



# ЗАЩИТИТЕ СВОЙ ОФИС

**Canon**

---



# НАСКОЛЬКО ЗАЩИЩЕНА ИНФОРМАЦИЯ В ВАШЕМ ОФИСЕ?

Современные предприятия в значительной степени полагаются на информацию, создавая сложные и высокотехнологичные сети, объединяющие процессы, людей и организации, находящиеся в разных странах. Появляются новые гибкие методы работы, которые трансформируют не только офисное пространство, но и то, как люди создают, передают и используют информацию. В столь сложной среде защиту данных уже не обеспечить с помощью старых методов, и большинство компаний инвестируют в высокотехнологичные решения, такие как брандмауэры, новые антивирусы, программные инструменты обеспечения безопасности и многое другое. Однако зачастую им не удается понять, что защищать нужно и офисные принтеры, которые гораздо более уязвимы, чем может показаться на первый взгляд.



## ЗАДУМАЙТЕСЬ О СВОИХ ПРИНТЕРАХ

Современные многофункциональные принтеры являются мощными инструментами, которые, так же как сервер или ПК, имеют свои операционные системы, жесткие диски большого объема, подключение к сети и Интернету, а также ежедневно используются для обработки огромного количества важнейших корпоративных документов.



## В ЧЕМ ЗАКЛЮЧАЕТСЯ РИСК?

- Несанкционированный просмотр конфиденциальной информации, хранящейся на незащищенных МФУ.
- Доступность вашей инфраструктуры печати может быть нарушена из-за неправильной работы.
- Злоумышленники получают доступ к вашей сети через принтер и используют его для дальнейших атак.
- Доступ к конфиденциальным документам, забытым в выходном лотке после печати.
- Общая стопка напечатанных заданий, принадлежащих разным пользователям.
- Отправка документов факсом или по электронной почте неверным адресатам в результате опечатки.
- Перехват печатаемых или сканируемых данных хакерами.
- Утеря данных в результате небрежной утилизации принтеров в конце их жизненного цикла.

«Внедрение основных стандартов информационной безопасности является стоящим вложением средств для офисов, в которых обрабатываются большие объемы данных. В наши дни принтер перестал быть простым устройством, теперь это сервер с функцией печати».

(руководитель отдела информационной безопасности, Publicis Groupe)

# БЕЗОПАСНЫЕ РЕШЕНИЯ ДЛЯ ПЕЧАТИ В ВАШЕЙ КОМПАНИИ

## Встроенные функции безопасности и конфиденциальности

Когда мы разрабатываем или выбираем технологии, продукты и услуги для наших клиентов, мы учитываем их возможное влияние на рабочую среду наших клиентов. Именно поэтому наши офисные многофункциональные принтеры оснащены широким набором встроенных и дополнительно приобретаемых функций безопасности, которые позволяют компаниям любого размера достичь необходимого уровня защиты для:



УСТРОЙСТВ



СЕТЕЙ



ДОКУМЕНТОВ



ПРЕДПРИЯТИЯ



### МЕЖДУНАРОДНЫЕ СТАНДАРТЫ И СЕРТИФИКАТЫ

Наши многофункциональные принтеры imageRUNNER ADVANCE проходят регулярную оценку и сертификацию на соответствие общим критериям и требованиям стандарта IEEE2600 по безопасности печатных устройств.



### ПРОВЕРКА БЕЗОПАСНОСТИ

Компания Canon использует один из самых строгих режимов проверки безопасности во всей индустрии офисного оборудования. Технологии, используемые в наших устройствах, тестируются на соответствие тем стандартам, которым должна соответствовать наша компания.

Являясь лидером в области разработки инновационных решений для печати и управления информацией в офисах и компаниях, Canon работает совместно с клиентами, помогая им использовать комплексный подход к информационной безопасности, который подразумевает, что меры безопасности в технологиях для офиса являются частью общей информационной экосистемы.



