Microsoft

Возможности комплексного предложения Microsoft 365

Сравнение возможностей планов OVS Desktop и Microsoft 365

		OVS Desktop	Microsoft 365 A3	Microsoft 365 A5
Настольные версии Office	Настольная версия Office ProPlus 2019/2022	●	●	●
	Настольная версия Office 365 ProPlus *(M365 Apps for Enterprise)*		●	●
ОС Windows 10/11*	Windows 10/11 Pro Education	●	●	●
	Windows 10/11 с дополнительными возможностями по безопасности *(Windows A3/A5)*		●	●
	Windows 10/11 в облачном решении Azure Virtual Desktop *(AVD)*		●	●
Управление ПК и базовые функции безопасности	Расширенная система мультифакторной аутентификации и условный доступ		●	●
	Поиск теневого IT *(Cloud App Discovery)*		●	●
	Защита локальной системы идентификации *(Advanced Threat Analytics)*		●	●
	Расширенные возможности по управлению учётными данными		●	●
	Прокси для безопасного доступа к локальным web-сайтам		●	●
	Управление мобильными устройствами Android и iOS		●	●
	Управление ПК на базе Windows 10/11 и MAC		●	●
Расширенная безопасность, голосовые возможности	Защита от фишинговых атак (*Defender for Office 365*)			●
	Поиск теневого IT *(Cloud App Security)*			●
	Комплексная защита персональных компьютеров *(Defender for Endpoint)*			●
	Аудио-конференции и функции телефонии			●
Аналитика	Система визуальных отчётов *(Microsoft Power Bi)*			●
Серверные и пользовательские лицензии	Пользовательские лицензии: Exchange, SharePoint, Skype	●	●	●
	Серверные лицензии: Exchange, SharePoint, Skype		●	●
	Пользовательские лицензии Windows Server	●	●	●
	Пользовательские лицензии: System Center Configuration Manager и Endpoint Protection	●	●	●
	Пользовательские лицензии: System Center Service Manager	●	●	●

Возможности для студентов	

* Не включает базовую лицензию на ОС.

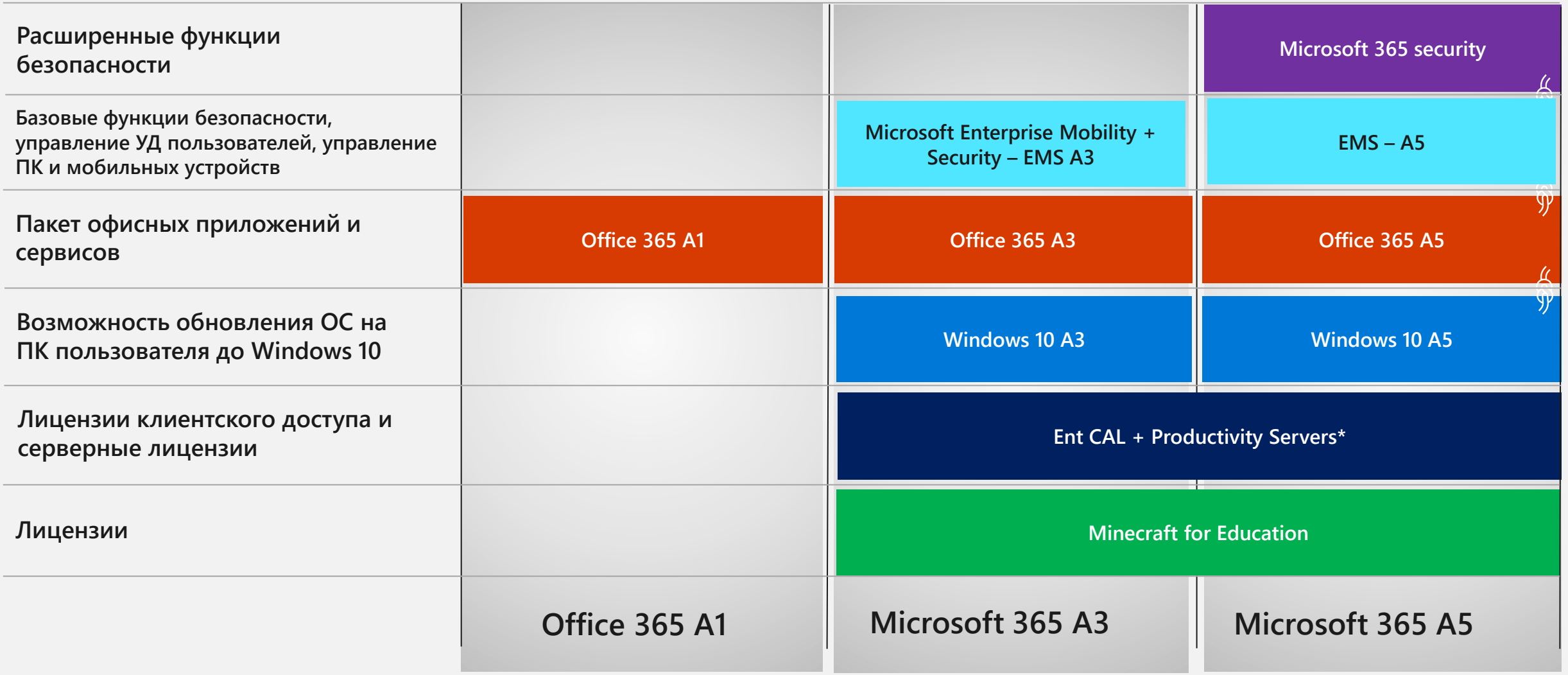
Сравнение возможностей планов Microsoft 365

		Microsoft 365 A3	Microsoft 365 A5
Настольные версии Office	Настольная версия Office ProPlus 2019/2022	●	●
	Настольная версия Office 365 ProPlus *(M365 Apps for Enterprise)*	●	●
ОС Windows 10/11*	Windows 10/11 Pro Education		
	Windows 10/11 с дополнительными возможностями по безопасности *(Windows A3/A5)*	●	●
	Windows 10/11 в облачном решении Azure Virtual Desktop *(AVD)*	●	●
Управление ПК и базовые функции безопасности	Расширенная система мультифакторной аутентификации и условный доступ	●	●
	Поиск теневого IT *(Cloud App Discovery)*	●	●
	Защита локальной системы идентификации *(Advanced Threat Analytics)*	●	●
	Расширенные возможности по управлению учётными данными	●	●
	Прокси для безопасного доступа к локальным web-сайтам	●	●
	Управление мобильными устройствами Android и iOS	●	●
	Управление ПК на базе Windows 10/11 и MAC	●	●
Расширенная безопасность, голосовые возможности	Защита от фишинговых атак (*Defender for Office 365*)		●
	Поиск теневого IT *(Cloud App Security)*		●
	Комплексная защита персональных компьютеров *(Defender for Endpoint)*		●
	Аудио-конференции и функции телефонии		●
Аналитика	Система визуальных отчётов *(Microsoft Power Bi)*		●
Серверные и пользовательские лицензии	Пользовательские лицензии: Exchange, SharePoint, Skype	●	●
	Серверные лицензии: Exchange, SharePoint, Skype	●	●
	Пользовательские лицензии Windows Server	●	●
	Пользовательские лицензии: System Center Configuration Manager и Endpoint Protection	●	●
	Пользовательские лицензии: System Center Service Manager	●	●

