КРАТКОЕ ОПИСАНИЕ МЕР БЕЗОПАСНОСТИ HP

Для защиты данных клиентов компания HP соблюдает комплекс мер по контролю информационной безопасности, включая политику и процедуры по обеспечению конфиденциальности, сохранности и доступности личной информации и информации клиентов (включая персональные данные, как определено в Приложениях HP для клиентов и в Условиях обработки данных). Ниже приводится обзор технических и организационных мер безопасности HP в масштабах компании.

1. Политика безопасности

HP следует глобальным политикам, стандартам и процедурам, разработанным для защиты данных HP и клиентов компании. Политика безопасности HP является конфиденциальной для целей защиты сохранности соответствующих данных и систем. Тем не менее, ниже мы приводим краткое описание основных аспектов нашей политики обеспечения безопасности данных.

2. Организация безопасности информации

HP разработала систему защиты информации, которая определяет стратегию обеспечения безопасности данных и контроль за ее выполнением. Для обеспечения соответствия политикам и средствам контроля HP, а также для соблюдения требований со стороны заказчиков, мы разработали Систему управления информационной безопасностью. Эта система соответствует требованиям обеспечения цифровой безопасности NIST и пересматривается на ежегодной основе.

3. Управление активами

В HP реализован процесс, в рамках которого компания идентифицирует все активы, находящиеся под ее управлением, и классифицирует наиболее критические из них. HP также следует комплексу документированных процедур для каждого типа классифицированной информации, включая активы, которые содержат личные данные. Процедуры такой обработки касаются хранения, передачи, связи, доступа, протоколирования, хранения, уничтожения, утилизации, управления данными и уведомлений о нарушениях.

4. Контроль доступа

Для обеспечения контроля доступа используется принцип «наименьших привилегий». Доступ пользователей осуществляется с помощью уникального идентификатора и пароля. Политика HP в отношении паролей определяет их уровень сложности, надежности, валидности и истории использования. Права доступа периодически пересматриваются и аннулируются в случае увольнения сотрудников из компании.

Процедуры создания и удаления учетных записей пользователей применяются для предоставления и отзыва доступа к информации клиентов, которая используется по ходу реализации проектов.

5. Обучение персонала

Сотрудники HP должны пройти специальный тренинг, который знакомит их с программой, политикой и ресурсами в отношении этичного поведения, обеспечения качества и соблюдения норм (Integrity at HP). Программа Integrity at HP включает в себя модули по обеспечению безопасности и конфиденциальности данных. Кроме того, сотрудники также должны проходить ежегодный курс переподготовки. Сотрудники HP также должны проходить ежегодный курс повышения осведомленности, посвященный основным политикам безопасности и их обязанностям, связанным с управлением происшествиями, конфиденциальностью данных и информационной безопасностью.

6. Третьи стороны и подрядчики

В HP разработаны процедуры, позволяющие выбирать подрядчиков, полностью соблюдающих требования к безопасности, предусмотренные контрактом.

В отношении существующих поставщиков (которые обрабатывают / хранят / передают данные HP/данные, принадлежащие клиенту или имеют доступ к сети HP) HP проводит оценку соответствующих рисков, чтобы проверить эффективность нашей программы обеспечения информационной безопасности. Такая программа должна включать в себя физические, технические и административные меры защиты безопасности данных. Оценка должна быть проведена до того, как поставщик получает доступ к информации HP.

7. Безопасность систем

Согласно нашей политике,разработка систем и вспомогательного программного обеспечения осуществляется в соответствии с методологией безопасной разработки в целях обеспечения безопасности на протяжении всего жизненного цикла такой системы / программного обеспечения. Жизненный цикл разработки программного обеспечения определяет требования к его запуску, разработке / приобретению, внедрению, эксплуатации и утилизации. Все компоненты систем, включая модули, библиотеки, сервисы и отдельные элементы, оцениваются на предмет их влияния на безопасность системы.

HP разработала средства защиты транзакций в рамках приложений. Они включают в себя проверку и подтверждение учетных данных пользователей, обязательное использование цифровых подписей и шифрования, внедрение протоколов безопасной связи, хранение данных о транзакциях в режиме онлайн на серверах в безопасной сети.

Мы также регулярно проводим проверку возможных внутренних уязвимостей.

8. Физическая и экологическая безопасность

Объекты HP защищены с помощью различных средств физического и электронного контроля доступа и средств наблюдения. В зависимости от объекта они могут включать в себя охранный

персонал, электронный контроль доступа и систему видеонаблюдения (CCTV).

Все сотрудники HP имеют специальную регистрацию и обязаны носить соответствующие идентификационные значки.

Все объекты располагают необходимой инфраструктурой, обеспечивающей температурный контроль и резервное электропитание с использованием ИБП и/или дизельных генераторов для поддержки критически важных сервисов.

9. Управление производством

HP определила минимальный набор требований к технологической инфраструктуре, включая наличие рабочих станций, серверов и сетевого оборудования. Рабочие станции / серверы располагают операционными системами, которые были предварительно сконфигурированы для обеспечения безопасности данных. Требования к обеспечению безопасности зависят от типа операционной системы и используемых средств контроля.

HP внедрила систему обнаружения и предотвращения сетевых вторжений (NIDS / NIPS), которая функционирует 24 часа в сутки 7 дней в неделю.

Политики и стандарты безопасности HP предписывают безопасную утилизацию носителей информации.

10. Криптография

HP разработала комплекс криптографических процессов, чтобы обеспечить конфиденциальность, надежность и доступность информационных активов. Наши протоколы требуют шифрования информации, содержащей персональные данные.

11. Управление происшествиями в области информационной безопасности

HP следует особому процессу управления происшествиями, учитывающему цели, сферу применения, роли, обязанности, организационную структуру, процедуры внедрения и проверку соответствия. HP анализирует и обновляет такие процедуры на ежегодной основе.

Группа срочного реагирования, в которую входят сотрудники соответствующего отдела HP и которые прошли обучение по реагированию на кризисные ситуации, регулярно анализирует текущие процессы и происшествия.

12. Обеспечение непрерывности деятельности

HP следует глобальной программе обеспечения непрерывности деятельности. В рамках этой программы применяется целостный подход к обеспечению непрерывности нашей деятельности при помощи набора стандартизированных и документированных инструментов для планирования.

HP периодически анализирует планы обеспечения непрерывности деятельности, чтобы убедиться в их эффективности. В настоящее время HP проверяет и обновляет такие планы не реже одного раза в год и обучает сотрудников, имеющих отношение к плану обеспечения непрерывности

деятельности.

Редакция от	Краткое описание изменений	Контактное лицо
Май 2018 г.	Первая публикация	Раелла Дайк (Raella Dyke)
Февраль 2022 г.	Обновления	Греттель Акунья (Grettel Acuña)