# ЗАЩИТИТЕ СВОЕ УСТРОЙСТВО

## Комплексная защита ваших физических активов



### РЕШЕНИЯ ДЛЯ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ

Защитите устройство от несанкционированного использования, внедрив контроль доступа пользователя с помощью аутентификации. Это также позволит пользователям быстрее получать доступ к нужным параметрам и заданиям печати, в то же время повышая видимость и прозрачность процессов. Наши офисные принтеры оборудованы гибким решением для входа Universal Login Manager, которое обеспечивает аутентификацию пользователей по базе данных на устройстве, по домену через Active Directory или через сервер uniFLOW. Это дает возможность контролировать доступ к устройству и достичь баланса между удобством пользователей и безопасностью.



### АДМИНИСТРИРОВАНИЕ УСТРОЙСТВА

Конфигурация устройства, а также параметры сети и другие возможности управления доступны только пользователям с правами администратора — это необходимо во избежание случайного или преднамеренного изменения конфигурации.



### СИСТЕМА УПРАВЛЕНИЯ ДОСТУПОМ

Эта функция позволяет предоставлять доступ к каждой отдельной функции устройства. Администраторы могут использовать стандартные доступные роли или создавать пользовательские роли с необходимыми правами и уровнем доступа. Например, некоторым пользователям можно ограничить доступ к копированию документов или использованию функции отправки.



### НАСТРОЙКА ПОЛИТИКИ БЕЗОПАСНОСТИ

Новейшие устройства imageRUNNER ADVANCE также оснащены функцией политики безопасности, которая позволяет администратору управлять всеми параметрами безопасности в одном меню и редактировать их до применения в качестве конфигурации устройства. После применения использование устройства и изменение параметров должны происходить в соответствии с этой политикой. Политику безопасности можно защитить отдельным паролем, чтобы она обеспечивала дополнительные возможности управления и безопасность, а доступ к ней был только у ответственного специалиста по ИТ-безопасности.



### ЗАЩИТА ДАННЫХ НА ЖЕСТКОМ ДИСКЕ

На многофункциональном принтере всегда хранится большой объем данных, которые необходимо защищать, — от заданий на печать, находящихся в очереди, до полученных факсов, отсканированных изображений, адресных книг, журналов активности и истории заданий. Устройства Canon предлагают ряд инструментов для защиты данных на всех этапах жизненного цикла устройства, а также для сохранения их конфиденциальности, целостности и доступности.



### ПРЕВЕНТИВНАЯ ЗАЩИТА

Продукты imageRUNNER ADVANCE предлагают ряд настроек безопасности, которые позволяют защитить принтеры от атак. Функция безопасной загрузки обеспечивает целостность системы устройства, а данные системного журнала предоставляют актуальную информацию о безопасности устройства, которую можно расшифровать совместимой сторонней системой SIEM.



## НАСКОЛЬКО ХОРОШО ЗАЩИЩЕНЫ ВАШИ УСТРОЙСТВА?

**1**

Ваши устройства расположены в общественных местах?

**2**

Могут ли пользователи получить незащищенный доступ к устройствам?

**3**

Используете ли вы инструменты для защиты информации на жестком диске устройства?

**4**

Можно ли получить несанкционированный доступ к настройкам устройства?

**5**

Задумывались ли вы о жизненном цикле и безопасной утилизации вашего устройства?

### ШИФРОВАНИЕ ЖЕСТКОГО ДИСКА

Наши устройства imageRUNNER ADVANCE шифруют все данные на жестком диске для повышения уровня безопасности. Чип безопасности, отвечающий за шифрование данных, соответствует стандарту безопасности FIPS 140-2 уровня 2, принятому правительством США, и сертифицирован в рамках программы CVMP (программа проверки криптографических модулей), организованной США и Канадой, а также ее японского аналога JCVMP.

### ОЧИСТКА ЖЕСТКОГО ДИСКА

Некоторые данные, например данные скопированных или отсканированных изображений, а также данные документов, распечатанных с компьютера, хранятся на жестком диске принтера ограниченное время и удаляются после выполнения соответствующего задания. Чтобы гарантировать полное удаление остаточных данных наши устройства оснащаются жестким диском с возможностью регулярного удаления остаточных данных в качестве этапа обработки заданий.

