Функции упорядоченных наборов

Windows IT Pro/RE

№8 АВГУСТ 2017 | WWW.WINDOWSITPRO.RU | ИНФО ДЛЯ ИТ-ПРО

Мобильная версия

App Store

Google play

Защита информации в Office 365

ISSN 1563-101X

Windows IT Pro/RE
№8 август 2017
12+

Содержание

Издание для специалистов, интересующихся технологиями компании Microsoft.

Главный редактор: **Д. Ю. Торопов** (toropovd@osp.ru)
Ответственный редактор: **Е. Петровичева**
Корректор: **Л. Теременко**
Верстка и дизайн: **О. Шуранова**
Номер также готовили: **Е. Овсянников**
Т. Евдокимова, А. Китаев, А. Федотов,
Н. Басалова, Ю. Власов, Д. Щепкин, А. Адзиев

Адрес для писем: 123056, Москва, а/я 82
Телефоны: (495) 725-4780/83, (499) 703-1854
Факс: (495) 725-4783
E-mail: windowsitpro@osp.ru

Журнал зарегистрирован в Роскомнадзоре.

Свидетельство о регистрации средства массовой информации ПИ № ФС 77-63737 от 16 ноября 2015 г.
Дата выхода в свет — 18.08.2017 г.

Цена свободная. Выходит 12 раз в год.

ОТКРЫТЫЕ СИСТЕМЫ
Open Systems Publications

Учредитель и издатель:
ООО «Издательство «Открытые системы»
127254, Москва, пр-д Добролюбова, д. 3, стр. 3, каб. 13.
Президент **М. Е. Борисов**
Генеральный директор **Г. А. Герасина**
Директор ИТ-направления **П. В. Христов**
Коммерческий директор **Т. Н. Филина**
Подписные индексы:
Объединенный каталог «Пресса России» — 38185,
«Каталог российской прессы» — 99483,
ФГУП «Почта России» — П2337
Отпечатано в ООО «Богородский полиграфический комбинат»,
142400, Московская обл., г. Ногинск, ул. Индустриальная, д. 40б
Тираж: 6900 экз. — печатная версия,
3280 экз. — PDF-версия

ИЛЛЮСТРАЦИЯ НА ОБЛОЖКЕ LUCADP© (FOTOLIA.COM)

Предотвращение утечек данных в Office 365

Лиам Клири

После включения в Office 365 компонента Security and Compliance Center пользователи получили возможность управления сложными инструментами, потребность в которой ощущалась уже довольно давно. К числу таких базовых инструментов относится компонент защиты от утечек данных, Data Loss Prevention. Этот модуль платформы Office 365 позволяет определять политики, которые предусматривают действия в отношении информации, соответствующие определенным правилам, а также направляют конечному пользователю уведомления о том, что данная информация тем или иным образом нарушает некое правило.

В этой статье будет поэтапно описан процесс формирования политик Data Loss Prevention с помощью нового мастера, недавно модернизированного для платформы Office 365.

Чтобы обратиться к центру Security & Compliance, перейдите в центр администрирования Office 365, затем раскройте раздел Admin Centers и выберите пункт Security & Compliance (экран 1).

В вашем браузере появится новая вкладка, отображающая центр Security & Compliance. Откройте раздел Data loss prevention и выберите пункт Policy (экран 2).

После загрузки страницы Policy на экране будут отображены политики (если они у вас уже сформулированы). Если же вы пока не приступали к формированию политик, экран останется пустым, и вы сможете создавать новые политики по мере необходимости. Чтобы создать политику, нажмите кнопку «+ Create Policy», после чего на экране появится мастер в правой части браузера поверх текущей страницы, как показано на экране 3.

Политика DLP включает в себя такие составляющие, как тип конфиденциальности Sensitive Type, расположение содержимого Locations of Content и специальные настройки Policy Settings. Для выбора уровня Sensitive Type выделите соответствующую категорию на отображаемой панели, а затем выберите нужный вам тип (экран 4).