Возможности для студентов

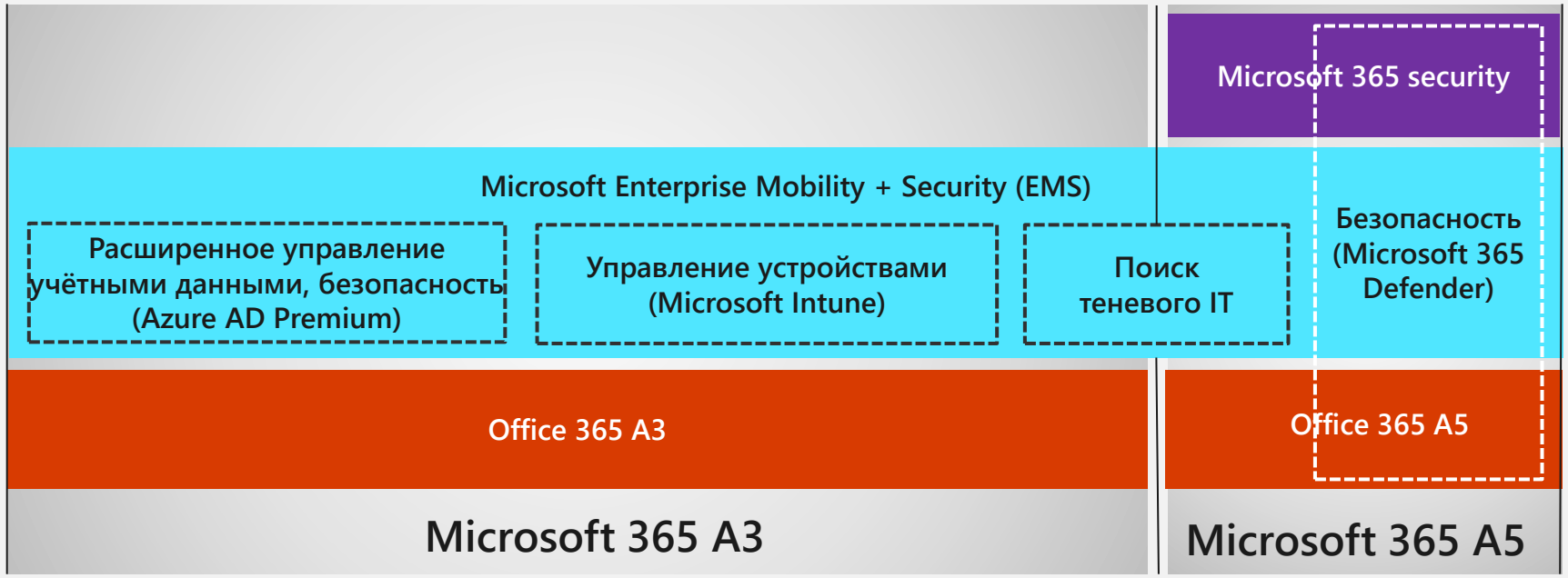
* Не включает базовую лицензию на ОС.

Структура комплексного предложения Microsoft 365

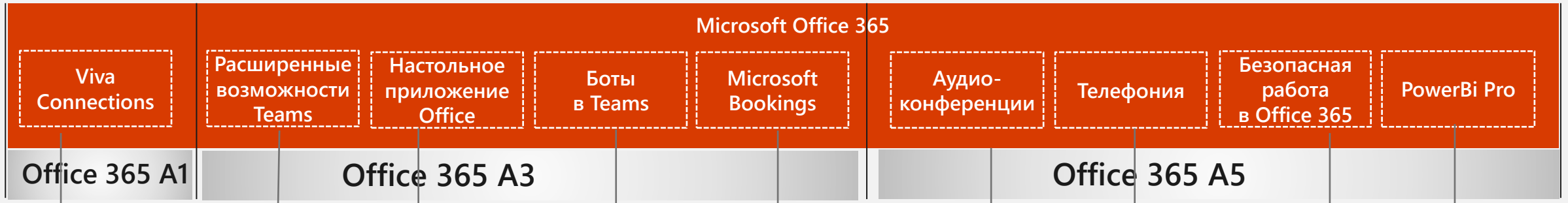


* Возможность установки в своём ЦОД: Exchange Server, SharePoint Server, Skype for Business Server

Ключевые возможности Microsoft 365



Возможности планов Microsoft Office 365



- Интеграция корпоративного портала на базе Sharepoint Online в качестве приложения Teams (Viva Connections)

- Трансляции Teams Live Events
- Собрания до 1000 пользователей
- Режим «просмотра» до 10K участников в обычном собрании
- Собрания с функцией регистрации (Webinar)
- Автозапись собраний
- Долговременное хранение записей собраний

- Возможность установки пакета Office 365 ProPlus (Word, Excel, PowerPoint, Outlook, Publisher) на 5 ПК (рабочих или персональных), а также на планшет и мобильный телефон
- Лицензируется при помощи учётной записи Office 365

- Создание и публикация бота в интерфейсе Teams
- Power Automate в качестве «математики» бота

- Пользователь определяет свободные слоты в своём календаре
- Внешний пользователь назначает встречи на это время через специальный портал

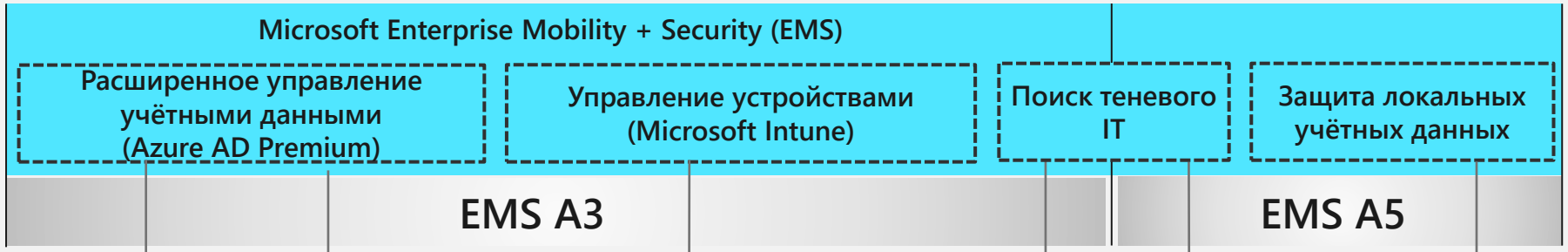
- Аудио-конференции
- Подключение пользователя в собрания Teams по мобильному номеру
- Не требует установки дополнительного шлюза телефонии

- Телефонные функции и звонки с Teams на городские и мобильные телефоны
- Требует установки шлюза телефонии

- Защита при работе с электронной почтой и файлами O365
- Защита от фишинговых атак
- Проксирование ссылок через специальную систему проверки сайтов
- Анализ вложений электронной почты
- Анализ опасных документов при открытии
- Анализ опасных документов
- Эмуляция фишинговых атак
- Обнаружение скомпрометированной учётной записи

- Интерактивные отчёты с функцией одновременного доступа

Возможности Microsoft Enterprise Mobility + Security (EMS)



- Многофакторная аутентификация (MFA)
- Условный доступ в MFA
- Защита от подбора паролей и «простых» паролей
- Самостоятельный сброс пользователем забытого пароля
- Обратная запись пароля в локальный AD
- Динамические группы на базе атрибутов пользователей в AD
- Динамическое лицензирование
- Самостоятельное обслуживание групп пользователями

- Защита локальных корпоративных приложений через облачный MFA и условный доступ (Azure App proxy)
- Шифрование файлов и контроль доступа к ним