### ИНИЦИАЛИЗАЦИЯ ВСЕХ ДАННЫХ И ПАРАМЕТРОВ

Чтобы предотвратить утерю данных при замене или утилизации жесткого диска, вы можете перезаписать все документы и данные на жестком диске, а затем выполнить сброс настроек до значений по умолчанию.

### РЕЗЕРВНЫЙ ЖЕСТКИЙ ДИСК\*

Компании получили возможность выполнять резервное копирование данных с жесткого диска устройства на дополнительно приобретаемый жесткий диск. При резервном копировании данные на обоих жестких дисках проходят полное шифрование.

### КОМПЛЕКТ СЪЕМНОГО ЖЕСТКОГО ДИСКА\*

Эта опция позволяет извлекать жесткий диск из устройства для его безопасного хранения, пока устройство не используется.

\* Приобретается дополнительно. Для получения подробной информации о доступных функциях и опциях на разных моделях устройств линейки обратитесь к представителю Canon.



# ЗАЩИТИТЕ СВОЮ СЕТЬ



## МОЖЕТ ЛИ ПРИНТЕР СТАТЬ ИСТОЧНИКОМ УГРОЗЫ ДЛЯ ВАШЕЙ СЕТИ?

- Есть ли возможность провести атаку на ваши сетевые порты?
- Могут ли гости выполнять печать и сканирование, не подвергая вашу сеть рискам?
- Поддерживаются ли вашей системой политики безопасного использования личных устройств пользователей?
- Шифруются ли данные печати при передаче с ПК на устройство вывода?
- Безопасен ли процесс передачи данных печати и сканирования?

# Canon предлагает ряд решений для обеспечения безопасности, которые защитят вашу сеть и данные от внутренних и внешних атак.

## **ФИЛЬТР IP- И MAC-АДРЕСОВ**

Защитите свою сеть от несанкционированного доступа сторонних лиц, разрешив связь только с устройствами, имеющими определенные IP- или MAC-адреса; эту функцию можно настроить как для передачи данных внутри сети, так и их вывода за ее пределы.

## **КОНФИГУРАЦИЯ ПРОКСИ-СЕРВЕРА**

Настройте прокси-сервер, чтобы управлять подключениями вместо вашего устройства, и используйте его при подключении к устройствам вне сети.

## **АУТЕНТИФИКАЦИЯ ПО IEEE 802.1X**

Несанкционированный доступ к сети блокируется LAN-коммутатором, который предоставляет доступ только клиентским устройствам, авторизованным сервером аутентификации.

## **ПОДКЛЮЧЕНИЕ ЧЕРЕЗ IPSEC**

Подключение через IPSec предотвращает перехват или расшифровку IP-пакетов, передаваемых по IP-сети, сторонними лицами.

Используйте шифрование связи TLS во избежание прослушивания сети и хищения данных, передаваемых между принтером и другими устройствами, например компьютерами.

## **УПРАВЛЕНИЕ ПОРТАМИ**

Настраивайте параметры портов в рамках конфигурации политики безопасности.

## **АВТОМАТИЧЕСКАЯ РЕГИСТРАЦИЯ СЕРТИФИКАТОВ**

С этой функцией вы сможете забыть о таком процессе, как поддержка сертификатов безопасности. С помощью проверенной технологии системный администратор может автоматически обновлять и выпускать сертификаты в целях соблюдения политик безопасности.

## **МОНИТОРИНГ ЖУРНАЛОВ**

Различные журналы позволяют отслеживать использование устройства, включая заблокированные запросы на подключение.

## **WI-FI DIRECT**

Обеспечьте возможность печати с мобильных устройств посредством однорангового соединения без необходимости подключать его к корпоративной сети.

## **ШИФРОВАНИЕ ДАННЫХ ПРИ ВЗАИМОДЕЙСТВИИ С УСТРОЙСТВОМ**

Эта опция шифрует задания печати при их отправке с пользовательского ПК на многофункциональный принтер. Вы также можете шифровать отсканированные данные в формате PDF, активировав универсальный набор функций безопасности.