После того как вы выберете компонент Sensitive Type, на экране будут отображены детали избранного варианта. Например, в законах

Дополнительная информация

- http://sharepointpromag.com/sharepoint/data-loss-prevention-sharepoint-premises-and-online
- https://blogs.office.com/2017/01/09/unifying-data-loss-prevention-in-office-365/
- https://support.office.com/en-us/article/View-the-reports-for-data-loss-prevention-41eb4324-c513-4fa5-91c8-8fbd8aaba83b

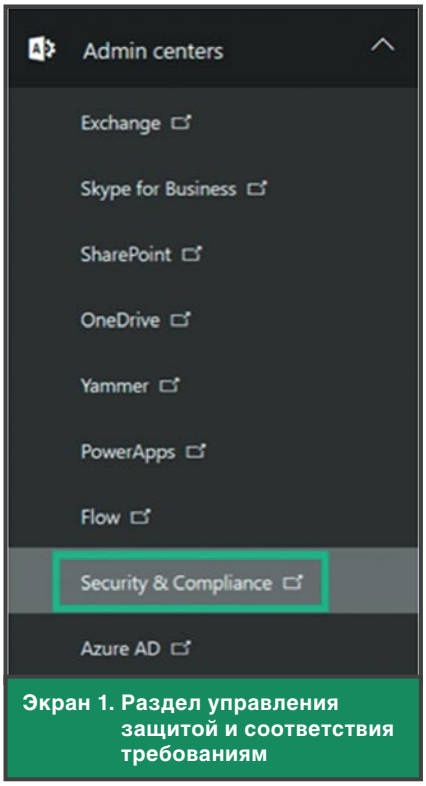
США, касающихся уведомления физических лиц со стороны частных или государственных организаций о случаях взлома механизмов защиты информации, соотносимой с конкретной личностью, U.S. State Breach Notification Laws, речь идет о данных, представляющих комбинацию номера кредитной карты, номера счета в банке США, номера американских водительских прав и номера социального страхования (U.S. Social Security Number, SSN). Завершив выбор, вы можете указать имя политики и перейти к выбору вариантов локации (экран 5).

По состоянию на сегодня модуль Data Loss Prevention предоставляет возможность выбора из ограниченного набора мест, то есть выбрать произвольное местоположение информации вы не можете. По умолчанию пользователю предлагается вариант All locations in Office 365. Сюда включается содержимое электронной почты Exchange, а также документы OneDrive и SharePoint. Однако пользователь может выбирать специализированные хранилища данных, подключать или отключать их, а затем указывать сайты SharePoint или учетные записи OneDrive для их подключения (экран 6).

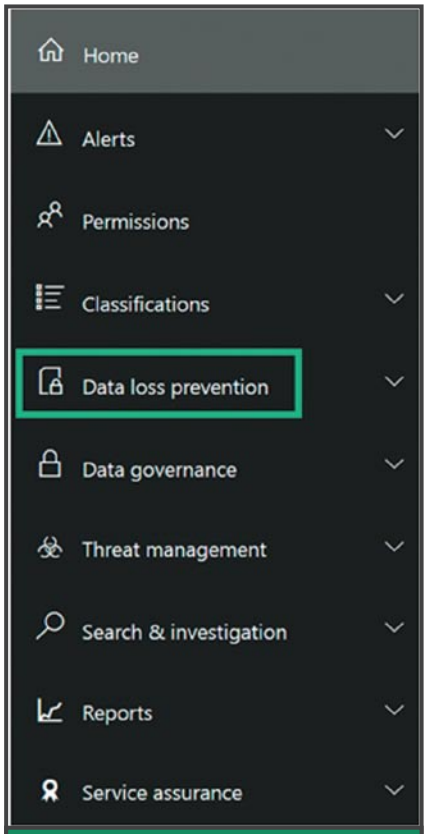
Чтобы добавить источник информации SharePoint или OneDrive, просто щелкните на ссылке Choose sites или Choose accounts, выберите нужный указатель URL и добавьте его в список. Позднее вы сможете добавлять новые источники по мере необходимости. Указатели URL для сайтов SharePoint должны быть указателями на коллекцию сайтов (https://name.domain.com), тогда как у сайтов OneDrive они должны иметь формат https://name-my.sharepoint.com/personal/username.

Далее вам нужно указать, какие настройки следует применять, простые или расширенные. Простые настройки дают пользователю возможность модифицировать типы конфиденциальности и указывать, когда их следует выявлять (экран 7).

