Содержание

1. Введение

1.1 Клиенты BT ожидают, что компания BT и ее цепочка сторонних поставщиков предоставляют свои услуги с использованием систем управления информационной безопасностью, соответствующих стандартам отрасли (ISMS). ISMS третьей стороны должна охватывать инфраструктуру, сети, оборудование и ИТ-системы с целью защиты предоставляемых услуг и информации BT и клиентов BT в рамках услуг. В настоящем документе изложены требования к безопасности BT, и он применяется ко всем третьим сторонам, работающим на или от имени BT Group, включая Openreach, EE и PlusNet (далее — «BT»). Третьей стороне будет сообщено, какие наборы средств контроля безопасности применимы к услугам, предоставляемым ею BT.

1.2 Настоящие Требования к безопасности дополняют и не ограничивают любые другие обязательства третьей стороны по контракту. Они разработаны для обеспечения контроля и надзора со стороны BT за своей сетью и данными пользователей.

2. Требования ограниченного доступа

2.1 Без ущерба для каких-либо обязательств конфиденциальности, которые может иметь персонал третьей стороны, имеющий доступ к информации BT, третья сторона должна:

2.2 гарантировать, что информация BT не разглашается и не доступна персоналу третьей стороны, за исключением случаев, когда это необходимо для предоставления услуг; и

2.3 внедрить все системы и процессы, как технические, так и организационные, необходимые для защиты информации BT (i) от случайного или незаконного уничтожения и (ii) потери, изменения, несанкционированного раскрытия или доступа к информации BT в соответствии с установившейся в отрасли практикой обеспечения безопасности.

3. Общая информационная безопасность

3.1 По обоснованному запросу третья сторона должна предоставить BT копии сертификатов безопасности и декларации соответствия, относящиеся к услугам, для подтверждения соответствия настоящим Требованиям к безопасности.

3.2 В случае существенного изменения технологий, отраслевых стандартов безопасности или каких-либо значительных изменений в услугах или способе их предоставления BT может внести поправки в контракт в течение срока его действия, если есть необходимость в изменении действующих мер обеспечения безопасности. Третья сторона обязуется выполнить положения согласованных поправок к контракту в разумный срок с учетом характера изменений и рисков для BT.

3.3 При любых существенных изменениях в услугах или способах их предоставления третья сторона должна пересмотреть настоящую политику Требований к безопасности, чтобы убедиться, что она по-прежнему соответствует всем действующим правилам безопасности.

3.4 Если третья сторона передает обязательства по контракту субподрядчикам, она должна гарантировать, что все контракты с соответствующими субподрядчиками и их субподрядчиками включают письменные условия, требующие от них соблюдения применимых частей настоящих Требований к безопасности или таких же требований к безопасности третьей стороны.

3.5 Если для хранения и обработки информации BT привлекается четвертая сторона, третья сторона должна получить от заинтересованного лица BT разрешение и разъяснения о том, какую информацию можно предоставлять. Третья сторона должна установить договорные отношения с четвертой стороной и убедиться, что та применяет стандартные нормы обеспечения безопасности отрасли.

3.6 Срок хранения информации BT должен быть достаточным для выполнения контракта, по завершении действия которого информация должна храниться не более двух лет, если только BT и третьей стороной не был согласован другой срок или продление срока не является требованием действующего законодательства.

3.7 Если услуги предоставляются по контракту с правительством Великобритании, третья сторона должна выполнять требования последней версии правил Государственного центра кибербезопасности: https://www.cyberessentials.ncsc.gov.uk/.

3.8 Если информация BT будет обрабатываться или храниться за границей, третья сторона должна сообщить BT о таком географическом местоположении. BT оставляет за собой право отклонить места, которые считаются высокорискованными.

Работа с информацией BT

3.9 Если заинтересованное лицо BT не сообщило иное, вся информация BT классифицируется как «конфиденциальная». Если речь идет о персональных данных или конфиденциальных персональных данных, третьей стороне следует обратиться к команде по защите данных и конфиденциальности и уточнить, не требуются ли дополнительные меры безопасности.

Следующие правила безопасности представляют собой «требования в отношении устной коммуникации» и распространяются только на устные сообщения.

3.10 Если есть необходимость обсудить, показать информацию BT или обменяться ею с помощью платформы для совместной работы, например Teams:

- убедитесь, что присутствуют только лица, которым необходимо получить эту информацию;
- если задействован внешний подрядчик, он должен либо иметь подписанный с третьей стороной контракт, либо подписать соглашение о неразглашении до начала обсуждения;
- перед началом сеанса связи третья сторона должна проверить, кто в нем участвует.

3.11 Если есть необходимость обсудить информацию BT с кем-либо лично, по мобильному телефону или стандартной телефонной линии:

- разговоры не должны вестись тем, кому не следует получать эту информацию, и не должно быть возможности, чтобы разговор слышал кто-то еще;
- если требуется обсуждение с внешним подрядчиком, они должны либо иметь подписанный с третьей стороной контракт, либо подписать соглашение о неразглашении до начала обсуждения;
- конфиденциальную или особо конфиденциальную информацию нельзя оставлять в сообщении голосовой почты.

Следующие правила безопасности являются «требованиями в отношении письменной коммуникации» и распространяются на материалы, хранящиеся на бумаге. Сюда входят, в частности, рукописные письма, протоколы, заметки и служебные записки. К ним также относятся распечатанные электронные материалы, такие как рабочие документы и отчеты, если они в бумажном формате.

3.12 Если бумажные копии информации BT хранятся в помещениях третьей стороны, когда они не используются, они должны храниться в запираемом помещении, с ограничением доступа только для тех, кому необходимо просмотреть материал. Документы не должны оставаться без присмотра.

3.13 Если есть необходимость в печати, фотокопировании или дублировании информации BT, применяются следующие правила безопасности:

- используйте средства печати или копирования только в собственных помещениях третьей стороны;
- фотокопии или распечатки не должны оставаться без присмотра в месте печати и должны быть забраны в момент создания;
- если принтер или копировальный аппарат имеет память, из которой можно вызвать и повторно распечатать скопированный материал, его следует перезагрузить, чтобы очистить память, как можно скорее.

