
MONOLITH
Information Security

MONOLITH+

Во всем мире информация перестает быть вашей собственностью. Ваши приватные и корпоративные данные принадлежат не вам.

Мы возвращаем вам право на конфиденциальность.

Необходимость в простом, понятном, эффективном и надежном IT-решении стала толчком к созданию такой системы безопасности, которой можно доверить защиту корпоративной и персональной информации.

Monolith Plus — это программно-аппаратный комплекс, в который входит безопасная и изолированная от внешнего мира информационная среда (серверная инфраструктура), а также защищенные сервисы для коммуникаций: почтовый сервер, собственная телефония и мессенджеры, свое облачное хранилище данных, удаленный рабочий стол.

Программная часть Monolith Plus основана на мировых стандартах информационной безопасности корпоративного уровня. Используются передовые решения на базе open-source software.

Внедряя Monolith Plus, вы повышаете уровень защищенности вашей коммерческой и конфиденциальной информации, снижаете риски и убытки, которые могли бы произойти в результате утечки данных.

Вам больше не придется опасаться кибератак, слежки и воровства информации.

MONOLITH+

Защита информации от всех видов угроз

Без компромиссов

Monolith Plus исключает все виды информационных угроз

Блокирует воровство информации извне и изнутри

Monolith Plus позволяет настроить работу внутри информационной системы без рисков утечки информации.

Закрывает доступ к вашим приватным данным

Monolith Plus скрывает идентификацию в сети, местонахождение и маршруты. Блокирует доступ к персональным устройствам, отслеживание звонков и сообщений.

Останавливает легальный и нелегальный кибершпионаж

Технологии Monolith Plus исключают перехват трафика, доступ к переписке, пересылаемым файлам, контактам, групповым конференциям, голосовым сообщениям и т. д.

Обеспечивает непрерывную работу IT-систем

Monolith Plus формирует отказоустойчивую IT-инфраструктуру. Система имеет географически распределенную архитектуру.

Защищает от воздействия вредоносного ПО

Monolith Plus распознает подозрительное программное обеспечение как вредоносное и блокирует его работу, не позволяя злоумышленникам получить доступ к данным.

Исключает насильственный захват информации

При возникновении угрозы Monolith Plus уводит атакующих на альтернативные ресурсы, применяя тактику достоверного отрицания.

Специалисты по безопасности хотят укрепить защиту своих организаций, учитывая сложную картину **угроз** и стремление **хакеров** расширить поле деятельности. Порой компании используют несколько решений от разных поставщиков.

При таком подходе защита информационных сетей становится более сложной и запутанной, поскольку скорость, количество подключенных к Интернету устройств и объем трафика постоянно растут.

ПРОСТОТА И ИНТЕГРАЦИЯ РЕШЕНИЙ – ТО, К ЧЕМУ СТОИТ СТРЕМИТЬСЯ С ЦЕЛЬЮ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПАНИИ.

Заявление Cisco, одной из крупнейших в мире компаний, специализирующихся в области высоких технологий.

Вероятность атак в различных отраслях.

Безопасных отраслей не существует

На графиках представлена динамика показателей блокировки трафика по отраслям за несколько месяцев: тот или иной объем трафика, имеющий отношение к атакам, присутствует в каждой отрасли. Время роста и снижения интенсивности атак в разных отраслях неодинаково, однако атаки так или иначе охватывают абсолютно все сферы.

Организации, сети которых еще не подвергались взлому, могут считать, что избежали опасности. Однако эта уверенность безосновательна.

С учетом разнообразия возможностей и тактических приемов хакеров, нарушение безопасности – это вопрос времени.

ПРОЦЕНТ ЕЖЕМЕСЯЧНЫХ БЛОКИРОВОК ПО ОТРАСЛЯМ

Годовой отчет Cisco по информационной безопасности, 2018 г.
Исследование проводилось в 26 странах с участием более чем 3600 респондентов.

Все новые и новые организации терпят убытки в результате взломов

Последствия несанкционированного доступа злоумышленников не ограничиваются сбоями систем. Взломы и утечка информации также приводят к потере денег, времени и репутации.

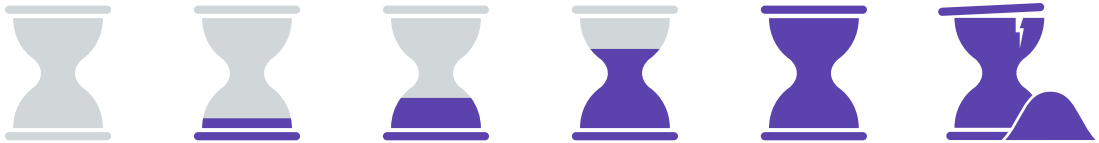
Ущерб организаций исчисляется не только временем, которое придется потратить на устранение сбоя и уязвимости системы.