- Управление ПК на базе Windows 10 и MAC
- Управление мобильными устройствами (Android, iOS)
- Удалённый Wipe, Reset…
- Инвентаризация аппаратной части
- Инвентаризация приложений
- Удалённая установка приложений
- Управление циклом обновлений Windows 10
- Возможность использования данных Intune для создания отчётов в PowerBi
- Интеграция с System Center

- Анализ логов с Firewall организации для обнаружения и анализа теневых приложений пользователей (Shadow IT)

- Анализ сетевых логов с устройств Windows 10 для обнаружения и блокировки теневых приложений пользователей
- Работает с лицензией Defender for Endpoint (A5)

- Сенсор локальной инфраструктуры AD и ADFS для обнаружения аномальной активности с учётными данными

Возможности комплексного решения по безопасности Microsoft 365 Defender

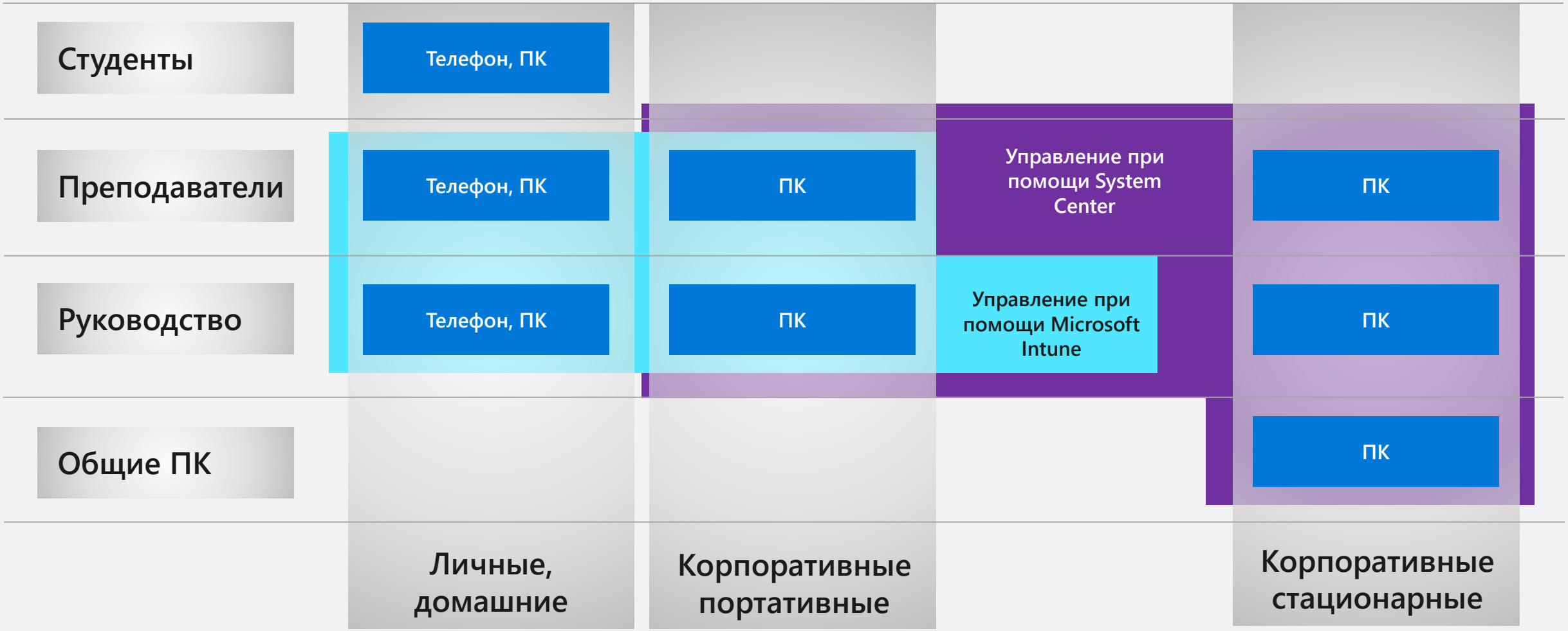
- Интеллектуальная облачная система предотвращения, распознавания, и противодействия комплексным атакам (EDR система), интегрированная со всеми другими подсистемами

- Сенсор локальной инфраструктуры AD и ADFS для обнаружения аномальной активности с учётными данными пользователя
- Защита от подбора паролей и «простых» паролей

- Защита при работе с электронной почтой и файлами O365
- Защита от фишинговых атак
- Проксирование ссылок через специальную систему проверки сайтов
- Анализ вложений электронной почты
- Анализ опасных документов при открытии
- Анализ опасных документов
- Эмуляция фишинговых атак
- Обнаружение скомпрометированной учётной записи

- Агент комплексной безопасности, интегрированный в систему Windows 10

Варианты управления устройствами пользователей



Внедрение функций безопасности в вузе

Возможности Office 365 A3

Возможности Office 365 A3

Название опции	Описание или основной функционал	Сценарий
Office 365 ProPlus	Установки толстого клиента на ПК	Возможность установки офисных приложений на ПК преподавателей и студентов. Активация приложения выполняется путём входа в учётную запись Office 365. Эта схема намного удобнее чем активация через ключ (как в стандартном Office 2019). Эту возможность можно также получить из студенческих бенефитов.

Возможности Office 365 A3

Название опции	Описание или основной функционал	Сценарий
Teams Live Events	Собрания Teams в режиме вебинара до 10 тыс. пользователей	• Количество участников: до 10 тыс. • Формат: вебинар. • Интерфейс проведения собрания: приложение Teams. • Интерфейс слушателя: облегчённая web-версия Teams. • Взаимодействие с участниками: модерируемый чат. • Запись собрания и размещение по той же ссылке что и сам вебинар. • Онлайн-перевод речи на другой язык.

Возможности Office 365 A3

Название опции	Описание или основной функционал	Сценарий
Large Teams meetings	Количество пользователей в собраниях Teams до 1000 участников	Для собраний, в которых организатор собрания имеет лицензию A3/A5, количество участников расширено до 1000 пользователей в режиме полного интерактива.

Возможности Office 365 A3

Название опции	Описание или основной функционал	Сценарий
View-only participants	Автоматический доступ пользователей в обычную конференцию в режиме просмотра	Когда количество пользователей в конференции достигает 1000, остальные пользователи подключаются в режиме просмотра. Они не могут взаимодействовать с другими пользователями но могут видеть, слышать спикера и видеть демонстрируемый контент. Преимущество – простота организации крупных мероприятий, в отличии от Teams Live Events.