3.14 Если есть необходимость удалить копии информации BT из помещений третьих лиц:

- если это не согласовано в рамках объема работ, третья сторона должна получить подтвержденное согласие от заинтересованной стороны BT;
- если согласие получено, информация не должна быть идентифицируемой во время транспортировки и должна храниться в анонимной или обычной папке, сумке или футляре;
- материал не должен оставаться без присмотра и должен находиться под непосредственным контролем лица, перевозящего материал, особенно в общественном транспорте.

3.15 Если бумажные копии информации BT больше не нужны, они должны быть утилизированы следующим образом:

- бумажные копии не должны выбрасываться в контейнеры для общих отходов;
- если используется шредер, он должен соответствовать как минимум стандарту P4 DIN66399;

- если соответствующие требованиям шредеры недоступны, информация должна утилизироваться в контейнеры для конфиденциальных отходов.

В отношении «особо конфиденциальной информации» дополнительно действуют следующие правила.

- После уничтожения шредером документы должны выбрасываться только в контейнеры для конфиденциальных отходов.
- Если информация должна быть уничтожена на месте поставщиком, необходимо получить сертификат об уничтожении от поставщика.

К информации BT в электронном формате применяются следующие правила безопасности.

3.16 При хранении информации BT на ПК или ноутбуке третьей стороны применяются следующие правила.

- Разрешается использовать только устройства с шифрованием жесткого диска, например Bitlocker.
- Все документы должны быть отдельно зашифрованы.
- К документу должно быть применено управление правами на информацию (IRM).
- Предоставленная информация должна сохранять метку классификации BT.

3.17 При сохранении документа BT во внутреннем файловом хранилище для общего хранения, совместной работы или обмена файлами применяются следующие правила безопасности.

- В месте, куда сохраняется материал, должны быть установлены разрешения на доступ, позволяющие видеть или использовать документ только тем, кому это необходимо.
- Предоставленная информация должна сохранять метку классификации BT.
- Все документы должны быть отдельно зашифрованы.
- К документу должно быть применено управление правами на информацию (IRM).
- Если в ходе предоставления услуги раскрываются материалы PCI и данные платежных карт, они никогда не должны сохраняться в местах хранения файлов.
- Если для предоставления доступа внешнему подрядчику необходимы гостевые учетные записи, они должны иметь подписанный с третьей стороной контракт или подписать соглашение о неразглашении до предоставления доступа.

3.18 Если есть необходимость сохранить информацию BT на съемном носителе третьей стороны, например на USB-накопителе, применяются следующие правила безопасности.

- Устройство должно быть зашифровано на том же уровне, что и жесткий диск.
- В случае потери или кражи третья сторона должна сообщить о случае нарушения безопасности.

- У третьей стороны должны быть доказательства предварительного разрешения от заинтересованной стороны BT на перенос «особо конфиденциальных» материалов на съемный носитель.
- Получаемые в рамках оказания услуг материалы PCI и персональные данные не должны храниться на съемных носителях.
- Устройства, предназначенные для поддержки и обслуживания, не должны использоваться в других целях.

3.19 Информация BT не должна храниться на личных компьютерах, ноутбуках, съемных носителях или мобильных устройствах.

3.20 Информация BT не должна отправляться или автоматически пересылаться с корпоративного адреса электронной почты третьей стороны на личную электронную почту или внешнюю учетную запись электронной почты, если только они не принадлежат внешним подрядчикам, которые имеют подписанный с третьей стороной контракт или соглашение о неразглашении, и используются для предоставления услуги.

3.21 Чтобы минимизировать поверхность атаки и возможности злоумышленников манипулировать поведением человека при взаимодействии с веб-браузерами и системами электронной почты, внедрите процессы, гарантирующие, что будут разрешены только полностью поддерживаемые веб-браузеры и почтовые клиенты, а также удалите или отключите любые несанкционированные плагины или дополнительные приложения для браузеров или почтовых клиентов.

3.22 Третья сторона должна применять резервное копирование, чтобы иметь возможность восстановить информацию BT в течение 3 рабочих дней в случае ее повреждения, потери или деградации.

3.23 При утилизации данных/информации BT необходимо обеспечить полный учет хранения и утилизации информации с ведением контрольного журнала, подтверждением и отслеживанием соответствующих действий. Обязательна следующая документация:

- сертификат уничтожения и/или утилизации (включающий дату выполнения и использованный метод);
- системные журналы регистрации удаления;
- сертификаты утилизации данных;
- сведения о том, кто выполнил утилизацию (включая любых партнеров, сторонние организации или подрядчиков);
- сгенерированный отчет, подтверждающий успешное или неудавшееся уничтожение/удаление (например, по результатам стирания данных должен быть предоставлен отчет с подробным перечнем секторов, которые не удалось стереть).

3.24 При утилизации оборудования, на котором находились данные/информация BT, необходимо вести контрольный журнал для следующих типов оборудования:

- съемные носители,
- жесткие диски,
- носители с резервными копиями,

- детали компьютеров.

3.25 В контрольном журнале должны вестись подробные записи, включающие как минимум:

- название приложения или службы, для которой использовалась конкретная единица оборудования;
- тип оборудования, например настольный компьютер, ноутбук, сервер, носитель информации, маршрутизатор и т. д.;
- количество жестких дисков в оборудовании (при наличии);
- серийный номер, идентифицирующий оборудование;
- серийные номера, идентифицирующие комплектующие оборудования;
- полное отслеживание всего оборудования и компонентов в течение всего процесса утилизации;
- сертификат уничтожения и/или утилизации (включающий дату выполнения и использованный метод);
- сведения о том, кто выполнил утилизацию (включая любых партнеров, сторонние организации или подрядчиков);
- сгенерированный отчет об уничтожении и проверке для подтверждения успешного или неудачного выполнения любой операции по утилизации, очистке или удалению. Например, для процесса стирания данных должен быть предоставлен отчет с подробным перечнем секторов, которые не удалось стереть. Эти отчеты должны содержать данные об объеме, марке, модели и серийном номере носителя.

Роли и обязанности

3.26 Каждая третья сторона должна знать и понимать эти правила обеспечения безопасности и следить за тем, чтобы все лица, участвующие в предоставлении услуг BT, знали и выполняли соответствующие требования.