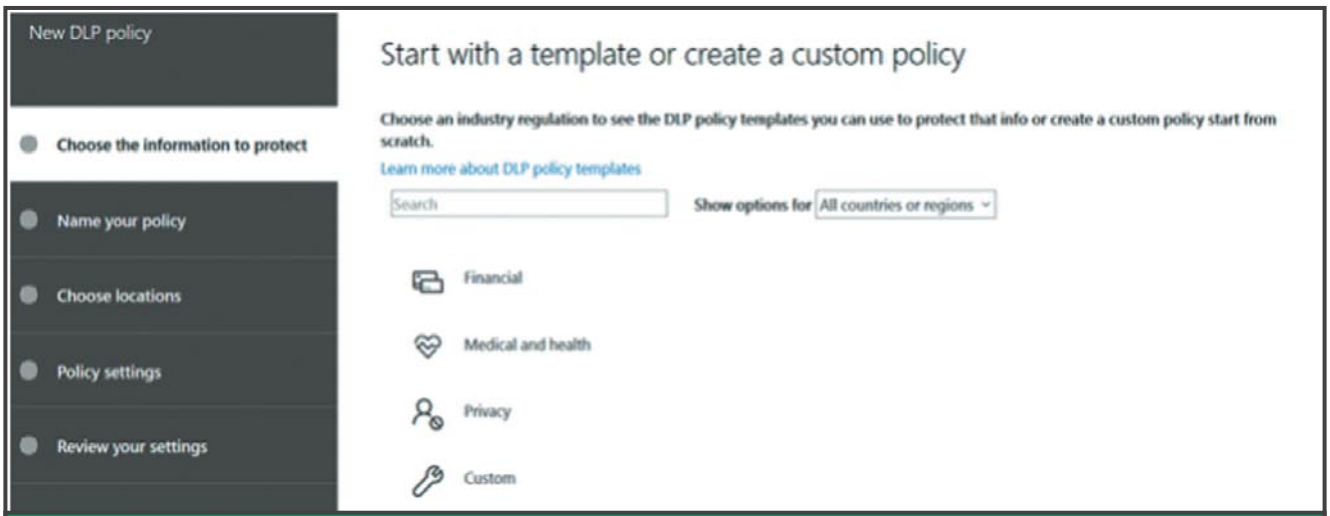
Все настройки могут быть модифицированы на экране правил в разделах Conditions, Actions,