Есть реальные серьезные последствия, которых компаниям следует всеми силами стараться избегать.

Ни одна организация, которая стремится расти и добиваться успеха, не хочет, чтобы ее важнейшие подразделения пострадали от атаки злоумышленников. Анализируя результаты опроса, специалисты по безопасности должны подумать о собственном предприятии и задать себе вопрос: **«Если ваша компания понесет подобный ущерб из-за нарушения безопасности, как это отразится на ее дальнейшей деятельности?».**

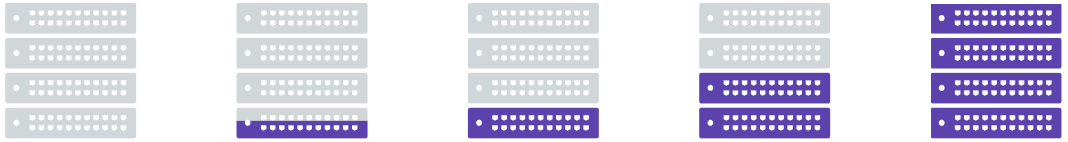
ПРОДОЛЖИТЕЛЬНОСТЬ И МАСШТАБ СБОЕВ, ВЫЗВАННЫХ НАРУШЕНИЯМИ БЕЗОПАСНОСТИ

Время простоя систем организации из-за нарушений безопасности



Без простоя	Менее **1** часа	**1–8** часов	**9–16** часов	**17–24** часов	Более **24** часов
7 %	13 %	45 %	15 %	11 %	9 %

Процент систем, пострадавших из-за нарушений безопасности



Не пострадали	**1–10 %** пострадали	**11–30 %** пострадали	**31–50 %** пострадали	**Более 50 %** пострадали
1 %	19 %	41 %	24 %	15 %

Годовой отчет Cisco по информационной безопасности, 2018 г.
Исследование проводилось в 26 странах с участием более чем 3600 респондентов.

Функции, которые чаще всего затрагивает взлом

36 % специалистов по безопасности отметили, что чаще всего **атаки хакеров** затрагивают эксплуатационную составляющую. Это означает, что системы, формирующие ядро предприятий из разных отраслей, могут замедлить или даже полностью прекратить работу.

Помимо эксплуатационной составляющей, нарушения безопасности **негативно сказываются на финансах** (их упомянули 30 % респондентов), **репутации бренда** и **удержании клиентов** (26 % в обоих случаях).

Операции

36 %

Финансы

30 %

Репутация бренда

26 %

Удержание заказчиков

26 %

Интеллектуальная собственность

24 %

Отношения с деловыми партнерами

22 %

Отношения с поставщиками

20 %

Правовые обязательства

20 %

Нормативные проверки

19 %

Нарушения безопасности за прошедший год отсутствуют

10 %

Годовой отчет Cisco по информационной безопасности, 2018 г.
Исследование проводилось в 26 странах с участием более чем 3600 респондентов.

Потери компаний, пострадавших от кибератак, поистине огромны из-за упущенных коммерческих возможностей

1. Многие организации могут количественно оценить потери своих доходов в результате резонансных инцидентов.