Возможности Office 365 A3

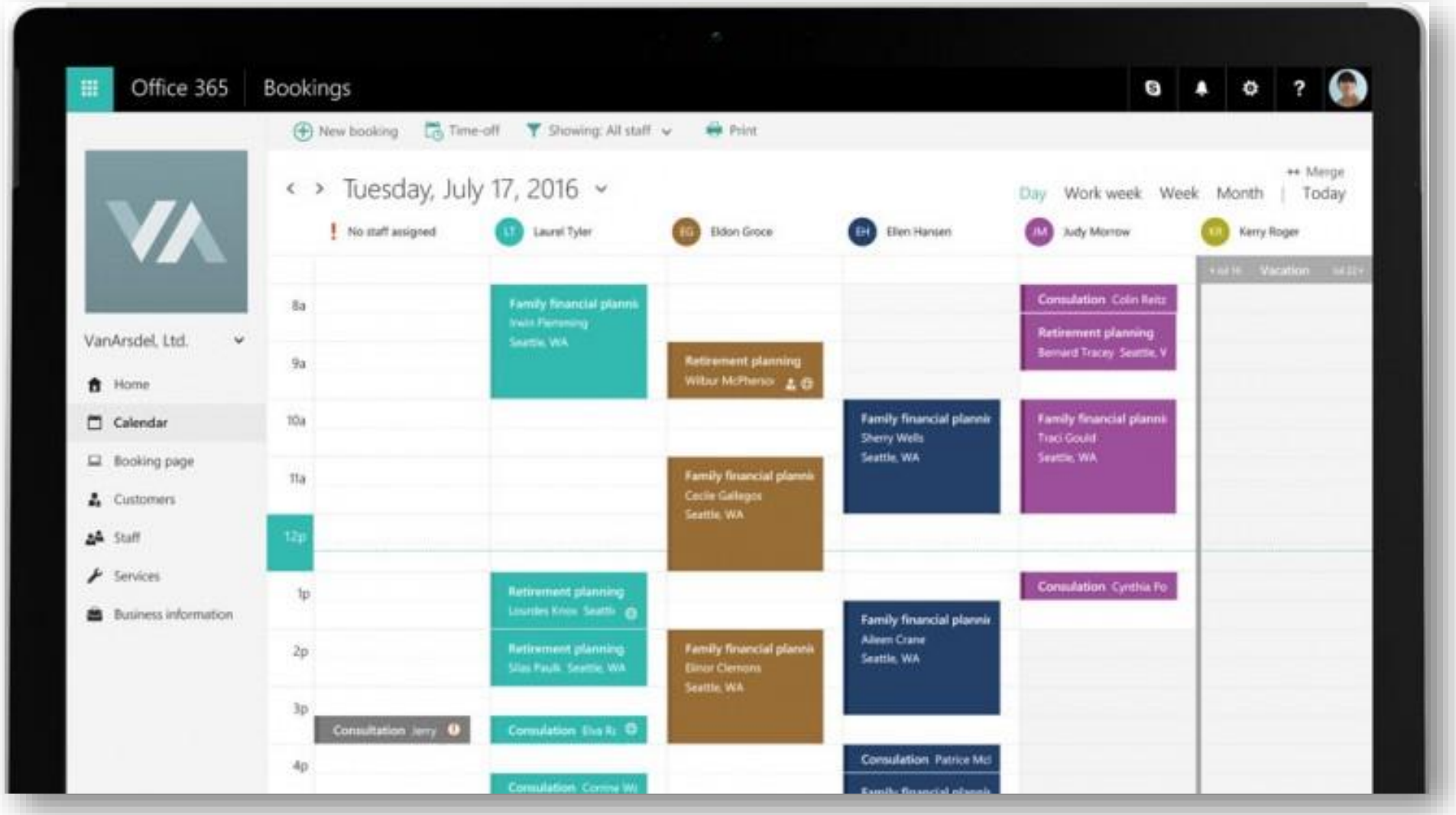
Название опции	Описание или основной функционал	Сценарий

Режим Webinar	Дополнительные возможности к обычным собраниям Teams	• Возможность создания отдельной страницы для регистрации пользователей для сбора регистрационной информации с пользователей:
		  • Контактные данные
		  • Почта
		  • Название организации и пр.
		• Отчёт о присутствии по каждому из зарегистрированных пользователей.
		
		Возможности вебинара идентичны обычному собранию.

Возможности Office 365 A3

Название опции	Описание или основной функционал	Сценарий
Microsoft Bookings	Сервис по резервированию и планированию встреч для внешних клиентов	Преподаватель/руководитель/декан/куратор выделяет определённые интервалы времени в своём календаре и даёт возможность внешним или внутренним пользователям бронировать встречи с ним в этих интервалах. В результате бронирования формируется ссылка на собрание Teams. Решение предоставляет интерфейс для бронирования и позволяет выполнить бронировать строго в определённых интервалах минуя секретарей или помощников.

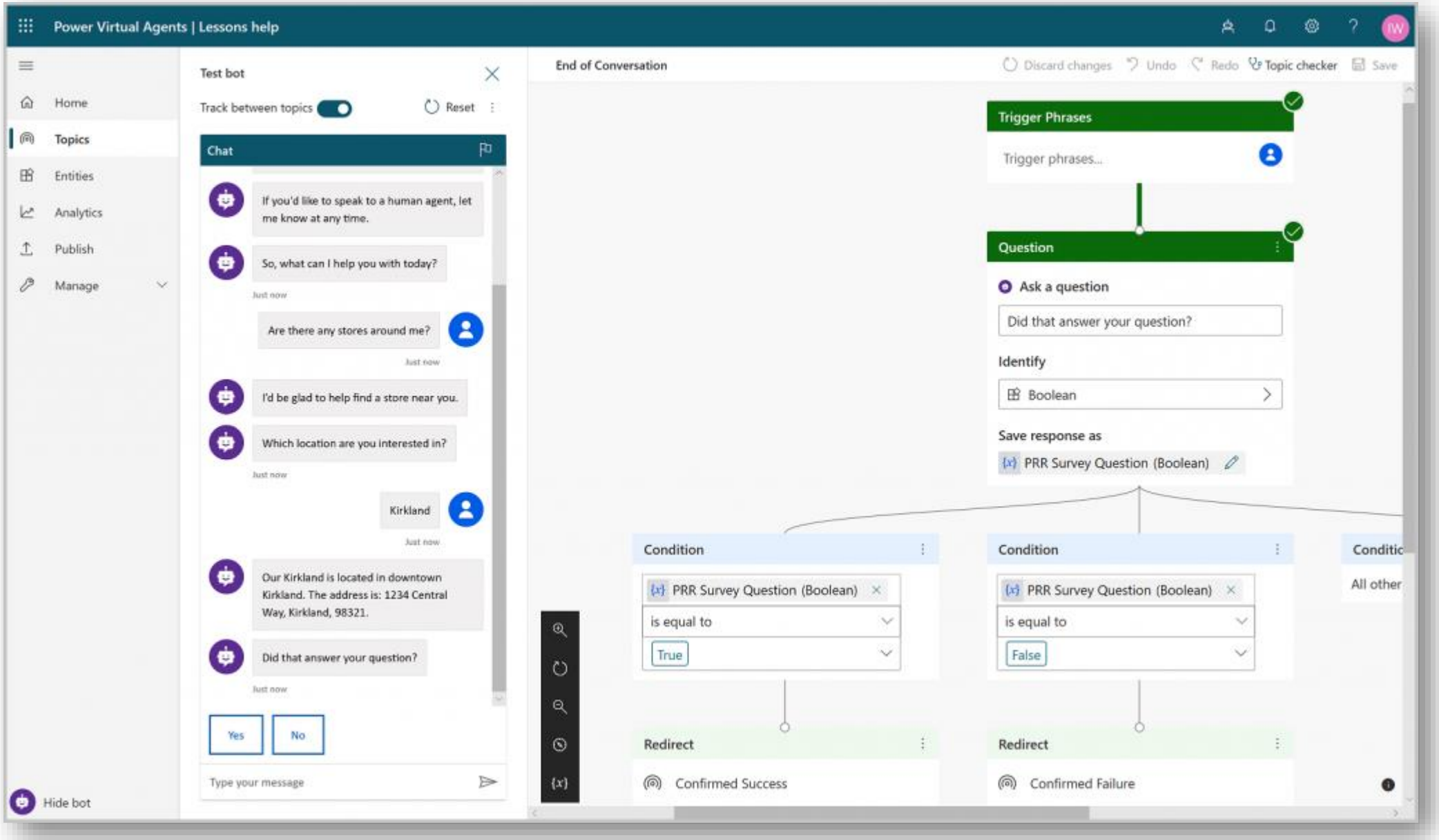
Возможности Office 365 A3. Microsoft Bookings



Возможности Office 365 A3

Название опции	Описание или основной функционал	Сценарий
Боты Power Virtual Agents в Teams	Автоматизация процессов	Возможность создания бота без написания кода (при помощи конструктора) и публикации его внутри ВУЗа для решения различных задач через Teams. Пользователь может взаимодействовать с ботом в отдельном приложении через текстовый чат. В ходе общения бот выполняет какие-то задачи, отвечает на вопросы и т.п.. Для этих ботов не требуется Azure, но и функционал у них слабее. Бот нельзя вынести в Telegram или поместить на сайт. Общение выполняется только из интерфейса Teams. Однако программировать такого бота значительно легче, так как это выполняется из интерфейса Teams при помощи визуального приложения.