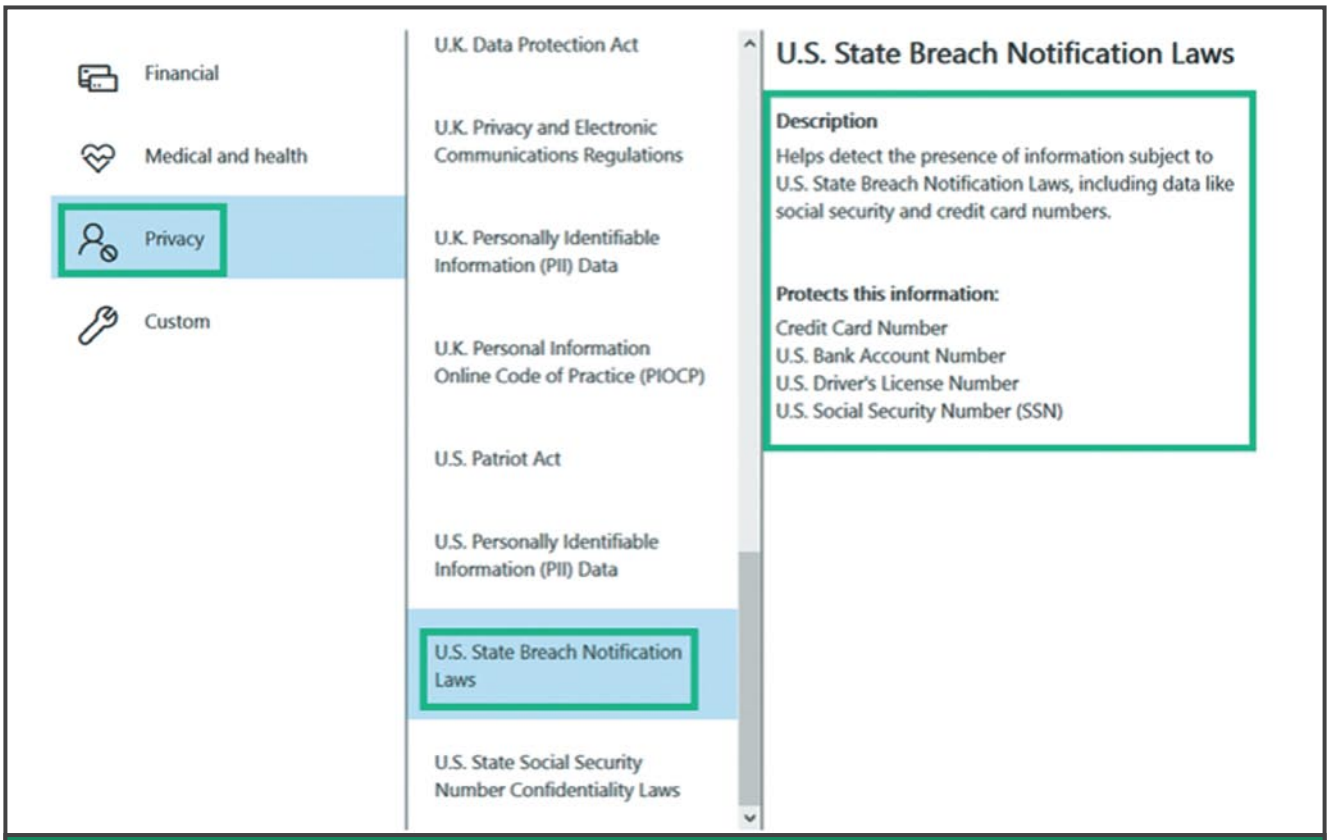
Экран 1. Раздел управления защитой и соответствия требованиям