## **ГОСТЕВАЯ ПЕЧАТЬ С МОБИЛЬНЫХ УСТРОЙСТВ**

Наше программное обеспечение для управления безопасной сетевой печатью и сканированием устраняет частотные проблемы, связанные с безопасностью печати с мобильных устройств и гостевой печати, предоставляя внешние способы отправки заданий на печать, такие как электронная почта, интернет и мобильное приложение. Это обеспечивает работу МФУ с безопасным источником, минимизируя вероятность взлома.



# ЗАЩИТИТЕ СВОИ ДОКУМЕНТЫ

Все компании имеют дело с конфиденциальными документами, такими как контракты, соглашения, бухгалтерские документы, данные о клиентах, планы отдела разработки и многое другое. В случае если такие документы попадут в чужие руки, последствия могут варьироваться от подрыва репутации до крупных штрафов или даже судебных исков.

Canon предлагает ряд решений для обеспечения безопасности, которые помогут вам защитить конфиденциальные документы на протяжении всего их жизненного цикла.



## КОНФИДЕНЦИАЛЬНОСТЬ ПЕЧАТНЫХ ДОКУМЕНТОВ

### Безопасная печать

Пользователь может задать PIN-код печати, чтобы печать документа начиналась только после ввода правильного PIN-кода на устройстве. Это позволяет защитить конфиденциальные документы.

### Приостановка всех заданий на печать

На устройстве imageRUNNER ADVANCE администратор может приостановить все отправленные задания на печать — таким образом для печати пользователям необходимо будет выполнить вход в систему, за счет чего обеспечивается защита конфиденциальности всех печатных материалов.



## ПРЕДОТВРАТИТЕ СОЗДАНИЕ ДУБЛИКАТОВ

### Печать с видимыми водяными знаками

Драйверы позволяют печатать на странице видимые отметки, которые располагаются поверх содержимого документа. Это можно использовать для информирования сотрудников о конфиденциальности документа и предотвратить его копирование.

### Печать/копирование с невидимыми водяными знаками

Если эта функция включена, документы будут печататься или копироваться со встроенным скрытым текстом на фоне, который будет проявляться при создании дубликата и играть роль сдерживающей меры.

### Предотвращение утери данных на корпоративном уровне

Выведите функции для предотвращения утери данных на новый уровень — используйте uniFLOW в сочетании с iW SAM Express. Это

### Почтовые ящики

Задания на печать или отсканированные документы можно хранить в почтовых ящиках для доступа в любое удобное время. Почтовые ящики можно защитить PIN-кодом, чтобы только назначенные пользователи могли осуществлять доступ к их содержимому. В этом защищенном пространстве на устройстве можно хранить часто печатаемые документы (например, бланки и формы), которые требуют осторожного обращения.

### Безопасная печать uniFLOW\*

Безопасная печать uniFLOW MyPrintAnywhere — это отправка заданий на печать через универсальный драйвер и их печать на любом принтере сети.

серверное решение позволяет выполнять оцифровку и архивирование документов, отправленных на принтер или полученных с устройства, а также анализировать текстовые данные и атрибуты при реагировании на угрозы безопасности.

### Блокировка сканирования документов\*

Эта опция встраивает в печатные документы и копии скрытый код, который предотвращает их дальнейшее копирование на устройстве, на котором активирована эта функция. Администратор может использовать этот параметр для всех заданий или только заданий, выбранных пользователем. Для встраивания доступны TL- и QR-коды.

### Отслеживание источника документа\*

Посредством встроенного кода вы можете отслеживать источник документа.



## НАСКОЛЬКО ХОРОШО ЗАЩИЩЕНЫ ВАШИ ДОКУМЕНТЫ?

**1**

Имеют ли несанкционированные пользователи доступ к конфиденциальным документам на принтере?

**2**

Можете ли вы обеспечить конфиденциальность документов, которые принадлежат разным пользователям, но обрабатываются на едином устройстве?

**3**

Можете ли вы отслеживать источник печатных документов?

**4**

Может ли другой человек забрать ваши конфиденциальные документы после печати?

**5**

Можете ли вы предотвратить частые ошибки, возникающие при отправке документов с устройства?