Управление

3.27 Третья сторона должна иметь организованную и согласованную систему информационной и кибербезопасности, соответствующую отраслевым стандартам и включающую следующие компоненты:

- соответствующие политики и процедуры информационной и кибербезопасности, утвержденные и доведенные до сведения сотрудников;
- стратегия информационной безопасности;
- соответствующие правовые и нормативные требования информационной и кибербезопасности (включая конфиденциальность), которые понятны и выполнимы;
- процедуры контроля и управления рисками в сфере информационной и кибербезопасности.

3.28 Третья сторона должна определить и ввести соответствующие должности и обязанности по информационной и кибербезопасности, включая следующие:

- штатный главный специалист по информационной безопасности (или аналогичная должность), имеющий достаточные полномочия и несущий ответственность за программу информационной безопасности;
- рабочая группа высокого уровня, комитет или равноценный орган для координации деятельности третьей стороны в сфере информационной безопасности, возглавляемый сотрудником с достаточными полномочиями и собираемый на регулярной основе;
- специалист по информационной безопасности с четкими полномочиями и обязанностями.

3.29 Третья сторона должна обеспечить личную ответственность, закрепив критические участки, информацию и системы за способными сотрудниками.

3.30 Третья сторона должна уведомлять (в письменном виде) BT, как только на это будет законное право и основания, о своем слиянии, приобретении или изменении формы собственности.

Управление инцидентами

3.31 Третья сторона должна иметь организованную и согласованную систему управления, ограничения и смягчения последствий инцидентов, включающую следующие элементы:

- знание персоналом своих обязанностей и порядка действий на случай необходимости принятия мер реагирования;
- отчетность об инцидентах в соответствии с установленными критериями;
- обеспечение понимания последствий инцидента;
- проведение расследования своими силами или с помощью приглашенного специалиста в случае необходимости;
- принятие мер по результатам расследования произошедших инцидентов и их внедрение в установленную практику;
- обеспечение конфиденциальности информации об инцидентах, связанных с BT.

3.32 Третья сторона должна назначить квалифицированных специалистов, к которым можно обратиться в случае угроз безопасности, для урегулирования инцидентов и обеспечения соблюдения соответствующих норм. Третья сторона должна сообщать заинтересованному лицу BT контактные данные ответственных лиц и о любых их изменениях.

3.33 Третья сторона должна в разумные сроки информировать через электронную почту security@bt.com или по телефону +44 0800 321 999 заинтересованное лицо BT о любом ставшем ей известным инциденте, влияющем на обслуживание компании BT или ее информацию, не позднее двадцати четырех (24) часов с момента получения информации об инциденте третьей стороной.

3.34 Третья сторона должна без необоснованных задержек устранять риски, способствовать смягчению серьезности и последствий инцидентов и уменьшению их продолжительности.

3.35 Третья сторона должна предоставлять заинтересованному лицу BT отчеты обо всех инцидентах, влияющих на обслуживание компании BT или ее информацию, в течение 30 дней с момента такого инцидента с указанием как минимум следующих данных:

дата и время, местоположение, тип инцидента, воздействие, статус и результат (включая рекомендации по решению или предпринятые действия).

3.36 Третья сторона должна проводить анализ первопричины всех инцидентов, связанных с безопасностью. Результаты этого анализа должны быть переданы на соответствующий уровень управления в организации третьей стороны.

Управление изменениями

3.37 Третья сторона должна обеспечить согласование, регистрацию и тестирование, включая отказ от неудачных, всех изменений в ИТ-системах перед их внедрением с целью предотвращения сбоев в обслуживании и нарушений безопасности, а также управляемую процедуру экстренных обновлений.

3.38 Третья сторона должна обеспечить внедрение изменений как в рабочей среде, так и в среде аварийного восстановления.

3.39 Третья сторона должна обеспечить выполнение и регистрацию технического обслуживания и ремонта активов организации с использованием утвержденных и управляемых инструментов.

3.40 Третья сторона должна обеспечить согласование, регистрацию и выполнение дистанционного обслуживания активов организации без риска несанкционированного доступа.

Управление киберрисками и киберугрозами

3.41 Третья сторона должна обеспечить наличие постоянной системы оценки рисков и угроз, гарантирующей, что кибербезопасность операций, активов и объектов организации и ее сотрудников понимается и контролируется посредством:

- оценки уязвимости активов;
- выявления как внутренних, так и внешних угроз;
- обеспечения конфиденциальности информации и данных;
- оценки потенциальных последствий для бизнеса;
- оценки угроз, уязвимостей, вероятностей и последствий для определения рисков;
- согласования системы управления киберрисками и киберугрозами на должном уровне в организации.

3.42 Третья сторона должна обеспечивать приоритетность всех рисков и угроз кибербезопасности и принимать соответствующие меры для их снижения в приемлемые сроки.

3.43 Третья сторона должна уведомлять заинтересованное лицо BT о невозможности исключения или уменьшения каких-либо существенных элементов риска, которые могут повлиять на предоставляемые услуги.

Управление идентификационными данными и контроль доступа

3.44 Третья сторона должна иметь организованную и согласованную систему безопасного управления идентификационными и регистрационными данными, которое осуществляется уполномоченным персоналом.

- Предоставление, повторное предоставление, изменение и лишение прав доступа только на основе документированных и санкционированных разрешений.
- Блокировка неактивных учетных записей.
- Отключение учетных записей уволенного/уволившегося персонала.
- Внедрение процессов и инструментов для отслеживания, контроля, предотвращения и исправления использования, назначения и конфигурации прав доступа на компьютерах, в сетях и приложениях.
- Периодическая проверка доступа на предмет соответствия цели.
- Повторная сертификация учетных записей пользователей не реже раза в год, а для привилегированных учетных записей — ежеквартально.
- Хранение постоянных учетных данных и секретных ключей (например, для доступа в случае чрезвычайной ситуации) в защищенном аппаратными средствами хранилище и предоставление доступа ответственным лицам только в чрезвычайной ситуации.
- Гарантия того, что непостоянные учетные данные (например, имя пользователя и пароль для аутентификации) хранятся в централизованной службе с соответствующим контролем доступа на основе ролей, которые должны обновляться в соответствии с любыми соответствующими изменениями ролей и обязанностей в организации.