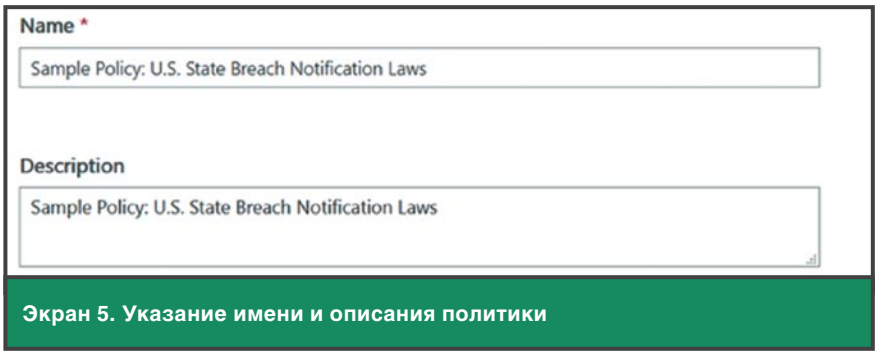
Экран 2. Раздел защиты от утечек данных



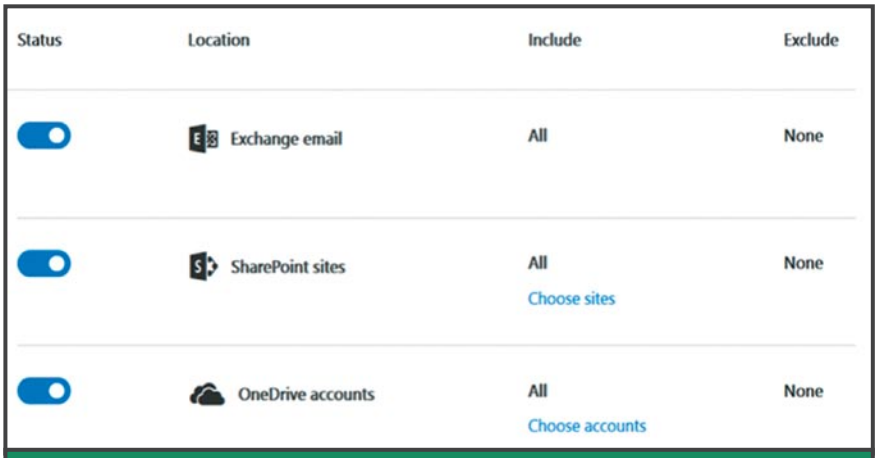
Экран 3. Мастер создания новой политики



Экран 4. Выбор типа конфиденциальности информации



Экран 5. Указание имени и описания политики



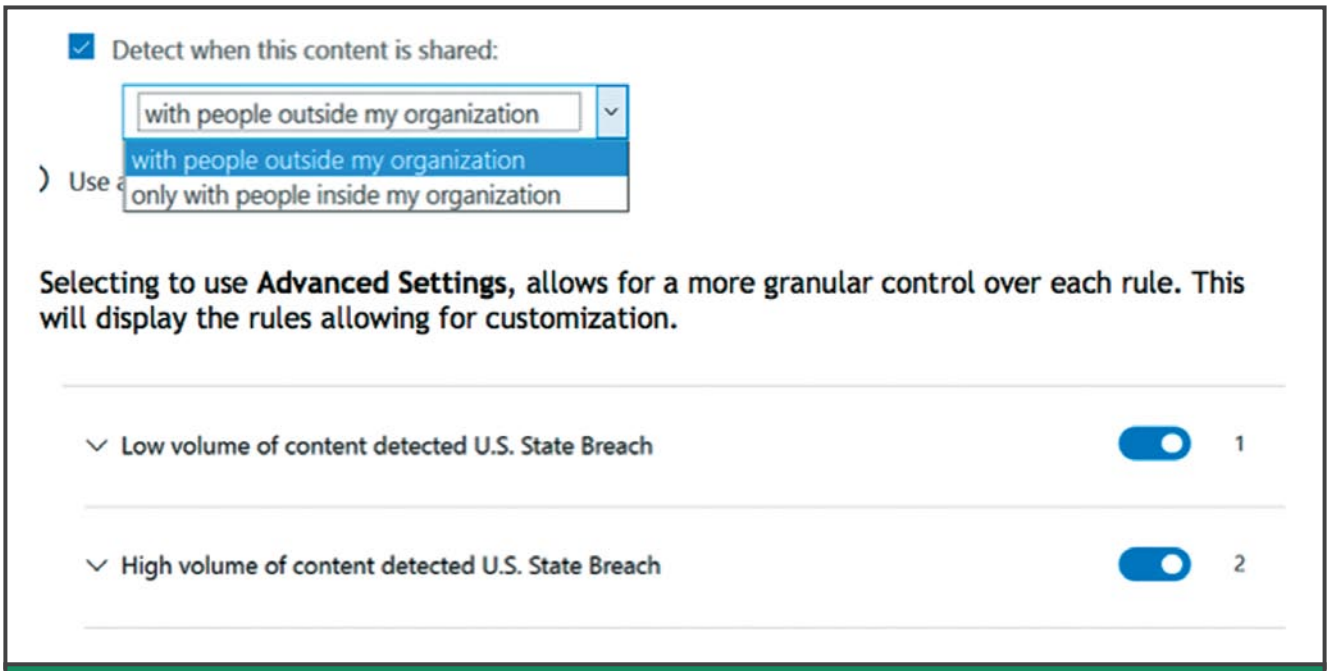
Экран 6. Выбор места расположения проверяемой информации

User Notifications, User Overrides и Incident Reports. В качестве примера, для выбранных типов конфиденциальности каждая метрика, определяемая по умолчанию, может быть изменена по мере необходимости (экран 8).