Возможности Office 365 A3. Боты Power Virtual Agents в Teams

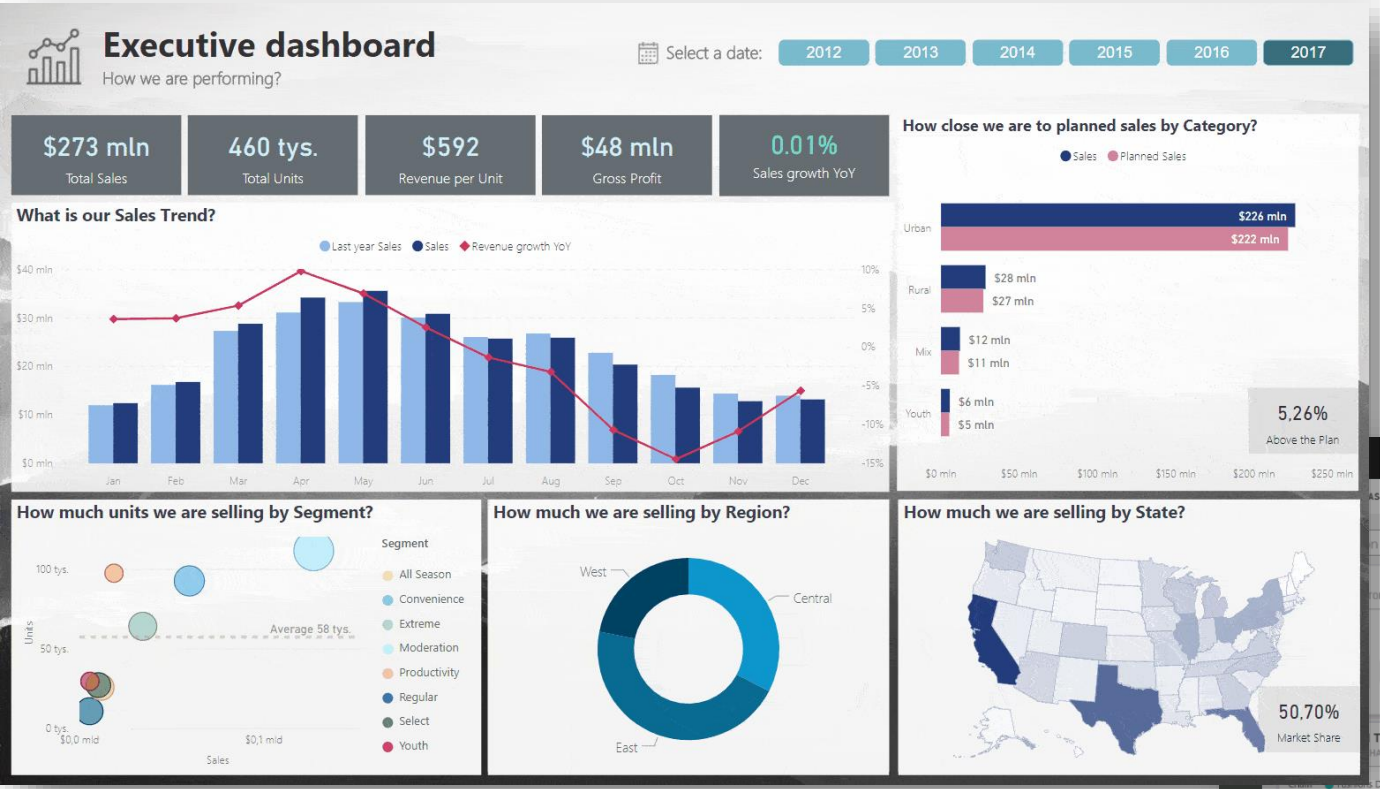


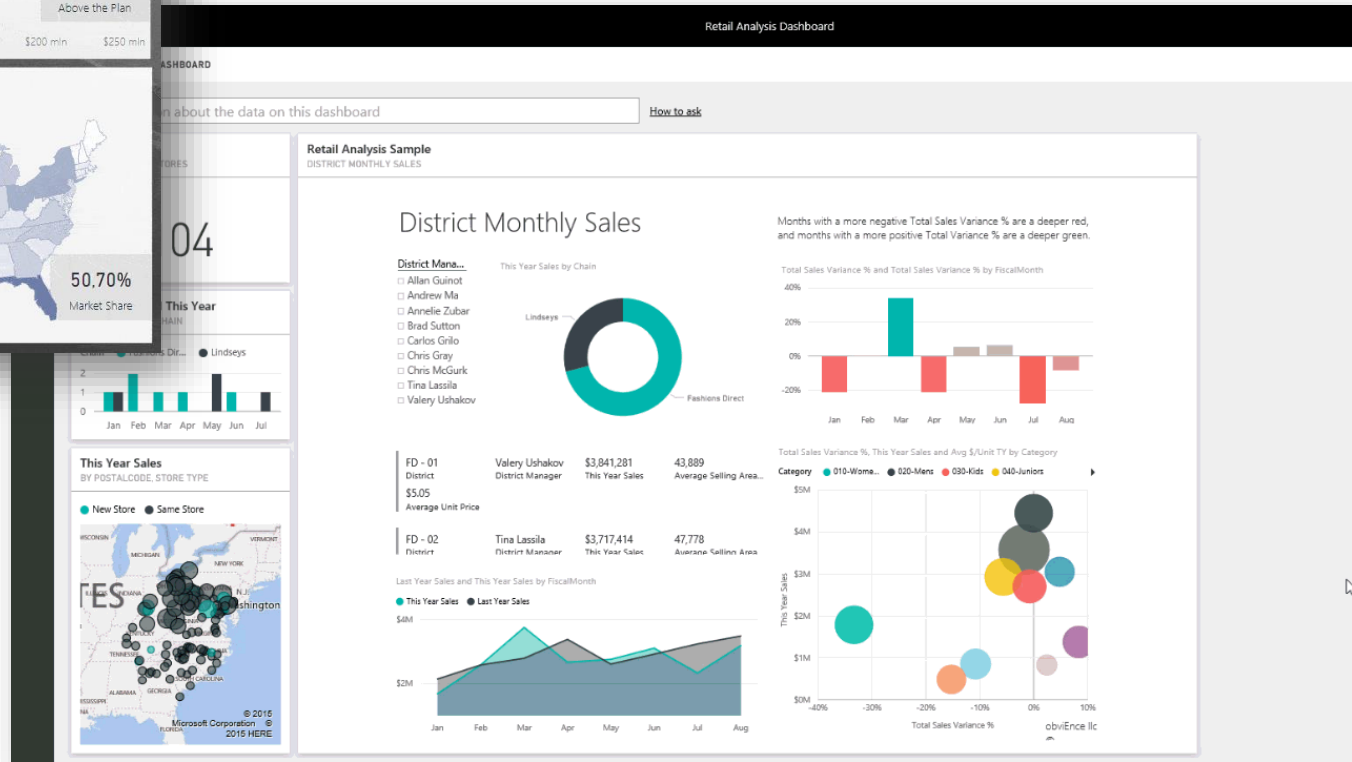
Возможности Office 365 A5

Возможности Office 365 A5

Название опции	Описание или основной функционал	Сценарий
PowerBi Pro	Интерактивные отчёты	Возможность создания и визуально красивого интерактивного отчёта на основе данных из различных источников. Возможно предоставление отдельных отчётов различным категориям пользователей. Пользователи с лицензией могут работать с отчётом одновременно.