3.45 Центральное хранилище для постоянных учетных данных должно быть защищено аппаратными средствами. Например, на физическом хосте диск может быть зашифрован с помощью модуля доверенной платформы (TPM). Если для предоставления услуги централизованного хранения используется виртуальная машина (ВМ), эта ВМ и данные, содержащиеся в ней, также должны быть зашифрованы, использовать безопасную загрузку и быть настроены таким образом, чтобы обеспечить загрузку только в соответствующей среде. Третья сторона должна обеспечить управление удаленным доступом таким образом, чтобы только уполномоченные лица могли подключаться к системам третьей стороны, соединения были безопасными и предотвращали утечки данных, а также имелся надлежащий контроль доступа, например многофакторная аутентификация.

Двухфакторная аутентификация должна обеспечиваться с использованием идентификатора пользователя, пароля и одного из следующих средств:

- генератор одноразовых паролей, при этом для просмотра одноразового пароля требуется специальный PIN-код или пароль пользователя;
- смарт-карта с микрочипом стандарта ISO 7816, соответствующим считывающим устройством и программным обеспечением. Использование бесконтактных смарт-карт не допускается;

- аутентификация на основе сертификатов согласно политике информационной безопасности третьей стороны.

Если привилегированный доступ к службе поддержки предоставляется удаленно, это должно быть безопасное соединение с использованием двухфакторной аутентификации.

3.46 Третья сторона должна обеспечить управление разрешениями и авторизацией доступа ко всем системам (включая инструменты, приложения, базы данных, операционные системы, аппаратное обеспечение и т. д.) на основе минимальных привилегий и разделения обязанностей.

3.47 Третья сторона должна гарантировать привязку каждой транзакции к одному уникальному идентифицируемому лицу, а также наличие соответствующих компенсирующих средств контроля (включая аварийные процедуры) при использовании общих регистрационных данных. Общие учетные данные для привилегированного доступа не разрешены.

3.48 Третья сторона должна гарантировать всю аутентификацию соразмерно с рискованностью транзакций, то есть с использованием пароля соответствующей длины и сложности, надлежащей частоты смены паролей, многофакторной аутентификации, безопасного управления регистрационными данными или других средств. Привилегированный доступ должен осуществляться через учетные записи, защищенные многофакторной аутентификацией. Учетные записи привилегированных пользователей, которые используются в чрезвычайных ситуациях, должны иметь надежные учетные данные, уникальные для каждой точки доступа к сетевому оборудованию.

3.49 Должны быть предусмотрены необходимые средства контроля в случае неудачных попыток аутентификации, включая всплывающие уведомления, журнал неудачных попыток входа и блокировку пользователей.

3.50 Должны быть предусмотрены процедуры и средства контроля для управления гостевыми и служебными учетными записями и их авторизации.

Классификация и защита данных

3.51 Третья сторона должна иметь организованную и согласованную систему классификации, маркировки и обработки информации (соответствующую установившейся в отрасли практике / требованиям BT), которая предусматривает следующее:

- указания по обработке информации;
- защиту информации в зависимости от уровня конфиденциальности;
- осведомленность сотрудников о том, что информация BT должна использоваться только для тех целей, для которых она была предоставлена.

Предотвращение утечки данных

3.52 Третья сторона должна иметь организованную и согласованную систему защиты от утечки данных, которая должна распространяться, в частности, на следующее:

- электронная почта, Интернет / веб-шлюз (включая онлайн-хранилище и веб-почту), USB, оптические и другие формы портов / портативных накопителей

и т. д., мобильные компьютерные среды и личные устройства, услуги удаленного доступа, механизмы обмена файлами и социальные сети;

- запрет использования несанкционированных устройств для подключения к сети (корпоративной сети поставщика или системам / сетям BT) или доступа к закрытой информации.

Управление уязвимостями

3.53 Третья сторона должна иметь организованную и согласованную систему управления уязвимостями, включающую следующие компоненты:

- политики и процедуры для процессов;
- четко определенные роли и обязанности;
- необходимые инструменты, такие как системы обнаружения вторжений и системы сканирования на предмет уязвимостей.

3.54 Система управления уязвимостями третьей стороны должна обеспечивать регулярный мониторинг следующих элементов для обнаружения потенциальных событий, связанных с нарушением кибербезопасности:

- ключевые системы и активы;
- несанкционированные подключения;
- несанкционированное программное обеспечение / приложения;
- сетевая активность.

3.55 Система управления уязвимостями третьей стороны должна обеспечивать следующее:

- наличие методик сбора, анализа и реагирования на уязвимости, ставшие известными организации из внутренних и внешних источников (например, с помощью внутреннего тестирования, из бюллетеней системы безопасности или результатов исследований безопасности);
- разрешение на использование и допуск только утвержденных инструментов, технологий и пользователей;
- минимизация выявленных уязвимостей или их документирование в качестве приемлемых рисков.

Непрерывная регистрация событий и мониторинг безопасности

3.56 Третья сторона должна обеспечить наличие организованной и согласованной системы аудита и управления журналами, гарантирующую, что ключевые системы, включая приложения, настроены на регистрацию ключевых событий (в том числе операций привилегированного доступа и действий персонала). Кроме того, такие журналы должны храниться в течение, по крайней мере, 13 месяцев. Журналы сетевого оборудования, имеющего критически важные для безопасности функции, должны быть полностью записаны и доступны для аудита в течение 13 месяцев.

Третья сторона должна гарантировать, что журналы содержат информацию о следующих событиях:

- запуск и отключение системы;
- успешная и неуспешная аутентификация;
- вход в систему и выход из нее;
- создание, изменение и удаление учетных записей;
- изменение учетных данных;
- расширение привилегий;
- блокировка учетной записи;
- подключение и удаление оборудования;
- предупреждения и сообщения об ошибках управления системой и сетью;
- изменения администратора событий безопасности; в том числе управление группами и изменения политики безопасности;
- точки запуска и остановки зарегистрированного процесса;
- регистрация событий активации и деактивации;
- изменения типа регистрируемых событий в соответствии с требованиями контрольного журнала (например, параметры запуска и любые их изменения);
- модификация (или попытка модификации) журналов;
- любая форма доступа к схеме управления системами, используемыми в связи с общедоступной сетью или службой электронных коммуникаций Великобритании.

Как минимум третья сторона должна обеспечить фиксацию следующих параметров журнала для каждого события:

- идентификация объекта, к которому относится событие;
- тип события;
- дата и время события;
- указание на успешность или неуспешность события;
- идентификатор пользователя учетной записи;
- идентификация источника события, например местоположение пользователя/системы, IP-адреса идентификатора терминала, идентификатор терминала или другие средства идентификации.

