Минимальный перечень контролей по Информационной Безопасности для Третьих сторон[1]

Версия 4.0

Апрель 2024 г.

Информационная безопасность и соответствие требованиям

[1] С Минимальным перечнем контролей по Информационной Безопасности для Третьих сторон можно ознакомиться на сайте https://www.novartis.com/esg/reporting/codes-policies-and-guidelines

Минимальный перечень контролей по Информационной Безопасности для Третьих сторон[2]

1. Управление и Соблюдение требований

- Третья сторона обязана внедрить и поддерживать программу информационной безопасности, соответствующую практике индустрии безопасности и применимым законам и нормам, для защиты систем и сетевой инфраструктуры, а также конфиденциальности, целостности, доступности и устойчивости данных, как минимум, как указано в настоящем документе и для обеспечения уровня безопасности, соответствующего риску.
- Третья сторона должна убедиться, что надлежащим образом назначено лицо, действующее от имени Третьей стороны и ответственное за обеспечение соблюдения технических и организационных требований к средствам контроля информационной безопасности.
- Программа информационной безопасности Третьей стороны должна содержать систему управления информационными рисками, включая необходимые политики по управлению рисками, которые обеспечивают и поддерживают соответсвующий процесс.

2. Обеспечение непрерывности бизнес-процессов

- Третья сторона должна иметь соответствующие планы обеспечения непрерывности бизнес-процессов и аварийного восстановления, чтобы обеспечить своевременное восстановление своих ИТ-систем, участвующих в любой операции с данными в любой форме, поддерживающих услуги, предоставляемые Новартис, в случае наступления стихийного бедствия или другого события, которое может привести к существенному сбою.
- Третья сторона обязана обеспечить периодическое тестирование и обновление своих планов аварийного восстановления для обеспечения их актуальности и эффективности.
- Третья сторона гарантирует, что технологии и процессы, используемые для резервного копирования и восстановления данных, регулярно проверяются и имеют достаточную защиту от любых разрушительных кибератак.

3. Обращение с носителями информации

- Третьей стороной должны быть установлены процедуры, описывающие порядок обращения с информацией и способы ее хранения, с целью обеспечения защиты информации от несанкционированного раскрытия или неправильного использования.
- Третья сторона обязана обеспечить конфиденциальность и безопасность в процессе утилизации носителей информации, которые более не требуются, в соответствии с применимыми процедурами и с заполнением надлежащей документации.
- Третья сторона обязуется после прекращения договорных отношений с Новартис или по требованию Новартис вернуть Новартис все носители и другие активы, предоставленные Третьей стороне Новартис.
- Третья сторона должна обеспечить защиту системной документации от несанкционированного доступа.

[2] Выражения с заглавной буквы, используемые в настоящем документе, имеют то же значение, что и в последней версии Кодекса взаимодействия с третьими лицами Новартис (доступен на сайте https://www.novartis.com/esg/reporting/codes-policies-and-guidelines), если только они не определены в прилагаемом Глоссарии или контекст не требует иного. В настоящем документе ссылка на "третью сторону" или "третьи стороны" ограничивается только теми третьими сторонами, которые подпадают под определение "Поставщики" в Кодексе третьих сторон Новартис.

4. Обмен данными

- Третья сторона обязана поддерживать конфиденциальность, целостность, доступность и устойчивость данных и систем, на которых размещены или через которые доступны такие данные, в рамках своей организации и на внешнем объекте; что включает в себя наличие соглашения об обмене, защиту физических носителей при передаче, безопасный способ отправки электронных сообщений и защиту информации, которая обрабатывается корпоративными информационными системами.

5. Контроль доступа

- Третья сторона должна иметь политику контроля доступа, которая обеспечивает доступ к данным Новартис только авторизованным пользователям, имеющим соответствующее разрешение и служебную необходимость.
- Третья сторона обязана проверять права доступа пользователей, чтобы гарантировать, что распределение и использование привилегий контролируется и ограничивается, где это необходимо и применимо к данным Новартис или любым системам, хранящим такие данные.

6. Криптографическая защита информации

- Учитывая соответствующие риски информационной безопасности, уровень техники, практику индустрии безопасности и применимые законы и нормативные акты, Третья сторона разрабатывает, внедряет и поддерживает криптографическую защиту информации, включая шифрование данных Новартис в соответствующих случаях.

7. Контролируемая обработка и использование искусственного интеллекта

- Третья сторона обеспечивает раздельную обработку данных, собранных для различных целей, например, возможность работы с несколькими клиентами, "песочница", разработка/тестирование по сравнению с производственной средой, используемой конечными пользователями.
- Третья сторона обеспечивает обработку только тех данных, которые необходимы для каждой конкретной цели обработки, применяя при необходимости методы санации/минимизации и удаления данных.
- Третья сторона должна использовать системы искусственного интеллекта для обработки данных Новартис только после предварительного согласования с Новартис. В этом случае Третья сторона должна обеспечивать соответствующие гарантии в соответствии с лучшими отраслевыми практиками (например, запрет на использование данных Новартис для обучения, анонимизация данных Новартис, безопасная обработка данных Новартис и т. д.), связанные с использованием таких систем искусственного интеллекта.