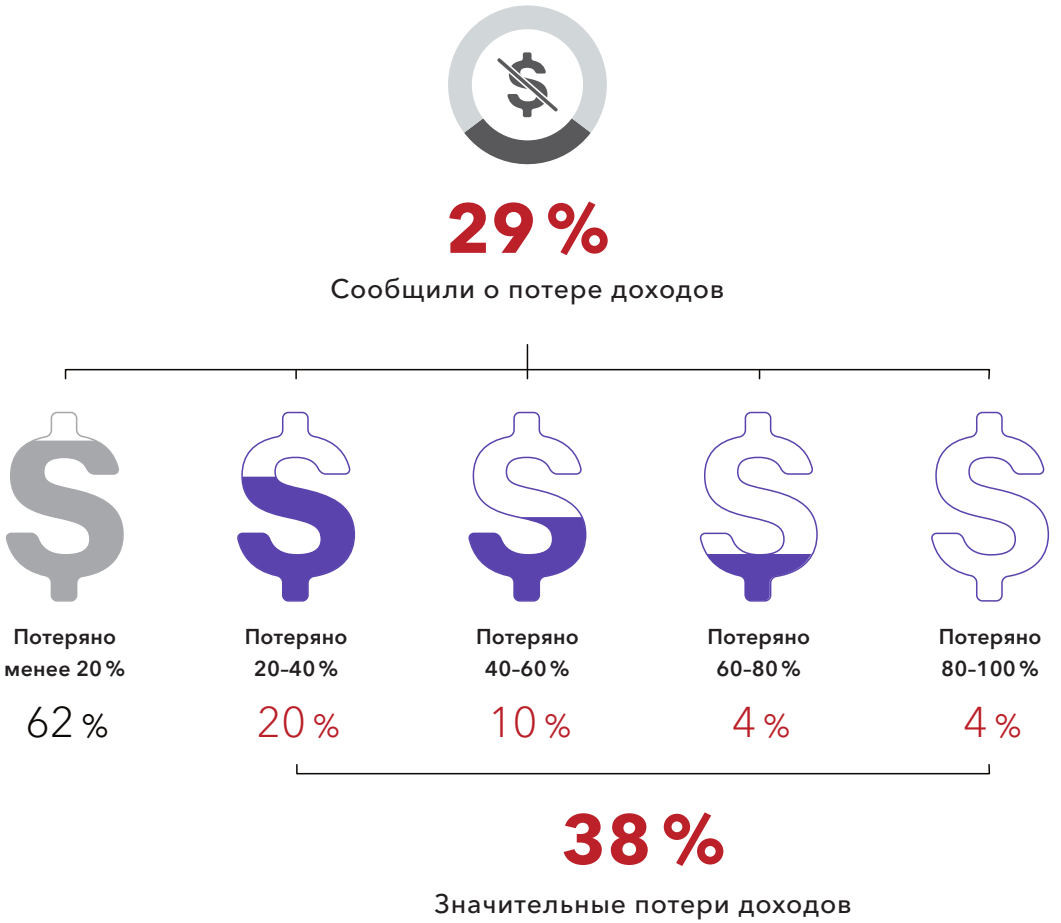
29% специалистов по безопасности сообщили о потере доходов своих организаций в результате атак. Из них 38% заявили, что финансовые потери составили 20% и более.

2. 23% опрошенных специалистов по безопасности сообщили, что в 2016 г. их организации потеряли коммерческие возможности из-за сетевых атак.

58% из них заявили, что совокупный ущерб от упущенных возможностей был менее 20%. По словам 25% респондентов, этот ущерб составил от 20 до 40%, а 9% указали ущерб от 40 до 60%.

3. Сетевые атаки также приводят к оттоку заказчиков. 22 % организаций отметили, что они потеряли заказчиков вследствие атак. Из них 39 % заявили, что потеряли 20 % заказчиков и более.

1. ПРОЦЕНТ ДОХОДА ОРГАНИЗАЦИЙ, ПОТЕРЯННОГО В РЕЗУЛЬТАТЕ АТАКИ



Годовой отчет Cisco по информационной безопасности, 2018 г.
Исследование проводилось в 26 странах с участием более чем 3600 респондентов.

2. ПРОЦЕНТ БИЗНЕС-ВОЗМОЖНОСТЕЙ, УПУЩЕННЫХ В РЕЗУЛЬТАТЕ АТАКИ

23 %

Потери бизнес-возможностей

Потеряно менее 20 %	Потеряно 20–40 %	Потеряно 40–60 %	Потеряно 60–80 %	Потеряно 80–100 %
58 %	25 %	9 %	5 %	3 %

42 %

Значительные потери бизнес-возможностей

3. ПРОЦЕНТ ЗАКАЗЧИКОВ, ПОТЕРЯННЫХ КОМПАНИЯМИ В РЕЗУЛЬТАТЕ АТАКИ

22 %

Потеря заказчиков

Потеряно менее 20 %	Потеряно 20–40 %	Потеряно 40–60 %	Потеряно 60–80 %	Потеряно 80–100 %
61 %	21 %	8 %	6 %	4 %