Возможности Office 365 A5. PowerBi Pro





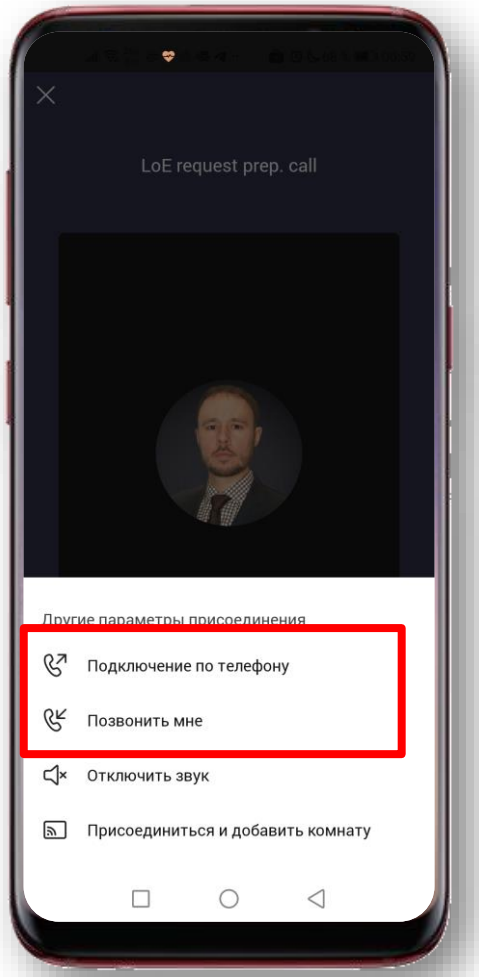
Возможности Office 365 A5

Название опции	Описание или основной функционал	Сценарий
Audio Conferencing	Аудио-конференции Teams	Если пользователь является организатором конференции, то: • В эту конференцию можно позвонить снаружи по телефону. • Из конференции можно позвонить на мобильный телефон и добавить абонента в конференцию. Эта возможность есть даже у пользователей без лицензии. • Возможность войти в конференцию с мобильного телефона. На каждого пользователя выделяется 900 минут в месяц*.

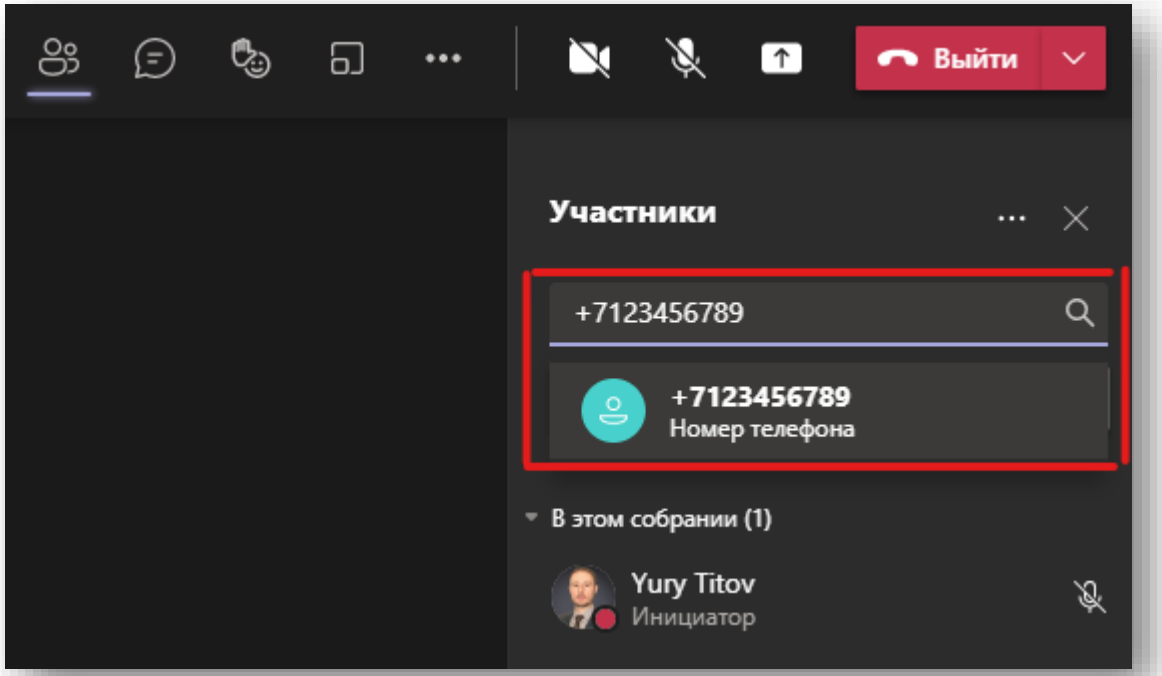
Microsoft 365: Protecting sensitive emails with policy-driven compliance - YouTube

*Подробности по ссылке - ссылка

Возможности Office 365 A5. Audio Conferencing



С телефона



С персонального компьютера

[Microsoft 365: Protecting sensitive emails with policy-driven compliance - YouTube]

Возможности Office 365 A5

Название опции	Описание или основной функционал	Сценарий
Phone System	Телефония	Пользователи с данной лицензией могут воспользоваться функциями телефонии, такими как: приём или совершение вызовов, удержание и перевод. Для подключения к сети общего пользования требуется настройка Direct routing и наличие специализированного голосового шлюза из списка совместимых.

Phone System Direct Routing - Microsoft Teams | Microsoft Docs
Session Border Controllers certified for Direct Routing - Microsoft Teams | Microsoft Docs

Возможности Office 365 A5

Название опции	Описание или основной функционал	Сценарий
Microsoft Defender for Office 365	Дополнительная защита от фишинговых атак Безопасные ссылки	Одним из основных способов проникновения злоумышленников внутрь организации является похищение учётных данных путём фишинга. Пользователь получает письмо с ссылкой на опасный сайт, и нажимает на неё. Если используется данная функция, то ссылка открывается не напрямую, а через облако Office 365, где происходит анализ сайта на предмет безопасности. Если сайт небезопасен, выводится соответствующее предупреждение. Преимущество в том, что проверка происходит непосредственно в момент нажатия на ссылку. Интерактивные отчёты по обнаруженным событиям в Security & Compliance Center.
	Безопасные вложения	Проверка вложений электронной почты, приходящих из сети Интернет в ящик конкретного пользователя, на предмет безопасности.