### ПОЛНЫЙ КОНТРОЛЬ НАД ОТПРАВКОЙ ДОКУМЕНТОВ И ФАКСОВ

#### Ограничение списка адресатов

Чтобы сократить риски утечки информации, администраторы могут ограничить доступ к различным адресатам, например отсутствующим в адресной книге на сервере LDAP, не зарегистрированным в системе или на определенном домене.

#### Отключение автозаполнения адресов

Предотвратите отправку документов неверным адресатам, отключив автозаполнение адресов электронной почты.

#### Защита адресной книги

Установите PIN-код для защиты адресной книги устройства от несанкционированного доступа пользователей.

#### Подтверждение номера факса

Предотвратите отправку документов неправильным адресатам, запросив повторный ввод номера факса пользователями.

#### Конфиденциальность получаемых факсов

Настройте устройство на хранение документов в памяти без их печати. Вы также можете сохранить конфиденциальность полученных посредством факса документов, применив параметр для их сохранения в конфиденциальную папку или защитив их PIN-кодом.



### ПРОВЕРКА ИСТОЧНИКА И ПОДЛИННОСТИ ДОКУМЕНТА ПОСРЕДСТВОМ ЦИФРОВЫХ ПОДПИСЕЙ

#### Подпись устройства

Подпись устройства можно добавить на отсканированные документы в форматах PDF или XPS с помощью ключа и механизма сертификации — таким образом получатель сможет проверить источник и подлинность документа.

#### Подпись пользователя\*

Эта опция позволяет пользователям отправлять файлы PDF или XPS с уникальной цифровой подписью пользователя, полученной от сертифицирующей компании. Таким образом получатель сможет проверить, кто поставил подпись под документом.



### ПРИМЕНЯЙТЕ ПОЛИТИКИ С ИНТЕГРАЦИЕЙ ADOBE LIFECYCLE MANAGEMENT ES

Пользователи могут защищать файлы PDF и применять к ним единообразные и динамические политики для контроля доступа и прав пользования, а также защиты конфиденциальной и ценной информации от неумышленного или злоумышленного

разглашения. Политики безопасности поддерживаются на уровне сервера, поэтому права можно изменить даже после распределения файла. Устройства серии imageRUNNER ADVANCE можно настроить для интеграции с Adobe® ES.

\* Приобретается дополнительно. Для получения подробной информации о доступных функциях и опциях на разных моделях устройств линейки обратитесь к представителю Canon.



# БЕЗОПАСНОСТЬ КОРПОРАТИВНОЙ ИНФОРМАЦИИ

Canon может внести свой вклад в повышение уровня защиты информации в вашей организации.

## **ПОЛНЫЙ КОНТРОЛЬ НАД КОМПЛЕКСНЫМИ ПОТРЕБНОСТЯМИ В ОЦИФРОВКЕ И РАБОТЕ С ДОКУМЕНТАМИ**

С нашим модульным программным обеспечением для управления документами компании могут наслаждаться безопасным совместным использованием сетевых устройств и безопасной печатью заданий на любом из принтеров, подключенных к серверу управления документами. Пользователи мобильных устройств могут воспользоваться сервисом с централизованным управлением, который обеспечивает безопасный доступ пользователей системы и гостей к печати с мобильных устройств.

Модуль сканирования на МФУ обеспечивает оцифровку корпоративных документов, а также их сжатие, конвертирование и распределение по различным местам назначения, включая облачные системы. Вы также можете безопасно перенаправлять задания печати на наиболее подходящий принтер, оптимизируя стоимость печати каждого документа.

Наше решение усиливает защиту документов в вашей компании с полным бухгалтерским учетом, обеспечивая прозрачность операций на уровне пользователей, устройств и отделов.

## **ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ ПАРКОМ УСТРОЙСТВ**

Наше ПО для управления устройствами iW MS дает доступ к параметрам устройства, политикам безопасности, паролям и сертификатам, а также установке обновлений встроенного ПО на устройства Canon в сети, что сократит нагрузку на ИТ-отдел и поможет обеспечить безопасность и актуальность вашей инфраструктуры печати.