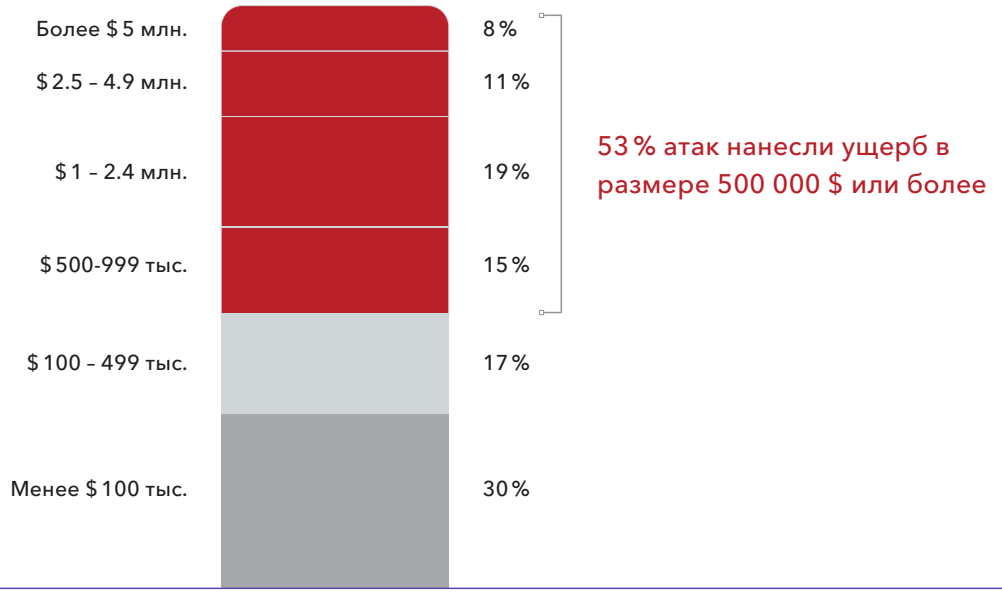
39 %

Значительные потери заказчиков

Годовой отчет Cisco по информационной безопасности, 2018 г.
Исследование проводилось в 26 странах с участием более чем 3600 респондентов.

Цена атак

Страх перед взломом давно перестал быть чем-то неопределенным. На сегодняшний день стоимость сетевых атак вполне конкретна и уже не представляет собой гипотетическую цифру. Взломы могут наносить организациям реальный экономический ущерб, на возмещение которого могут уходить месяцы и даже годы. Согласно ответам респондентов, более половины (53 %) всех атак злоумышленников привели к финансовому ущербу в размере свыше 500 000 долларов США с учетом упущенных прибыли и возможностей, потери клиентов, прямых расходов и прочих убытков.



Годовой отчет Cisco по информационной безопасности, 2018 г.
Исследование проводилось в 26 странах с участием более чем 3600 респондентов.

Основные принципы Monolith Plus

Простота использования и обслуживания

Не требует специальных знаний.
Работа с информацией проходит по привычным алгоритмам.

Возможность достоверного отрицания

Возможность отрицания факта существования информационной системы и предъявление доступа, который автоматически ведет атакующих к несекретной информации.

Полная передача сервиса под ваше владение и контроль

Передается не просто логин и пароль – мы передаем вам весь комплекс.
Только вы контролируете систему.

Комплексный подход к защите информации

Monolith Plus контролирует и защищает все возможные каналы коммуникаций. Снижает влияние человеческого фактора, организуя изолированную информационную среду.

Сервисы и услуги

Monolith Plus – программно-аппаратный комплекс, позволяющий обеспечить конфиденциальность информации и ее сохранность.