Возможности Office 365 A5

Название опции	Описание или основной функционал	Сценарий
Advanced Message Encryption	Шифрование сообщений электронной почты	Применение ограничений на просмотр, пересылку электронного сообщения пользователя на основе правил, меток (например, номер кредитной карты) или в ручном режиме. Например, вы хотите, чтобы электронное сообщение с маркировкой «Конфиденциально» было недоступно за пределами организации. Или вы хотите, чтобы конкретное сообщение было доступно для прочтения только определённым адресатам внутри или за пределами организации.

Microsoft 365: Protecting sensitive emails with policy-driven compliance - YouTube

Возможности Office 365 A5

Название опции	Описание или основной функционал	Сценарий
Advanced Audit	Расширенный аудит действий пользователя	Данная функция позволяет увеличить лог действий пользователя со стандартных 90 дней до 1 года. Протоколирование ведётся по ключевым действиям пользователя при работе с файлами, письмами в сервисах Exchange Online и SharePoint Online. Обычно данная функция применяется при проведении расследований, связанных с компрометацией учетных записей. Если у пользователя включена данная функция, то можно определить масштаб бедствия, поняв – к каким файлам или письмам успел получить доступ злоумышленник.

Microsoft 365 Advanced Auditing for forensic and compliance investigations - YouTube

Возможности Office 365 A5

Название опции	Описание или основной функционал	Сценарий
Compromised user detection	Автоматическое обнаружение скомпрометированной учётной записи пользователя	При взломе учетной записи пользователя возникает нетипичное или аномальное поведение. Например, фишинговые и спам-сообщения могут быть отправлены внутри от учетной записи пользователя. Данная функция может обнаруживать такие аномалии в шаблонах электронной почты и совместной работе в Office 365. Когда это происходит, срабатывают предупреждения и начинается процесс устранения угроз.

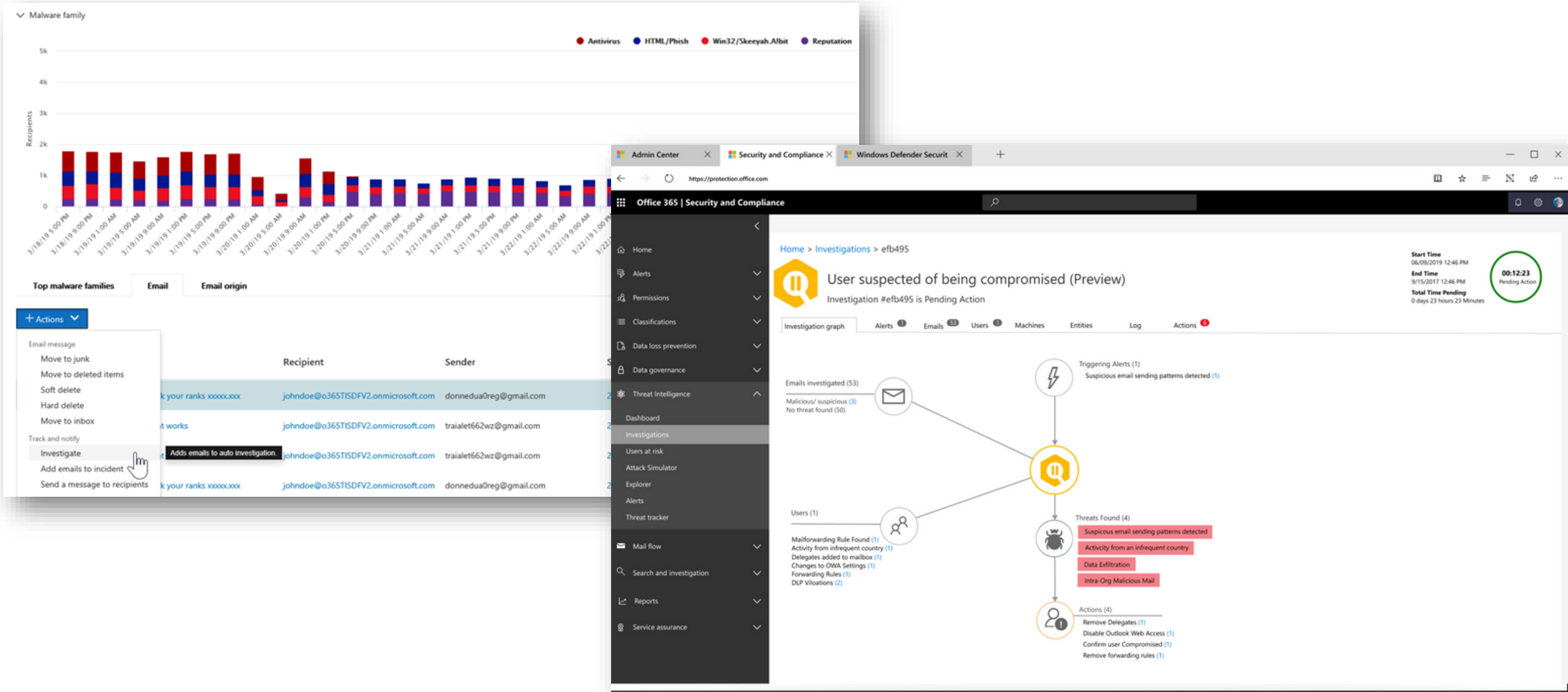
Detect and respond to compromise in Microsoft Defender for Office 365 – YouTube
Address compromised user accounts with automated investigation and response - Office 365 | Microsoft Docs

Возможности Office 365 A5

Название опции	Описание или основной функционал	Сценарий
Automated investigation and response (AIR)	Автоматическое расследование	Автоматическое создание инцидентов, связанных с аномальной активностью пользователя или различными атаками. Решение позволяет связать различные процессы в единую цепочку (кейс) и предложить службе безопасности быстрые способы для устранения угроз, такие как – блокировка, сброс пароля, очистка почтовых ящиков и пр.

Microsoft 365: Protecting sensitive emails with policy-driven compliance – YouTube
Detect and respond to compromise in Microsoft Defender for Office 365 - YouTube

Возможности Office 365 A5. Automated investigation and response (AIR)



Возможности Microsoft 365 A3

Возможности Microsoft 365 A3

Название опции	Описание или основной функционал	Сценарий
MFA with conditional access	Двухфакторная аутентификация с условным доступом	Решение позволяет повысить безопасность вашей системы, за счёт организации дополнительной проверки пользователя во время аутентификации через сервисы Microsoft. Условный доступ - это механизм проверки каждого процесса подключения к системе на основе настроенного сценария и решения, устанавливающего, что делать с этим подключением. Например, при подключении из неизвестной сети, к определённому приложению или с неизвестного устройства, система попросит подтвердить личность при помощи второго фактора: телефон, приложение. Внедрение решения позволяет повысить защиту от фишинговых атак, когда пользователь неумышленно вводит свои учётные данные на опасных сайтах.

Что такое условный доступ в Azure Active Directory? | Microsoft Docs

Возможности Microsoft 365 A3

Название опции	Описание или основной функционал	Сценарий
Self Service Password Recovery (SSPR)	Сброс пароля	Самостоятельный сброс пароля пользователем при помощи второго фактора. Внедрение данной опции позволяет повысить удобство использования гибридных сервисов Microsoft и снизить нагрузку на существующее решение по сбросу пароля.

Возможности Microsoft 365 A3

Название опции	Описание или основной функционал	Сценарий
Password writeback	Перезапись изменённого пароля в облаке назад в корпоративный каталог в корпоративной сети	Если у заказчика есть интеграция локального AD с облачным Azure AD, то: • Без данной опции. Пользователь меняем пароль в облаке, но он затирается паролем из локального AD при следующей процедуре синхронизации. • С данной опцией. Пароль из облачного AD возвращается в корпоративный AD и заменяет его.