## **КОМПЛЕКСНЫЙ АУДИТ ДОКУМЕНТАЦИИ**

Нашу архитектуру сервисов для офисной документации можно дополнить уникальными опциями для полной оцифровки (т.е. сканирования и записи метаданных) всех документов, обработанных устройствами imageRUNNER ADVANCE.

## **УПРАВЛЯЕМЫЕ ПРОЦЕССЫ ПЕЧАТИ**

Canon MPS сочетает в себе инновационные технологии и программные решения с подходящими сервисами, которые помогают должным образом настроить процессы печати и работы с документами без необходимости в дополнительной нагрузке для ИТ-отдела. Благодаря упреждающему управлению и непрерывной оптимизации инфраструктуры печати и процессов документооборота мы можем помочь вам достичь необходимых показателей безопасности, одновременно оптимизируя расходы и повышая производительность вашего бизнеса.

## **ВОЗМОЖНОСТИ ПЕРСОНАЛИЗАЦИИ**

Наша команда штатных разработчиков может предложить и разработать для вас персонализированное решение, которое удовлетворит ваши уникальные потребности.

## НАСКОЛЬКО КОМПЛЕКСНЫМ ЯВЛЯЕТСЯ ВАШ ПОДХОД К ОБЕСПЕЧЕНИЮ КОРПОРАТИВНОЙ БЕЗОПАСНОСТИ?

- Распространяется ли ваша политика безопасности на парк многофункциональных устройств?
- Как вы обеспечиваете актуальность инфраструктуры печати, а также своевременную и эффективную установку исправлений и обновлений?
- Могут ли гости выполнять печать и сканирование, не подвергая вашу сеть риску?
- Поддерживается ли вашим парком печатных устройств безопасное использование личных устройств пользователей?
- Достаточно ли у вашего ИТ-отдела времени для рассмотрения проблем безопасности?
- Нашли ли вы баланс между обеспечением безопасности и удобством использования устройств?



# ПОЧЕМУ CANON?



## ПРОФЕССИОНАЛИЗМ

Интеграция программных и аппаратных решений снижает вероятность сбоев в работе системы.



## ПАРТНЕРСКАЯ РАБОТА

Мы помогаем клиентам вести бизнес увереннее, предоставляя им решения для проблем, связанных с безопасностью данных.



## СЕРВИС

Общая команда по обеспечению информационной безопасности для наших клиентов и внутренней системы ИТ-безопасности в Canon. Мы рассматриваем все возможные угрозы, как внутри, так и вне корпоративной сети.



## ИННОВАЦИИ

Мы внедряем в свои продукты и услуги интеллектуальные способы минимизировать возможные риски для информационной безопасности.



Заслуги Canon в сфере обеспечения кибербезопасности были отмечены на 2017 SCA Awards Europe.

Canon U.S.A. стала обладателем награды **BLI PaceSetter Awards 2017** (категория «Печать с мобильных устройств и безопасность процессов оцифровки документов»).

ООО «Канон Ру»  
Россия, 109028, Москва,  
Серебряническая наб., 29,  
Бизнес-центр «Серебряный город»  
Тел.: +7 (495) 258-56-00  
Факс: +7 (495) 258-56-01  
canon.ru

Центр поддержки клиентов:  
Тел.: +7 800 700 28 19

Санкт-Петербургский филиал  
ООО «Канон Ру»  
Россия, 191036, Санкт-Петербург,  
ул. Жуковского, 63,  
Бизнес-центр «Сенатор»  
Тел.: +7 (812) 449-55-00  
Факс: +7 (812) 449-55-11

Новосибирский филиал  
ООО «Канон Ру»  
Россия, 630132, Новосибирск,  
ул. Красноярская, 35,  
Бизнес-центр «Гринвич»  
Тел.: +7 (495) 258-56-00  
Факс: +7 (495) 258-56-01

Представительство  
ООО «Канон Ру»  
в Республике Казахстан  
Алматы,  
район Бостандыкский,  
пр. Аль-Фараби,  
д/7, кв 26  
Canon.kz