Серверная инфраструктура с системой автоматической защиты

Безопасные сервисы

- Телефония
- Мессенджеры
- Почта
- Сервис удаленной работы
- VPN

Защищенное оборудование

- Смартфон
- ПК
- Ноутбук
- Токен – аппаратный ключ

Защита, контроль и интеграция стороннего ПО

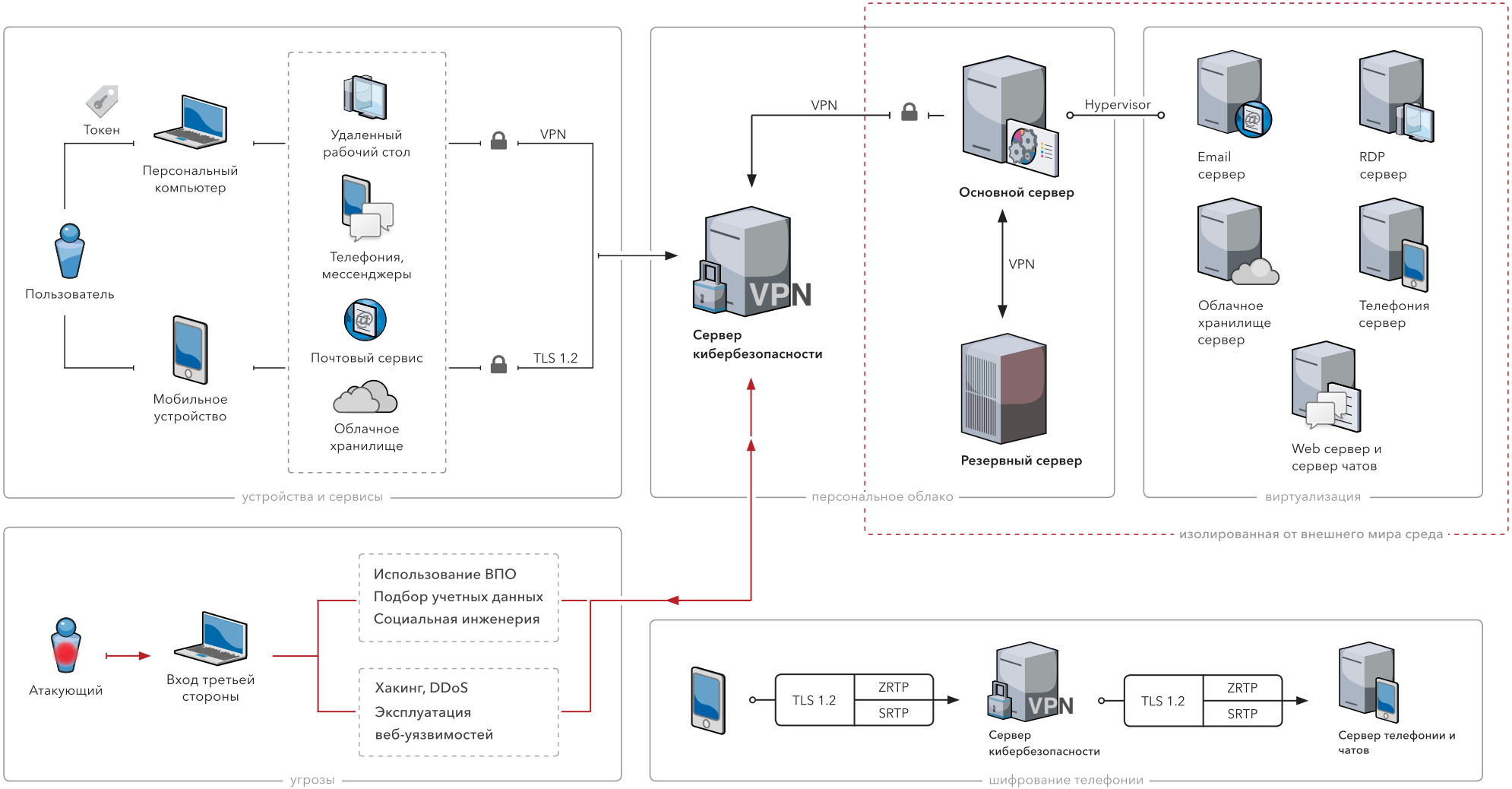
- Отраслевое ПО
- Специализированное ПО
- Базы данных
- CRM
- CMS

Поддержка

- Информационная поддержка
- Техническая поддержка

Обучение и формирование культуры информационной безопасности

Безопасная и изолированная от внешнего мира информационная среда



MONOLITH.PLUS

Описание структуры

Физические серверы

Серверная структура представлена системой из трех основных частей: сервер кибербезопасности, основной сервер, резервный сервер (Backup).

Сервер кибербезопасности (межсетевой сервер) – сервер распределённой сетевой инфраструктуры, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами.

Его возможности:

- защищенная связь (VPN, Proxy) с персональными устройствами;
- аутентификация пользователей и ресурсов в системе;
- глубокая проверка трафика (Deep Packet Inspection);
- блокировка несанкционированного доступа (Intrusion Detection System);
- перенаправление трафика на гостевую систему при вводе гостевого и пароля (сервис гостевого доступа).

Основной сервер – сспециализированный основной сервер для запуска и эксплуатации сервисного программного обеспечения. Управление данными и их хранение происходит в этой части системы.

Резервный сервер (Backup) – сервер, который создает копии данных в облачном хранилище. Последнее предназначено для восстановления информации в прежнем или новом месте в случае ее повреждения.

Сервер обеспечивает:

- отказоустойчивость работы системы;
- восстановление данных при аварийном отключении от основного сервера;
- быстрое восстановление и непрерывность работы всей системы.