3.57 Система аудита, протоколирования и мониторинга третьей стороны должна включать следующие компоненты:

- журналы событий генерируют оповещения в реальном или близком к реальному времени для выявления несанкционированных действий;
- события и оповещения отслеживаются независимой функцией на постоянной основе, изучаются, сортируются и им присваивается уровень серьезности;
- устраненные оповещения вызывают процессы управления инцидентами безопасности на основе установленных сценариев использования защитного

мониторинга и игровых сценариев в соответствии с соглашениями об уровне обслуживания и уровнем серьезности;

- журналы рассматриваются по меньшей мере как информация с классификацией «конфиденциальных» и защищаются от попыток фальсификации, несанкционированного доступа и потери;
- ведение журналов и мониторинг синхронизируются с утвержденным источником времени NTP;
- организованы процессы для определения и настройки дополнительных сценариев использования защитного мониторинга и соответствующих журналов событий, корреляций и оповещений, необходимых для устранения существующих или возникающих значительных угроз и рисков.

4. Требования к безопасности, касающиеся персонала третьей стороны

4.1 Третья сторона должна обеспечить, чтобы весь ее персонал подписал соглашения о конфиденциальности перед началом работы в зданиях BT или с системами BT либо получением доступа к информации BT. Эти соглашения о конфиденциальности должны храниться третьей стороной и предъявляться BT для аудита.

4.2 Третья сторона должна реагировать на нарушения действующих правил контроля и стандартов безопасности (ее и BT), принимая официальные меры, включая дисциплинарные, которые могут предусматривать:

- лишение нарушителя доступа к системам или информации BT; или
- отстранение нарушителя от работ, связанных с предоставлением услуг.

Кроме того, третья сторона должна гарантировать наличие процедур, препятствующих доступу отстраненного персонала к системам и информации BT и работе, связанной с предоставлением услуг BT.

4.3 Третья сторона, в рамках, разрешенных законом, должна организовать службу анонимного информирования, куда ее персонал сможет сообщать о фактах побуждения к действиям, не соответствующим настоящим Требованиям к безопасности или нарушающим их. Соответствующие отчеты должны передаваться BT.

4.4 После прекращения персоналом третьей стороны предоставления услуг любые физические активы или информация BT, находящиеся у персонала третьей стороны, должны быть либо переданы обратно соответствующей рабочей группе BT, либо надежно уничтожены в соответствии с правилами безопасности 3.22 и 3.23.

4.5 Третья сторона должна иметь организованную и согласованную систему приемлемого использования личных и корпоративных социальных сетей, включая обеспечение того, чтобы персонал:

- не публиковал клеветнические, непристойные или оскорбительные материалы об организации, ее клиентах или заказчиках;

- не использовал логотипы организации или клиента без предварительного разрешения;
- не разглашал конфиденциальную информацию организации или клиента без предварительного согласия;
- не публиковал комментарии о компании, ее клиентах или заказчиках, которые могут быть обоснованно истолкованы как официальное мнение организации или ее клиентов;
- не разглашал информацию BT, помеченную как «общая», «конфиденциальная» или «строго конфиденциальная».

4.6 Третья сторона должна организовать обязательное обучение всего контролируемого ею персонала методам защиты информации, киберзащиты и защиты персональных данных в течение одного месяца после приема на работу и в дальнейшем не реже раза в год. Обучение должны, в частности, пройти:

- привилегированные пользователи;
- заинтересованные лица третьей стороны (например, субподрядчики, клиенты, партнеры);
- руководители высшего звена;
- персонал, обеспечивающий физическую безопасность и кибербезопасность.

4.7 Третья сторона должна провести тестирование на предмет понимания материала и знания пользователями всех требований к безопасности.

5. Аудит и проверка безопасности

5.1 Без ущерба для любого другого права аудита, которое может иметь BT, для оценки соответствия третьей стороны правилам безопасности настоящей политики Требований к безопасности третья сторона будет предоставлять BT или ее представителям доступ и содействие (по мере необходимости) для проверки документов и проведения выездных аудитов безопасности. Перед проведением планового выездного аудита третья сторона будет уведомляться о нем не менее чем за 30 рабочих дней.

Предметом аудита являются любые или все аспекты политик, процессов и систем третьей стороны, связанных с предоставляемыми услугами (если третья сторона защищает конфиденциальность какой-либо информации, не связанной с предоставлением услуг BT).

5.2 Третья сторона обязуется сотрудничать с BT и выполнить за свой счет согласованные рекомендации и любые корректирующие действия, определенные как необходимые в результате проверки документации или выездного аудита безопасности в течение 30 дней после получения уведомления от BT о серьезном несоответствии, 90 дней после получения уведомления от BT о незначительном несоответствии, или в течение периода, согласованного между сторонами, за счет третьей стороны.

6. Право инспектирования

6.1 Третья сторона должна предоставлять BT возможность проверки средств контроля в местах разработки, реализации или предоставления услуг, а также тестирования и оценки систем безопасности по обоснованному запросу (или сразу после инцидента).

6.2 Все расходы по устранению слабых мест системы, выявленных BT, несет третья сторона, которая должна устранять их в течение срока, согласованного обеими сторонами.

6.3 В случае серьезного инцидента третья сторона обязуется полностью сотрудничать в любом расследовании BT, любого регулирующего или правоохранительного органа, предоставляя по мере необходимости доступ и помощь для расследования инцидента. BT может запросить у третьей стороны изоляцию любого ее связанного актива в целях расследования, и третья сторона не должна необоснованно отклонять такой запрос или медлить с его выполнением.

7. Сертификация системы безопасности

7.1 Системы, услуги, связанные услуги, процессы и физические объекты третьей стороны должны постоянно соответствовать стандарту ISO/IEC 27001 (или сертификации, обеспечивающей эквивалентный уровень контроля и подтвержденной актом проверки независимого аудитора), а также любой исправленной или будущей редакции этого стандарта. Это соответствие должно быть обеспечено путем сертификации ISMS третьей стороны Службой по Аккредитации Великобритании (UK Accreditation Service, UKAS) или эквивалентным международным утвержденным органом сертификации, указанная область применения и заявление о применимости должны распространяться на предоставляемые услуги в местах, из которых они будут предоставляться.

7.2 Третья сторона должна предоставлять действительный сертификат после подписания контракта и повторной сертификации в будущем.

