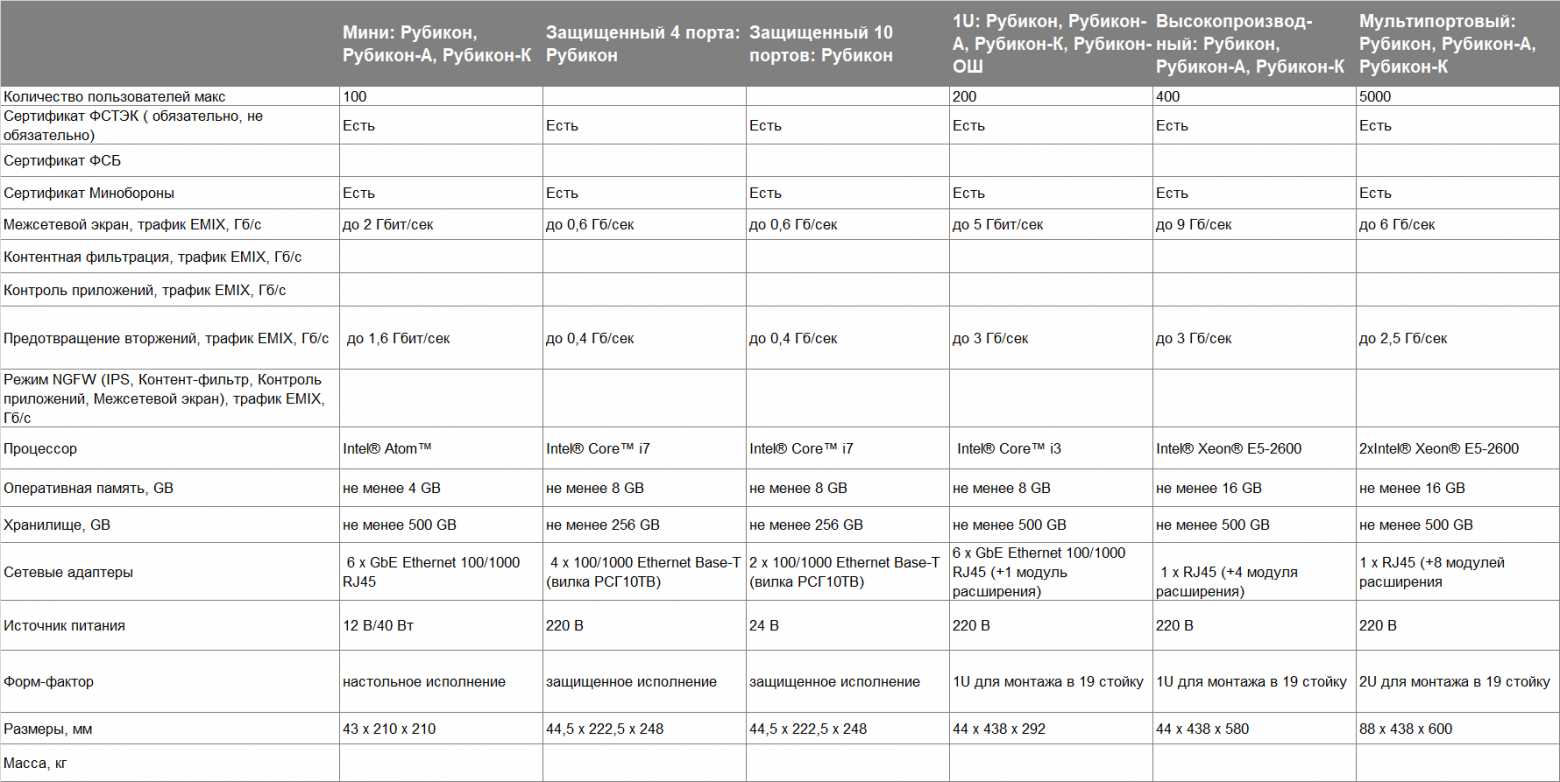


Таблица 4

### 5. Межсетевые экраны UserGate



МЭ UserGate серии Е1000

Решения от российской компании UserGate в области разработки электроники и программного обеспечения для сферы информационной безопасности предназначены для предприятий среднего бизнеса, корпоративного сектора и государственных структур. В нашем обзоре мы остановимся на [линейке аппаратных межсетевых](http://usergate.ru/) экранов этого производителя. МЭ UserGate работает как корпоративный межсетевой экран, осуществляет защиту сети на периметре для средних и крупных предприятий. Дополнительно, к основной функции брандмауэра, российские межсетевые экраны UserGate защищают от угроз нового поколения, поддерживают концепцию SOAR, имеют встроенную систему обнаружения вторжений (IDS/IPS), обеспечивают анализ инцидентов безопасности (SIEM) и фильтрацию интернет-контента. Для МЭ UserGate доступна функция «удаленное администрирование». Продукция UserGate обладает высокой отказоустойчивостью и поддерживает кластеризацию. Отметим еще некоторые функции, которые выполняют МЭ UserGate:

* доступ к внутренним ресурсам через SSL VPN Portal;
* обратный прокси, контроль доступа в интернет и контроль приложений L7;
* дешифрование SSL;
* антивирусная защита;
* Advanced Threat Protection;
* безопасность почты и идентификация пользователей;
* поддержка концепции BYOD (Bring Your Own Device);
* виртуальная частная сеть (VPN);
* поддержка АСУ ТП (SCADA).

Мы сделали сравнительный обзор различных моделей аппаратных межсетевых экранов UserGate в таблице 5.

Например, представлена модель начального уровня UserGate С100 (для малого бизнеса, филиалов, POS-систем, школ, Wi-Fi-точек), количество пользователей, которое возможно подключить к этому МЭ — не более 100. Для среднего бизнеса, ритейла и крупных филиалов предлагаются модели Usergate D200 и D500, с возможностью подключения до 300 и 500 пользователей соответственно. Эти модели обеспечивают соблюдение корпоративных политик для групп пользователей, предоставляют защиту гостевого Wi-Fi, дают возможность контроля персональных устройств, таких как смартфоны и планшеты (концепция BYOD — Bring Your Own Device).  Для больших корпоративных сетей и интернет-провайдеров производитель рекомендует модели Usergate E1000 и E3000 с возможностью подключения 1000 и 3000 пользователей соответственно. Межсетевой экран UserGate F8000 предназначен для обеспечения ИТ-безопасности корпоративных сетей, дата-центров, федеральных университетов, министерств, крупного ритейла. К нему можно подключить до 10000 пользователей максимально. Также производитель выпускает модель UserGate X10, предназначенную для защиты промышленных объектов. UserGate X10 имеет все функции NGFW, предоставляет защиту от кибератак и вредоносных программ. Межсетевые экраны UserGate сертифицированы ФСТЭК.

Таблица 5. Cравнение моделей МЭ UserGate.



Таблица 5

### 6. Межсетевые экраны Ideco

(Фото)

МЭ Ideco серии MX

В завершении нашего обзора рассмотрим [аппаратные межсетевые экраны Ideco](http://ideco.ru/). Сразу отметим, что сертифицированные ФСТЭК межсетевые экраны — это Ideco MX Cert и Ideco MX+ Cert.

МЭ Ideco MX Cert позволяет подключать до 350 пользователей максимально, также этот межсетевой экран служит для защиты локальной сети предприятия от внешних угроз, контролирует потоки трафика и эффективно решает все потребности сетевой инфраструктуры. Производитель заявляет следующие дополнительные функции:

* контентная фильтрация;
* контроль приложений;
* предотвращение вторжений;
* режим NGFW.

Данный межсетевой экран рекомендован для предприятий малого и среднего бизнеса.

Следующая модель Ideco MX+ Cert, которая также рассчитана на предприятия сектора СМБ позволяет подключить уже до 700 пользователей. Она также сертифицирована ФСТЭК и рассчитана на решение широкого круга задач и возможность интеграции с AD/LDAP.

В линейке моделей Ideco есть МЭ для предприятий малого бизнеса, который позволяет подключать до 75 пользователей. Однако, даже младшая модель Ideco имеет следующий функционал:

* вводит ограничения по трафику для каждого из сотрудников или отдельных групп;
* защищает периметр сети;
* умеет сегментировать сеть и использовать несколько интернет‑провайдеров (благодаря 6 сетевым интерфейсам);
* предоставляет возможность удаленной работы сотрудников по VPN.

Для предприятий малого и среднего бизнеса предназначены модели: Ideco MX (до 350 пользователей максимально), Ideco MX2+ Cert (до 400 пользователей максимально) и Ideco LX (до 1000 пользователей максимально).

Также в нашей таблице сравнения мы рассматриваем и старшие модели этого производителя, например, Ideco-LX-Cert (до 2000 пользователей максимально), Ideco LX+ (до 3000 пользователей максимально) и Ideco EX (до 5000 пользователей максимально). Эти модели предназначены для крупных компаний.

Таблица 6. Сравнение моделей МЭ Ideco.