Компьютер – Сервер кибербезопасности

Для передачи данных на Сервер кибербезопасности используется технология VPN (Virtual Private Network), позволяющая выполнить одно или несколько сетевых соединений (логическую сеть) поверх другой сети. Она обеспечивает:

- высокий уровень шифрования передачи данных (AES256-GCM-SHA384);
- анонимность в сети;
- фильтрацию сетевого трафика;
- защиту передаваемых данных между двумя узлами выстроенной сети.

Для установления связи **Компьютер – Сервер кибербезопасност**и понадобится **Токен**, который идентифицирует пользователя.

Мобильное устройство – Сервер кибербезопасности

Для повышения безопасности данных используется протокол TLS, включающий в себя:

- асимметричное шифрование для аутентификации;
- симметричное шифрование для конфиденциальности;
- коды аутентичности сообщений для сохранения их целостности.

Сервер кибербезопасности – Основной сервер – Резервный сервер

Все серверы связаны защищенной внутренней сетью VPN. Для передачи данных на основной сервер используется технология обратного прокси, что позволяет скрыть IP-адреса основного и резервного серверов.

Токен – компактное устройство, предназначенное для обеспечения информационной безопасности пользователя. Токен используется для идентификации его владельца, получения безопасного удаленного доступа к информационным ресурсам.

АУДИТ ВАШЕЙ IT-СТРУКТУРЫ

Предлагаем провести бесплатный аудит вашей персональной и/или корпоративной системы коммуникаций.

Мы проверим вашу систему на уязвимости, предоставим их предметный анализ и дадим рекомендации по защите – **все это совершенно бесплатно**.

Закажите аудит по номеру: +7 495 957 48 49

Анонимизация и защита персонального компьютера

Шифрованный ноутбук с двумя независимыми рабочими системами.
Реализовано безопасное хранение информации на самом компьютере.

Два рабочих изолированных пространства + скрытый том

Выбор системы определен сценарием входа. Пример: один пароль запускает основную систему, второй – гостевую.

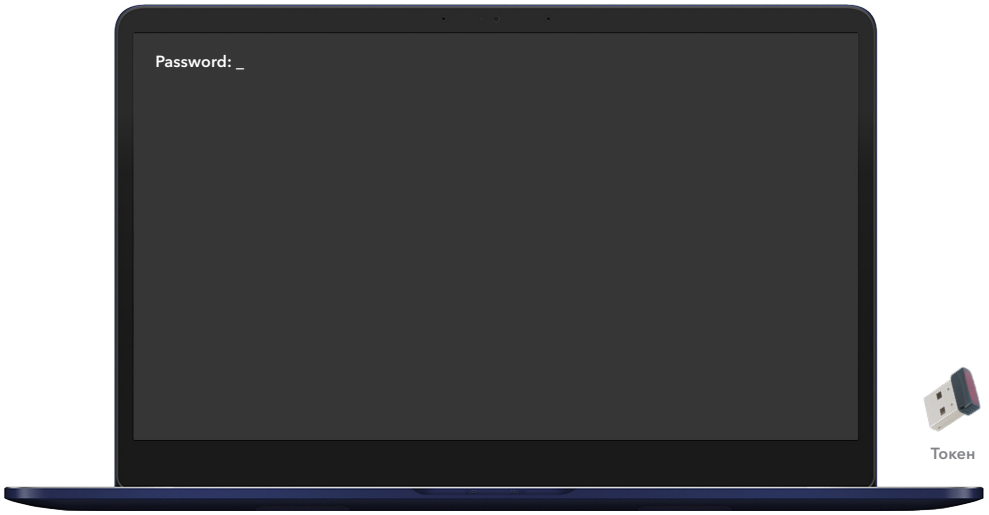
Токен-авторизация

Вход в систему при помощи токена для идентификации и безопасного удаленного доступа к информационным ресурсам.

RDP

Работа на удаленном сервере.

Авторизация при помощи токена.



«два компьютера в одном» – зашифрованная система токен-авторизация

Зашифрованные ОС

Система шифрования разделов делает их невосприимчивыми к последним технологиям в области кибератаки.

IC-лазер

Контроль положения ноутбука в пространстве.

При поднятии компьютера со стола автоматически завершается работа системы.

Защита оперативной памяти и USB

Аппаратная и программная защита.