7.3 Если область действия сертификата или заявления о применимости будет изменена в течение срока действия контракта до такой степени, что он больше не будет охватывать все предоставляемые услуги в местах, из которых они предоставляются, третья сторона должна сообщить об этом BT в разумные сроки. Третья сторона должна сообщать BT в течение 2 рабочих дней о любом серьезном несоответствии, выявленном органом сертификации или третьей стороной, которое представляет риск для предоставляемых услуг.

8. Физическая безопасность — помещения BT

8.1 Третья сторона обязана соблюдать все предоставленные ей инструкции в отношении доступа в помещения BT и к системам входа в здания. Весь персонал третьей стороны, работающий в помещениях BT, должен иметь при себе и сразу же предъявлять идентификационную карточку, предоставленную третьей стороной или BT, с фотографией, позволяющей четко идентифицировать личность работника.

8.2 BT может также предоставить персоналу третьей стороны электронную карту доступа и/или карту посетителя с ограниченным сроком действия, которая должна использоваться в соответствии с местными инструкциями по выдаче и отзыву карт.

8.3 Если сотруднику третьей стороны больше не требуется доступ в здание BT и/или доступ к системам входа BT, третья сторона должна сообщить об этом BT в течение 24 часов.

8.4 Напрямую к доменам BT могут подключаться (посредством LAN-порта или беспроводного соединения) только серверы конфигурации, одобренной BT, ПК вебтоп BT и доверенные конечные устройства BT. Подключение любого ранее не согласованного с BT оборудования к домену BT без письменного разрешения BT не допускается.

8.5 Необходимо соблюдать требования физической безопасности и инструкции по работе в помещениях BT, которые, кроме всего прочего, предусматривают сопровождение персонала третьей стороны и применение особых правил работы на режимных территориях.

8.6 Если третьей стороне разрешено предоставлять своему персоналу самостоятельный доступ в помещения BT, уполномоченный представитель третьей стороны и ее персонал должны соблюдать требования документа «Доступ поставщика на объекты BT — обязательное руководство по безопасности (продажи компании BT)».

9. Физическая безопасность — помещения третьей стороны

9.1 Третья сторона должна иметь процедуру физического доступа с описанием методов доступа и допуска в помещения третьей стороны (площадки, здания, внутренние территории), где предоставляются услуги, хранится и обрабатывается информация BT. Метод доступа должен включать один или более из следующих элементов:

- действительная идентификационная карточка работника третьей стороны с четко распознаваемой и узнаваемой фотографией;
- действительная электронная карта доступа в соответствующие помещения;
- система защищенного доступа с использованием клавиатуры с возможностью авторизации, изменения кода (по крайней мере ежемесячно) и целевой смены кода;
- биометрическое распознавание.

9.2 Третья сторона должна иметь методики и процедуры контроля и мониторинга посетителей, включая персонал с правом доступа в режимные зоны, а также работников служб экологического контроля, организаций, обслуживающих системы сигнализации, и уборщиков помещений.

9.3 Режимные зоны третьей стороны, используемые для обеспечения услуг (например, помещения для сетевой передачи данных), должны отделяться от зон общего доступа и защищаться средствами контроля, гарантирующими доступ только лицам, имеющим на это разрешение. Доступ в эти зоны должен регулярно проверяться и минимум один раз в год должен проводиться пересмотр прав доступа в них.

9.4 Третья сторона должна иметь системы видеонаблюдения в местах хранения и обработки информации BT. Записи камер и записывающие устройства должны размещаться в защищенных местах во избежание изменения, удаления или «случайного» просмотра видеоматериалов, при этом доступ к записям должен контролироваться и ограничиваться только уполномоченными лицами. Записи камер видеонаблюдения должны храниться не менее 20 дней.

9.5 Третья сторона должна принимать следующие необходимые меры физической безопасности:

- противопожарные меры, включая системы сигнализации, оборудование обнаружения и тушения;
- контроль состояния окружающей среды, в частности температуры, влажности, статического электричества, а также связанные с ним управление, мониторинг и реагирование на нештатные ситуации (такие как автоматическое отключение, аварийные сигналы);
- контрольное оборудование, в частности системы кондиционирования воздуха и обнаружения попадания воды;
- предотвращение повреждения водой, размещение емкостей для воды, труб и т. д. вне помещений.

9.6 Третья сторона должна обеспечивать физический доступ в зоны хранения информации BT с помощью смарт-карт или бесконтактных карт (либо равноценных или более совершенных систем безопасности). Третья сторона также должна проводить ежемесячные проверки, подтверждающие возможность доступа только для уполномоченных лиц.

9.7 Третья сторона должна запретить фотографирование и/или создание изображений любой информации BT. При необходимости в создании таких изображений следует получить письменное разрешение у заинтересованного лица BT.

10. Предоставление помещений для размещения оборудования BT

10.1 Если на территории третьей стороны в зоне с защищенным доступом размещено оборудование BT или клиентов BT, третья сторона должна:

- предоставить BT план этажа с выделенным местом в безопасной зоне;
- гарантировать, что стойки BT и клиентов BT в помещениях заперты и доступны только уполномоченным работникам и представителям BT и третьей стороны;
- внедрить безопасный процесс управления ключами.

10.2 BT предоставит третьей стороне:

- перечень физических активов BT и клиентов BT, находящихся в помещениях третьей стороны;
- сведения о сотрудниках, субподрядчиках и агентах BT, которым необходим доступ в помещения третьей стороны (на постоянной основе).

11. Безопасная разработка программного обеспечения

11.1 Третья сторона должна обеспечить надлежащее управление производственной и непроизводственной сферами, включая следующие элементы:

- разделение производственной и непроизводственной сфер с распределением обязанностей;
- предотвращение использования оперативных данных в тестовом режиме без согласия владельцев данных и соответствия средств контроля условиям производства;
- распределение обязанностей при разработке для производственной и непроизводственной сфер.

11.2 Третья сторона должна иметь организованную и согласованную инфраструктуру разработки систем для исключения уязвимостей системы безопасности и предотвращения нарушений кибербезопасности, обеспечивающую следующие условия:

- системы создаются с использованием передовых методов безопасной разработки ПО (например, OWASP);
- код хранится надежно и проходит проверку качества;
- после тестирования и внедрения код надежно защищен от несанкционированного изменения.