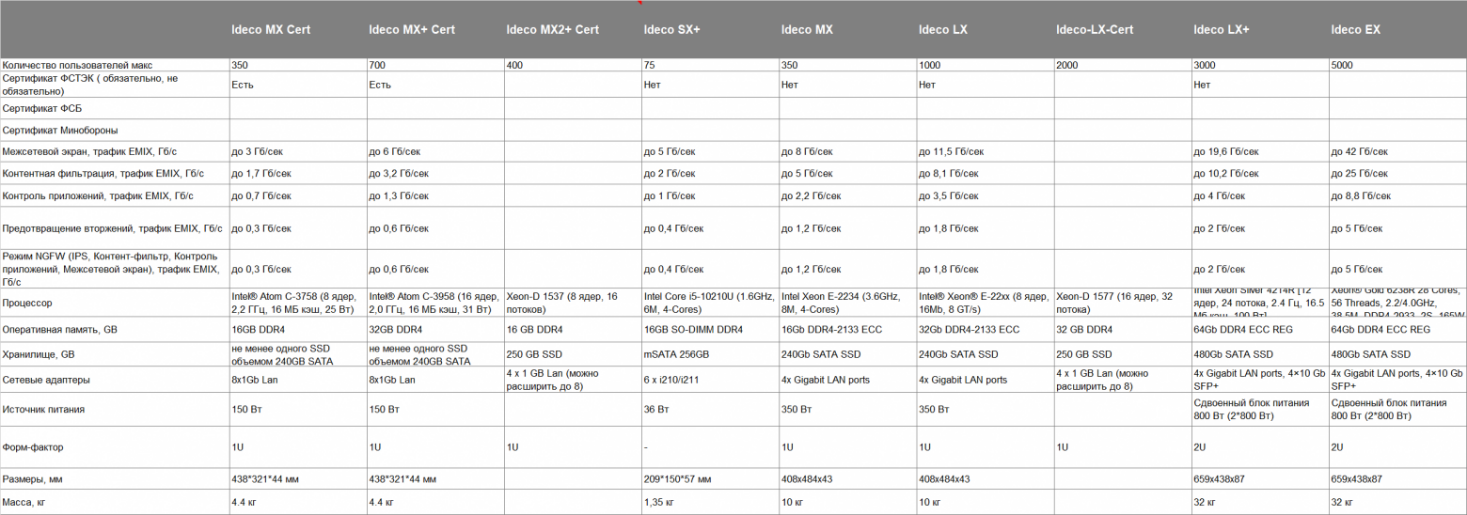


Таблица 6

## Выводы

В данном обзоре мы рассмотрели аппаратные межсетевые экраны следующих отечественных брендов: Diamond, Dionis DPS, «Континент», «Рубикон», UserGate и Ideco. Если подвести итоги нашего исследования, то можно сделать следующие выводы:

1. При выборе надежного и производительного аппаратного МЭ для своей компании можно ориентироваться на оборудование российского производства.
2. Практически все отечественные бренды, приведенные в нашем обзоре, имеют сертификат ФСТЭК (не всегда сертифицирован весь модельный ряд, как у Ideco).
3. Некоторые производители имеют также сертификаты ФСБ (Дионис, Diamond, Континент 3) и Минобороны (Континент 3, Рубикон).
4. Всегда можно выбрать подходящее решение для малого, среднего или крупного бизнеса, так как почти все производители делают градацию своих изделий по максимальному количеству пользователей и производительности в режиме МЭ.
5. Достаточно много моделей, которые кроме основного режима МЭ, работают и в режиме NGFW (IPS, Контент-фильтр, Контроль приложений, Межсетевой экран).
6. Среди представленных для обзора МЭ есть решения для работы с военными системами, гос. тайной, с КИИ, персональными данными и конфиденциальной информацией, аппаратно-программные криптошлюзы.

# **2.2 (еще устройства с российского рынка)**

# **2.3 Программно-аппаратные комплексы защиты**

1.VipNEt(https://blog.cortel.cloud/2023/11/30/rossijskie-sredstva-zashhity-informaczii-vipnet/)

2.Соболь-4

3. [**Kaspersky Endpoint Security**](https://blog.cortel.cloud/2023/07/20/rossijskie-sredstva-zashhity-informaczii-kaspersky-endpoint-security/?utm_source=blog&utm_medium=statya&utm_campaign=vipnet_301123)

4. [**Сканер-ВС**](https://blog.cortel.cloud/2023/06/29/skaner-vs/?utm_source=blog&utm_medium=statya&utm_campaign=vipnet_301123)

5. [**Secret Net Studio**](https://blog.cortel.cloud/2023/08/31/rossijskie-sredstva-zashhity-informaczii-secret-net-studio/?utm_source=blog&utm_medium=statya&utm_campaign=vipnet_301123)

# **3 ………………(что-то типо сравнительной характеристики устройств)**

# **Заключение**

1

2

3

Таким образом, в результате выполнения работы задачи были выполнены и цель достигнута.

# **Список использованных источников**

1https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/