Наиболее сложные для защиты области: мобильные устройства и данные в облаке

Перед отделами безопасности, пытающимися защитить свои организации, стоит ряд препятствий. Защита компаний должна работать в разных направлениях, что затрудняет обеспечение безопасности.

Самую большую сложность для защиты представляют мобильные устройства, данные в общедоступном облаке и поведение пользователей.

Годовой отчет Cisco по информационной безопасности, 2018 г.
Исследование проводилось в 26 странах с участием более чем 3600 респондентов.

Анонимизация и защита мобильных устройств

Защищенный от кибератак смартфон с возможностью анонимного использования.
Смартфон, сохранивший обычный функционал и привычные сценарии использования.

Невозможно перевыпустить SIM-карту.

Как следствие, невозможно получить доступ к сервисам, с авторизацией по номеру телефона.

Защищенное использование публичных мессенджеров, Telegram или WhatsApp.

Телефон имеет два изолированных рабочих пространства с отдельными файлами и приложениями.

Возможность совершать звонки из любой точки планеты, где есть Интернет.

Без ограничений.

Защищен от прослушивания, перехвата данных, слежения и идентификации пользователя.

Все файлы, история переписки и пароли защищены шифрованием при передаче и хранении.

анонимный – защищенный – функциональный

Защита мобильных устройств: уязвимости мобильных устройств

НЕЗАЩИЩЕННОЕ МОБИЛЬНОЕ УСТРОЙСТВО	**MONOLITH PLUS:** ЗАЩИТА МОБИЛЬНОГО УСТРОЙСТВА
Уязвимости и системы слежения на уровне операционной системы и приложений.	**Защищенная мобильная операционная система** без систем слежения и передачи данных на сторонние ресурсы. Политика полного контроля прав доступа приложений.
Уязвимости и системы слежения на аппаратном уровне устройства.	У телефона **отсутствуют функции слежения на аппаратном уровне**. Телефон не использует средства хранения и передачи третьей стороне пользовательской информации (данные карт, отпечатки, пароли).
Уязвимости на уровне централизованной архитектуры сервисов предоставляющих услуги коммуникаций (телефония, чаты).	**Сервисы коммуникации устанавливаются на вашем сервере**, образуя персональную изолированную и только вам подконтрольную систему для общения и обмена информацией.
Уязвимости на уровне GSM-оператора и интернет-провайдера.	**Установлена защита от прослушивания и перехвата сигнала** от GSM-вышек, обеспечена полная анонимизация в Интернете путем шифрования и маскировки трафика всех каналов коммуникаций.
Уязвимости на уровне сетевой инфраструктуры.	Коммуникации (телефония, обмен сообщениями и файлами) организованы с **применением сквозного тройного шифрования**.

Сравнительная таблица сервисов передачи голоса и сообщений

	Telegram	WhatsApp	VPole Enterprise	Signal	Сервисы IP-телефонии	Monolith Plus
Хранение и управление данными третьей стороной	Управление и контроль принадлежит сервису	Управление и контроль принадлежит сервису	Управление и контроль принадлежит вам	Управление и контроль принадлежит сервису	Управление и контроль принадлежит сервису	Управление и контроль принадлежит вам
Отсутствие явной идентификации пользователя	Идентификация по номеру телефона	Идентификация по номеру телефона	Не требуется	Идентификация по номеру телефона	Идентификация по номеру телефона, паспортным данным	Не требуется
TLS (защита метаданных)	Да	Да	Да	Да	Нет	Да
End-to-End-шифрование	Управление шифрованием в руках разработчика	Управление шифрованием в руках разработчика	Управление шифрованием в руках разработчика	Управление шифрованием в руках разработчика	Управление шифрованием в руках разработчика	Управление шифрованием принадлежит вам
Открытый исходный код серверного ПО	Закрытый исходный код	Закрытый исходный код	Закрытый исходный код	Частично открытый исходный код	Протокол открыт, серверная часть закрыта	Открытый исходный код протоколов и ПО
Протокол шифрования сообщений	MTProto, закрытый протокол	Протокол на базе Signal, изменен и закрыт	VIPole, закрытый протокол	Signal	–	E2EE/OMEMO/OTR – открытые протоколы
Протокол шифрования голосовых данных	Да, контроль в руках сервиса	Да, контроль в руках сервиса	Да, контроль в руках сервиса	Да, контроль в руках сервиса	Нет	Да: SRTP/ZRTP
Хранение данных на уровне приложения/ устройства	Частично шифрует ключом устройства	Частично шифрует ключом аккаунта	Частично шифрует ключом аккаунта	Частично шифрует ключом устройства	Нет	Полное шифрование данных AES256
Разработчики / Провайдер может заблокировать аккаунт	Может/Блокируют	Может/Блокируют	Может	Может	Может/Блокируют	Полный контроль принадлежит вам
Отслеживает местоположение	С разрешения пользователя	С разрешения пользователя	С разрешения пользователя	Не отслеживает	По IP адресу	Не отслеживает
Не хранит историю сообщений и другую информацию об использовании на устройстве	Хранит	Хранит	Не хранит	Хранит	Хранит	Не хранит, backup на вашем сервере
Не раскрывает IP-адрес пользователя	Доступен оператору	Доступен оператору	Доступен оператору	Доступен оператору	Доступен оператору	Не раскрывает
Нормирование трафика – анонимизация	Нет	Нет	Нет	Нет	Нет	Маскируется под обычный HTTPS
Уровень защиты информации мобильного устройства	На уровне приложения	На уровне приложения	На уровне приложения	На уровне приложения	На уровне приложения	На уровне системного ПО и приложения