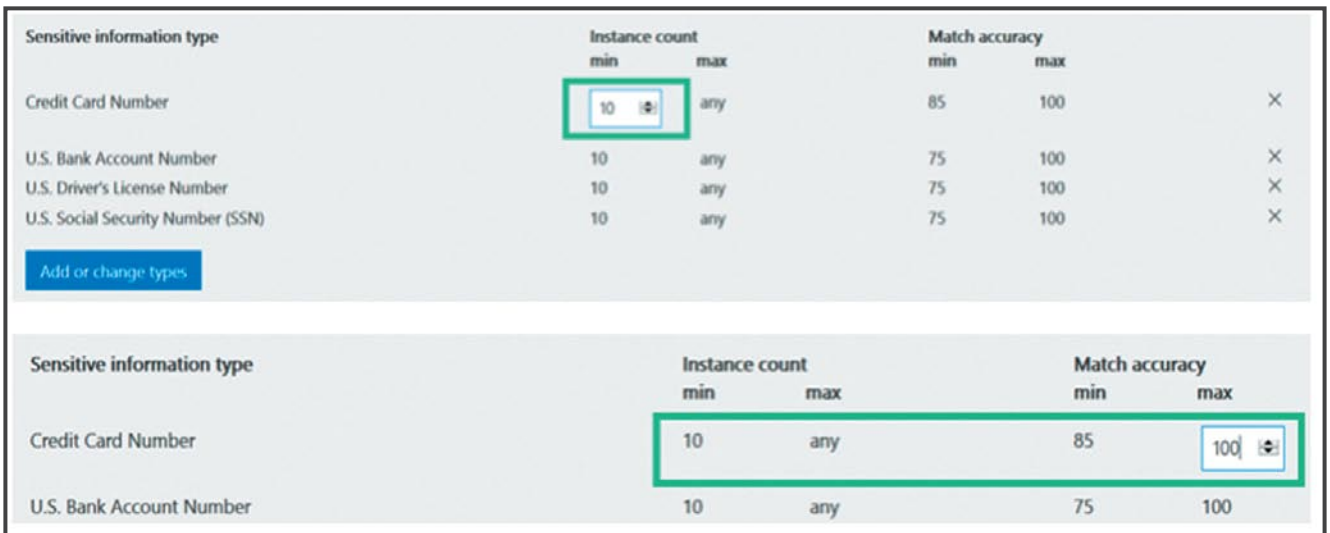
После того как все настройки будут выполнены, вы сможете сохранить все правило целиком, а затем его можно будет либо протестировать, либо применить и перевести в активный режим (экран 9).

Как видите, использование и создание правил защиты от утечек данных Data Loss Prevention не вызывает особых затруднений. Далее процесс незаметно для пользователя проверит информационное содержимое с помощью функции поиска SharePoint и применит правила по необходимости.

Интерфейс конечного пользователя просто модифицирует способ отображения файлов, чтобы можно было воспользоваться новым значком, и затем согласно правилам либо отказывает в доступе, либо



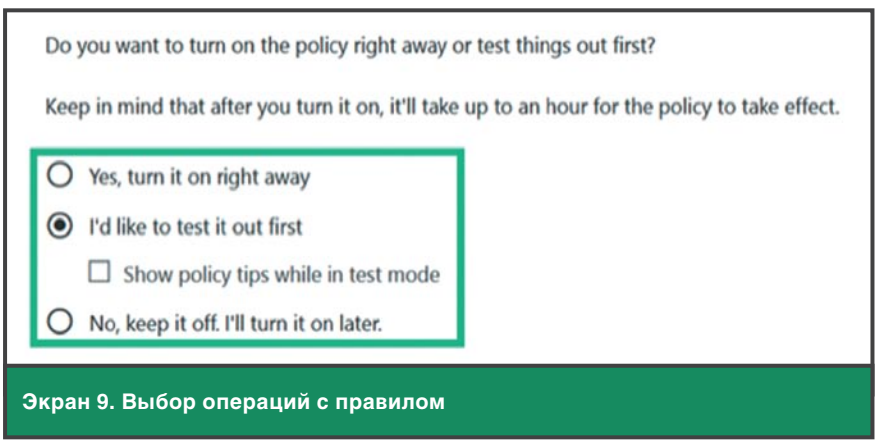
Экран 7. Указание условия отслеживания действий с информацией



Экран 8. Детальная настройка политики

предоставляет его с указаниями относительно политик, разъясняющими пользователю, что следует предпринять.

Более подробная информация о функции защиты от утечек данных Data Loss Prevention, реализованной в Office 365 или SharePoint 2016 On-Premises, приведена во врезке «Дополнительная информация».



Экран 9. Выбор операций с правилом

Лиам Клири — архитектор решений, имеет сертификат Microsoft MVP

Создание отчетов в Office 365

При навигации по Центру безопасности и соответствия требованиям Security & Compliance вы можете просматривать подробные отчеты для Office 365. Для доступа к отчетам разверните раздел отчетов Reports и выберите панель мониторинга Dashboard (экран 1).