Возможности Microsoft 365 A3

Название опции	Описание или основной функционал	Сценарий
Dynamic Group	Динамические группы в Azure AD	Возможность автоматического добавления пользователя в ту или иную группу на базе атрибутов его учётной записи. Например: Пользователь определённого филиала будет автоматически добавлен в группу пользователей всего этого филиала. Преподаватель будет добавлен в группу «Преподаватели». Если атрибуты пользователя меняются, то пользователь удаляется из группы также в автоматическом режиме. После попадания в нужную группу, пользователь получает доступ к заранее сконфигурированным для данной группы ресурсам (сайт, рассылка, хранилище и пр). Внедрение данного решения позволяет значительно упростить нагрузку на администратора, который управляет назначениями лицензий, а также сэкономить время на получение доступа пользователя к нужным ресурсам (а впоследствии, удаление этого доступа).

Возможности Microsoft 365 A3

Название опции	Описание или основной функционал	Сценарий
Dynamic Group Licensing	Динамическое лицензирование пользователей на базе принадлежности к группе	Пользователю автоматически назначается та или иная лицензия в зависимости от принадлежности к определённой группе. Данная технология позволяет свести к минимуму ручное назначение лицензий и значительно сократить временные затраты в крупных организациях.

Возможности Microsoft 365 A3

Название опции	Описание или основной функционал	Сценарий
Self-service Group Management	Самообслуживание групп пользователей без необходимости вовлечения администратора	Возможность пользователям самостоятельно обслуживать подключение к той или иной группе через отдельный портал. Решение позволяет организовать процесс самообслуживания и значительно снизить нагрузку с группы системных администраторов, которые управляли данным процессом до этого. Set up self-service group management - Azure Active Directory | Microsoft Docs

Возможности Microsoft 365 A3

Название опции	Описание или основной функционал	Сценарий
Azure Information Protection	Защита данных посредством наложения шифрования файлов и управления доступом	Microsoft Azure Information Protection помогает защитить данные в условиях их постоянного перемещения между пользователями, устройствами и приложениями. При создании файла, он классифицируются, конфиденциальные данные попадают под защиту с помощью шифрования и разграничения прав доступа. Открыть данный файл смогут лишь те пользователи, которые входят в специальные группы пользователей (например, только внутренние сотрудники вуза). Таким образом, даже если секретный файл попадёт в чужие руки, злоумышленник не сможет его открыть, так как при открытии будет выполнен запрос в систему AIP.

Возможности Microsoft 365 A3

Название опции	Описание или основной функционал	Сценарий
Cloud App Discovery	Функция обнаружения использоания несанкционированных приложений в компании	Анализ логов траффика с корпоративного Firewall на предмет обнаружения запрещённых или опасных приложений на ПК пользователей. Так называемое обнаружение Shadow IT. Внедрение данного сервиса помогает службе ИТ вуза обнаружить приложения, которые пользователи самостоятельно установили на свои ПК, а также их сетевую активность. Решение позволяет повысить безопасность сети.

Deploy Cloud Discovery | Microsoft Docs

Возможности Microsoft 365 A3

Название опции	Описание или основной функционал	Сценарий
Microsoft Intune		Облачная система управления устройствами на базе Windows 10, MAC или мобильными устройствами пользователя (iOS, Android), позволяющая управлять устройствами удалённо, располагающимися вне корпоративной сети вуза: • Принудительная настройка устройств на базе специальных профилей. • Установка, удаление ПО. • «Перезаливка» (сброс до начального состояния и установка нужных приложений). • Инвентаризация аппаратного обеспечения. • Инвентаризация программного обеспечения. • Подробная отчётность. • Возможность подключения к БД Intune средствами PowerBi Pro для создания персональных дашбордов.

Возможности Microsoft 365 A3

Название опции	Описание или основной функционал	Сценарий
Windows 10 E3		Расширенные функции безопасности, встроенные в Windows 10

Возможности Microsoft 365 A3

Название опции	Описание или основной функционал	Сценарий
Azure AD Application Proxy	Использование Azure AD Application Proxy для публикации локальных приложений для удаленных пользователей	Azure AD Application Proxy могут реализовать ИТ-специалисты, которым требуется опубликовать во внешней сети локальные корпоративные веб-приложения. В этом случае удаленные пользователи, которым требуется доступ к внутренним приложениям, смогут получить к ним безопасный доступ на базе MFA и условного доступа. Например у заказчика есть локальный сервер Exchange. Данный сервер имеет web-портал для работы с ним пользователями – Outlook Web Access (OWA). При помощи решения Azure AD Application Proxy можно повысить безопасность доступа к данному интерфейсу через инструменты Azure AD.

Возможности Microsoft 365 A3

Название опции	Описание или основной функционал	Сценарий
Право на подключение к WVD		Доступ в платформе виртуализации рабочих столов или приложений Windows Virtual Desktop на базе Azure.

Возможности Microsoft 365 A5

Возможности Microsoft 365 A5

Название опции	Описание или основной функционал	Сценарий
Defender for Endpoint	Антивирус нового поколения, встроенный в Windows 10 + облачная платформа для анализа	Microsoft Defender for Endpoint — это платформа безопасности для интеллектуальной защиты, обнаружения, исследования и реагирования. Microsoft Defender for Endpoint защищает конечные точки от угроз кибератак, обнаруживает сложные атаки и нарушает данные, автоматизирует инциденты безопасности и улучшает безопасность. Microsoft Defender для конечной точки использует защиту следующего поколения, предназначенную для улавливания всех типов возникающих угроз. Microsoft Defender for Endpoint представляет собой EDR решение, располагающееся в облаке Microsoft 365 на базе технологий: • Датчики встроенные в Windows 10 • Облачная аналитика поведения и безопасности на базе больших данных • Дополнительные сведения об угрозах от глобальной системы Microsoft

Возможности Microsoft 365 A5

Название опции	Описание или основной функционал	Сценарий
Defender for Endpoint (Mobile)		Microsoft Defender for Endpoint для мобильных устройств

Возможности Microsoft 365 A5

Название опции	Описание или основной функционал	Сценарий
Cloud App Security		Дополнение к системе Cloud App Discovery. Microsoft Cloud App Security интегрируется с Microsoft Defender for Endpoint и использует сведения о трафике, собранные с устройств Windows 10. Интеграция упрощает развертывание Cloud Discovery, расширяет возможности Cloud Discovery **за пределами корпоративной сети,** обеспечивая расследования на основе информации с конкретных устройств.

[Integrate Microsoft Defender for Endpoint with Cloud App Security | Microsoft Docs]

Возможности Microsoft 365 A5

Название опции	Описание или основной функционал	Сценарий
Threat Analytics		Threat Analytics - это набор отчетов экспертов Microsoft security researchers, охватывающих наиболее актуальные угрозы, в том числе: • Активные субъекты угроз и их кампании • Популярные и новые методы атаки • Критические уязвимости • Общие поверхности атаки • Распространенные вредоносные программы В каждом отчете содержится подробный анализ угрозы и подробные рекомендации по защите от этой угрозы. В данном отчёт также включены визуальные **данные из сети вашей организации**, указывающие, активна ли у вас конкретная угроза и есть ли у вас применимые средства защиты.

[Track and respond to emerging threats with Microsoft Defender for Endpoint threat analytics | Microsoft Docs]