12. Эскроу

12.1 Если для защиты всех сторон требуется условное депонирование у первой или третьей стороны (например, интеллектуальной собственности, исходного кода и т. д.), третья сторона должна иметь организованную и согласованную систему, предусматривающую следующее:

- договор условного депонирования с независимым, нейтральным и авторитетным эскроу-агентом;
- постоянное обновление исходного кода и других материалов у эскроу-агента для поддержания актуальности необходимой информации;
- безопасное хранение исходного кода и других материалов до выполнения условий возврата;
- разумные условия возврата;
- постоянные обновления, надлежащие платежи и возможность пересмотра договора условного депонирования.

13. Доступ к системам BT

13.1 Третья сторона обязана соблюдать все предоставленные ей инструкции доступа и использования систем BT.

13.2 Третья сторона обязана в течение 24 часов уведомить BT об отпавшей необходимости доступа для ее работника.

13.3 Третья сторона должна гарантировать использование идентификационных данных пользователя, паролей, PIN-кодов, токенов и доступа к конференциям только своим персоналом. Данные должны храниться безопасно и отдельно от используемого для доступа устройства. Если пароль становится известен постороннему лицу, он должен быть немедленно изменен.

Межсистемные соединения

13.4 Междоменное соединение с системами BT недопустимо без специального согласования и разрешения BT.

13.5 Третья сторона должна принимать все необходимые меры, чтобы гарантировать отсутствие вредоносных программ (в стандартном для компьютерной отрасли понимании) в системах BT.

13.6 Системы третьей стороны должны подключаться к системам BT через защищенные каналы, данные должны защищаться шифрованием согласно требованиям разделов 14.9, 14.10, 14.11, 14.12 и 14.13.

13.7 Третья сторона обязана использовать системы и инфраструктуру, находящиеся в выделенной логической сети. Такая сеть должна состоять только из систем, образующих защищенный комплекс обработки данных клиентов.

14. Системы третьей стороны, в которых хранится информация BT

14.1 Третья сторона должна обеспечивать установку последних обновлений и исправлений безопасности для систем, активов, сетей и приложений и должна гарантировать, что:

- Третья сторона развертывает исправления как можно скорее и прилагает все усилия, чтобы развернуть их в следующие сроки после выпуска исправления:

	Активно используемые для проведения атак	**Высокий показатель EPSS** Уязвимость CVSS: > 8,0 (высокий + критический) EPSS: ≥ 70 % (Сетевой вектор атаки — см. раздел «Определения»)	**Низкий показатель EPSS** Уязвимость CVSS: > 8,0 (высокий + критический) EPSS: < 70 % (Сетевой вектор атаки — см. раздел «Определения»)	**Другое** (несетевой вектор атаки)
Внешний интерфейс	7 дней	14 дней	30 дней	90 дней
Внутренний интерфейс	7 дней	14 дней	30 дней	90 дней/BAU

- третья сторона использует исправления, полученные от поставщиков непосредственно для конкретных систем, и исправления, которые (i) имеют

цифровую подпись или (ii) проверены с использованием хеш-кода поставщика (не следует использовать хеши MD5) для пакета обновления. Должно быть подтверждено, что эти исправления получены от авторитетной организации технической поддержки программного обеспечения с открытым исходным кодом;

- третья сторона тестирует все исправления в системах с конфигурацией, аналогичной конфигурации целевых производственных систем, перед их установкой в производственных системах, а после установки проверяется правильность работы затронутых служб;
- предупреждения об уязвимостях отслеживаются у всех поставщиков и во всех источниках информации;
- в случае невозможности установки исправлений применяются необходимые меры реагирования;
- третья сторона будет устанавливать критические исправления безопасности отдельно от функциональных обновлений, чтобы максимально ускорить развертывание исправлений, и по возможности будет отдавать приоритет критическим исправлениям безопасности, а не обновлениям функциональности.

14.2 Третья сторона должна обеспечить по крайней мере ежегодную независимую оценку ИТ-безопасности / тест на проникновение, одобренные службой безопасности BT, для ИТ-инфраструктуры и приложений третьей стороны, используемых для предоставления услуг, включая узлы послеаварийного восстановления, для выявления уязвимостей, которые могут быть использованы для взлома данных/служб. Кроме того, должна быть предусмотрена защита от любых нарушений системы безопасности посредством кибератак. Третья сторона должна по обоснованному запросу BT предоставлять доступ к отчетам по результатам тестов на проникновение, относящихся к предоставляемым услугам.

14.3 Третья сторона должна обеспечивать надежный контроль доступа к портам диагностики и управления, а также контроль средств диагностики.

14.4 Третья сторона должна обеспечить доступ к инструментам аудита только соответствующему персоналу поставщика и обеспечить контроль их использования.

14.5 Третья сторона должна гарантировать, что серверы, используемые для предоставления услуг, не развернуты в ненадежных сетях (за пределами периметра безопасности третьей стороны, вне ее административного контроля, например с подключением к Интернету) без соответствующих мер безопасности.

Управление активами

14.6 Третья сторона должна поддерживать точный и актуальный реестр всех технологических активов, способных хранить или обрабатывать информацию, чтобы доступ предоставлялся только авторизованным устройствам, а неавторизованные и неуправляемые устройства были обнаружены и не могли получить доступ. Этот реестр должен включать все аппаратные средства независимо от того, подключены они к сети организации или нет. Все

оборудование BT, размещенное в помещениях третьей стороны, если такое имеется, должно быть включено в реестр.

14.7 Третья сторона должна внести в реестр информационных активов следующие элементы:

- физические устройства и системы, программные платформы и приложения, внешние информационные системы;
- ресурсы (например, аппаратные средства, устройства, данные, время и программное обеспечение), приоритет которых определен на основе их классификации, критичности и ценности для бизнеса;
- организационные и коммуникационные потоки данных, включая внешние/сторонние потоки;
- процессы ручной обработки данных BT или клиентов BT.

14.8 Третья сторона должна поддерживать точный и актуальный реестр программных активов для всего программного обеспечения в сети, чтобы только авторизованное программное обеспечение было установлено и могло выполняться, а неавторизованное и неуправляемое программное обеспечение было обнаружено и не было установлено или выполнено.