После того как откроется панель мониторинга, вы увидите, что сейчас она не содержит большого числа элементов (экран 2). Эта страница представляет собой просто заполнитель места для отчетов, которые будут доступны в дальнейшем. Чтобы запустить отчеты в центре безопасности и соответствия требованиям, выберите любой из четырех участков из раздела Search & Investigation («Поиск и исследование»), как показано на экране 3.

Наиболее часто используемый — Audit log search («Поиск по журналу аудита»), в котором приведены подробные сведения о том, что конечные пользователи могли делать на сайте (экран 4).

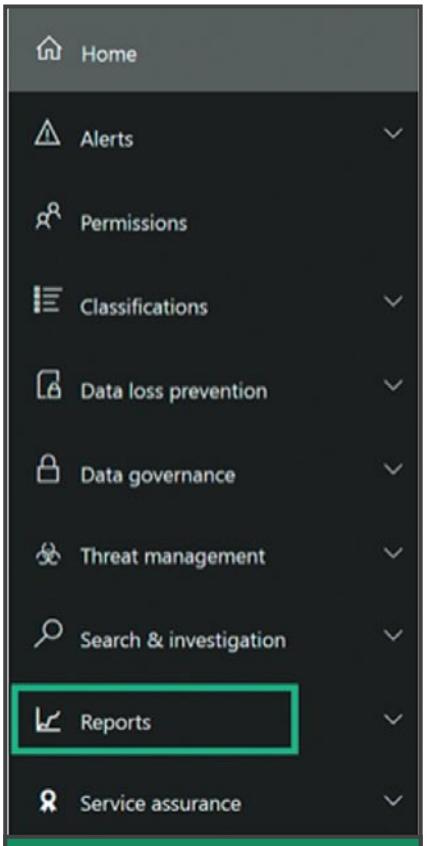
В процессе поиска первый шаг — выбрать Activities («Действия»), которые вы хотите увидеть (экран 5).

Список действий очень обширный, он охватывает следующие категории операций:

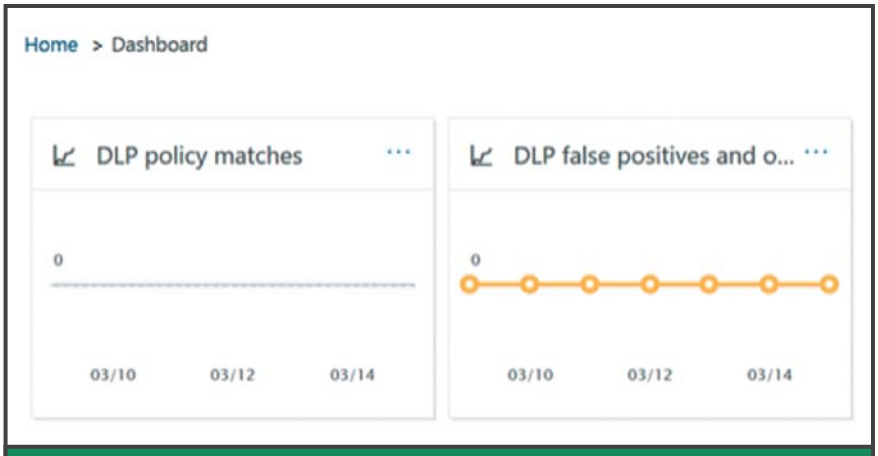
1. Действия с файлами и папками.
2. Действия по общему доступу и запросам доступа.
3. Действия по синхронизации.
4. Действия по администрированию сайтов.
5. Действия с почтовым ящиком Exchange.
6. Действия Sway.
7. Действия по администрированию пользователей.
8. Действия по администрированию группы AD Azure.
9. Действия по администрированию приложений.
10. Действия по администрированию ролей.
11. Действия по администрированию каталогов.
12. Действия eDiscovery.
13. Действия Power BI.
14. Действия с группами Microsoft.

Как видите, список велик. Если мы выбираем категорию Directory administration activities («Действия по администрированию каталогов»), то будут выбраны все действия (экран 6).

Выбирая нужные действия, мы получаем возможность выполнять поиск на основе конкретного критерия и дат. Поиск возвращает данные о пользователе, который выполняет действие, а также обновляемый или изменяемый объект наряду с учет-



Экран 1. Раздел отчетов Reports



Экран 2. Панель мониторинга