8. Коммуникации и сетевая безопасность

- Третья сторона обеспечивает адекватное управление, контроль и защиту сетей, находящихся под контролем Третьей стороны, от угроз и уязвимостей, а также поддерживает конфиденциальность, целостность и доступность данных и предотвращает несанкционированный доступ к таким системам и приложениям, используемым для обработки данных в процессе хранения или передачи.
- Третья сторона, подключающаяся к среде Новартис, должна убедиться, что она способна соответствовать соответствующим техническим стандартам Новартис, применимым к такой среде.

9. Обучение и осведомленность в области безопасности

- Третья сторона должна обеспечить, чтобы все ее работники, подрядчики и агенты были осведомлены об угрозах и проблемах информационной безопасности, своих обязанностях и были готовы поддерживать политику безопасности организации в ходе своей работы.
- Третья сторона обеспечивает, чтобы все работники, подрядчики и агенты проходили соответствующее обучение по вопросам информационной безопасности и защиты данных.
- Третья сторона гарантирует, что ее работники будут использовать корпоративные адреса электронной почты (вместо того, чтобы использовать личную электронную почту или учетные записи платформ для обмена сообщениями) для любой переписки, содержащей или имеющей отношение к данным Новартис.

10. Физическая безопасность и Безопасность среды

- Третья сторона обязана обеспечить наличие соответствующих периметров информационной безопасности и контроль за доступом для предотвращения несанкционированного физического доступа, повреждения и вмешательства в помещения и данные Третьей стороны, включая все устройства конечных пользователей.
- Третья сторона обязана обеспечить надлежащую инвентаризацию и обслуживание оборудования для обеспечения его постоянной информационной безопасности.

11. Защита документации организации

- Программа информационной безопасности Третьей стороны должна включать в себя политики, касающиеся хранения и уничтожения данных в соответствии с принятой отраслевой практикой.
- Третья сторона обеспечивает внедрение соответствующих средств контроля для предотвращения потери, уничтожения или фальсификации записей в течение периода их хранения, включая определение того, были ли данные введены, доступны, изменены или удалены из систем обработки данных и кем они были введены.
- Третья сторона соглашается, что по запросу компании Новартис или в соответствии с иными требованиями закона она должна избавиться (например, стереть, уничтожить или сделать невоспринимаемыми) от всех данных Новартис, которыми владеет или управляет Третья сторона, ее филиалы или субподрядчики (признавая, что копии данных Новартис могут находиться на стандартных носителях резервного копирования Третьей стороны, которые подлежат стандартной схеме ротации резервных копий и защищены в соответствии с признанной и действующей на тот момент практикой защиты данных и практикой индустрии безопасности). Третья сторона должна предоставлять Новартис отчет с соответствующим уровнем детализации о данных Новартис, хранящихся на резервных носителях, по запросу Новартис без каких-либо дополнительных затрат для Новартис. Новартис имеет право на получение копии данных Новартис в форме и в сроки, указанные Новартис, до их уничтожения.
- По запросу Новартис Третья сторона должна письменно подтвердить, что эти действия были выполнены.
- Исключениями из этого требования об утилизации считаются следующие случаи:
  - Третья сторона должна хранить данные Новартис в архиве для юридических или нормативных целей; такие данные Новартис должны быть удалены, как только истекут установленные законом сроки хранения
  - Данные Новартис, которые Новартис попросила третью сторону сохранить в архиве для целей, связанных с судебными разбирательствами и другими юридическими причинами.
  - Если Новартис в письменной форме согласовала с Третьей стороной особые требования к возврату/уничтожению/хранению определенных данных Новартис, в этом случае применяются такие особые требования.

12. Управление техническими уязвимостями

- Третья сторона должна иметь программу управления уязвимостями, которая отслеживает и поддерживает состояние информационной безопасности ИТ-среды Третьей стороны.
- Третья сторона обязана внедрить и поддерживать политики, демонстрирующие надлежащее применение и управление обновлениями и исправлениями в ИТ-системах Третьей стороны.
- Третья сторона создает и поддерживает инвентаризацию аппаратного и программного обеспечения и проводит регулярное сканирование уязвимостей.

13. Управление инцидентами информационной безопасности

- Третья сторона гарантирует, что будут установлены обязанности и процедуры управления для обеспечения быстрого, эффективного и упорядоченного реагирования на инциденты безопасности, а также для сообщения и управления инцидентами и недостатками информационной безопасности, включая соответствующую отчетность.
- Третья сторона будет незамедлительно информировать Новартис в случае инцидента безопасности, связанного с данными Новартис.

14. Мониторинг

- Третья сторона должна осуществлять мониторинг своей среды для обнаружения и реагирования на инциденты информационной безопасности или другие несанкционированные действия.
- Третья сторона обязана использовать средства аудиторского контроля в среде под управлением Третьей стороны, которые обеспечивают независимый аудит / оценку соответствующих данных аудиторского контроля в операционных системах с сокращением до минимума риска нарушения процессов бизнеса..

15. Управление конфигурацией и изменениями

- Третьей стороной должен быть установлен процесс управления изменениями, который учитывает этап оценки влияния изменений до их внедрения, включает критерии для определения эффективности или неэффективности изменения и обеспечивает согласование процедуры отмены неэффективных изменений до осуществления изменений

16. Защита от воздействия вредоносных кодов

- Третья сторона обязана разработать политику управления рисками, связанными с использованием вредоносного кода, и внедрить средства защиты от вредоносных программ.