Установка защищенного соединения телефонии

Для безопасной передачи голосовых данных используется тройное шифрование:

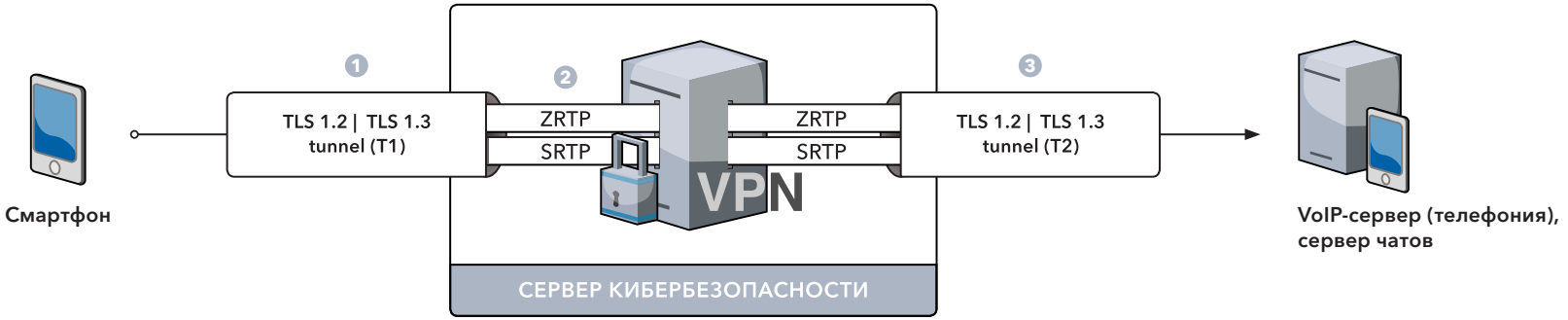
- шифрование данных – преобразование информации в другую форму;
- шифрование метаданных – защита файлов на персональных устройствах и передаваемой по сети информации от серверов;
- шифрование платформы (серверная часть системы).

1. Смартфон с собственным IP-адресом устанавливает защищенный TLS 1.2 / TLS 1.3 туннель **(T1)** с сервером кибербезопасности.
2. Данные в зашифрованном виде отправляются на внешний IP-адрес сервера кибербезопасности.
3. Далее сервер кибербезопасности отсылает данные на внутренние адреса VoIP-сервера, устанавливая с ним свой защищенный туннель **(T2)**. Информация расшифровывается только на VoIP-сервере.

Сервер кибербезопасности перенаправляет зашифрованные данные из одного TLS-туннеля в другой. Проверяет пакеты данных на предмет атаки и скрывает путь до VoIP-сервера.

Сервер кибербезопасности устроен таким образом, что он незаметен для смартфона.

VoIP-сервер подключается к серверу кибербезопасности как клиент, что обеспечивает полную анонимность.



Смартфон связывается с внешним миром через серверную инфраструктуру. Итог – безопасная и анонимная работа.

Сервер кибербезопасности в первую очередь проверяет защиту самого соединения. Без TLS к нему невозможно подключиться.

ZRTP – криптографический протокол согласования ключей шифрования, используемый в системах передачи голоса по IP-сетям (VoIP).

SRTP – предназначен для шифрования, установления подлинности сообщения, целостности, защиты от замены данных.

MONOLITH.PLUS

Site: monolith.plus
E-mail: hello@monolith.plus
Telegram: @monolithplus