Криптография

14.9 Третья сторона должна обеспечить, чтобы информация BT, классифицированная как конфиденциальная или строже, была соответствующим образом зашифрована (во время передачи и в состоянии покоя), и все шифрование должно выполняться с помощью надежных современных криптографических алгоритмов и шифров, использующих надежные механизмы защиты целостности, а также в соответствии с отраслевыми стандартами безопасного согласования ключей и протоколов и управления ключами. Для передачи данных не допускаются следующие варианты TLS: TLS версий 1.0, 1.1 и SSL (все версии). Не допускаются следующие варианты SSH (SFTP): SSH версии 1. Следующие параметры IPSec не разрешены: IKE версии 1.

14.10 Длина криптографических ключей должна соответствовать следующим значениям или превышать их:

- симметричные ключи (например, AES) должны иметь длину не менее 256 бит;
- асимметричные ключи (например, RSA) должны иметь длину не менее 3072 бит;
- ключи эллиптической кривой должны иметь длину не менее 384 бит.

14.11 После объявления NIST о том, что криптоалгоритм больше не безопасен, его нельзя использовать для новых развертываний. Для существующих развертываний необходимо пересмотреть дальнейшее использование устаревших криптоалгоритмов и предложить план перехода от устаревших криптоалгоритмов к более безопасной альтернативе.

14.12 Для симметричного шифрования не допускается использование следующих алгоритмов: 3DES-168 (если его использование не является требованием международного стандарта), 3DES-112, Blowfish, Twofish, RC4, IDEA, Camellia, Seed и ARIA.

14.13 Для защиты хранимых данных, то есть паролей, необходимо использовать «соленое» хеширование. Хеширование также может быть использовано для анонимизации данных перед обработкой, например для MSISDN или платежей. Использование алгоритмов хеширования MD2, MD4, MD5 и SHA-1 не допускается.

Конфигурация систем

14.14 Третья сторона должна иметь организованную и согласованную инфраструктуру для обеспечения надлежащей конфигурации систем, включающую следующие элементы:

- конфигурация систем и сетевых устройств в соответствии с принципами безопасной работы (по принципу наименьшей функциональности и отсутствия несанкционированного программного обеспечения);
- правильная и стабильная настройка времени на устройствах;
- отсутствие вредоносного программного обеспечения в системах;
- проверка и мониторинг целостности сборок / устройств.

Защита от вредоносного ПО

14.15 Третья сторона должна обеспечивать самую современную защиту от вредоносных программ для всех используемых ИТ-активов, чтобы предотвращать сбои в обслуживании или нарушение безопасности, гарантировать реализацию необходимых процедур информирования пользователей.

Защита от вредоносных программ должна включать, в частности, обнаружение программ-вымогателей, несанкционированного мобильного кода, вирусов, шпионских программ, программ для перехвата вводимой с клавиатуры информации, ботнетов, червей, троянов и т. д.

Защита от атак типа «отказ в обслуживании»

14.16 Третья сторона должна обеспечить защиту ключевых систем от простых (DoS) и распределенных (DDoS) атак типа «отказ в обслуживании».

15. Хранение третьей стороной информации BT

15.1 В дополнение к средствам контроля, указанным в разделе 14, системы третьей стороны, в которых хранится информация BT, если третья сторона хранит информацию BT в центре данных или облачном решении: для помещений хранения должен быть получен сертификат ISO/IEC 27001 для системы управления безопасностью (или сертификаты, которые демонстрируют наличие эквивалентных средств контроля, что подтверждается отчетом независимого аудитора).

16. Безопасность сети — собственная сеть BT

В тех случаях, когда третья сторона будет устанавливать оборудование, настраивать, обслуживать, ремонтировать, контролировать сеть BT или управлять ею, будут применяться следующие правила.

16.1 По запросу третья сторона должна предоставить BT имена, адреса и другие сведения, которые BT может обоснованно потребовать, обо всех отдельных сотрудниках третьей стороны, которые:

- время от времени будут непосредственно вовлечены в развертывание, обслуживание услуг и/или управление ими (до того как они будут соответственно привлечены);
- должны поддерживать связь с BT в отношении обсуждения уязвимостей, выявленных BT и/или третьей стороной в услугах.

16.2 Что касается деятельности по поддержке в Великобритании, третья сторона должна предоставить группу специалистов по безопасности, включающую минимум одного гражданина Великобритании, который должен быть доступен для связи с BT. Кроме того, эта группа должна присутствовать на собраниях, которые BT время от времени назначает.

16.3 Третья сторона должна предоставлять BT перечень (обновляемый по мере необходимости) всех активных компонентов услуг и их поставщиков.

16.4 Третья сторона должна обеспечить, чтобы при установке новых систем, оборудования или программного обеспечения в собственной сети BT использовалась самая последняя версия программного обеспечения и исправление.

16.5 Третья сторона должна обеспечить, чтобы на всем сетевом оборудовании, установленном третьей стороной, были активированы все журналы, относящиеся к безопасности, и отправлены в сетевые системы регистрации BT.

16.6 Третья сторона должна своевременно предоставить BT (т. е. как можно скорее, чтобы дать возможность исправить ситуацию до публичного объявления) информацию в отношении любых уязвимостей в услугах и выполнить за свой счет такие обоснованные требования в отношении уязвимостей, которые могут быть выдвинуты BT.

16.7 Третья сторона должна обеспечить за свой счет периодическую независимую проверку всех связанных с безопасностью элементов услуг, оказываемых BT или для BT, с удовлетворительным для BT результатом.

16.8 Третья сторона обязуется незамедлительно и в любом случае в течение 7 рабочих дней предоставлять BT полную информацию о любых функциях и/или функциональных возможностях (существующих или запланированных) любой услуги:

- которые, как известно третьей стороне, являются; или
- которые BT обоснованно считает (и уведомляет об этом третью сторону) предназначенными или возможными к использованию для законного или любого другого перехвата телекоммуникационного трафика. Информация должна быть максимально подробной, чтобы компания BT могла полностью понять суть, состав и объем таких функций и/или функциональных возможностей.

16.9 Третья сторона не должна использовать какие-либо инструменты мониторинга сети, позволяющие просматривать информацию о приложениях.

16.10 Персонал третьей стороны, создающий, развивающий и/или поддерживающий собственную сеть BT, должен пройти проверку перед приемом на работу уровня как минимум L2. Проверки перед приемом на работу уровня L3 необходимы для должностей, определенных компанией BT.

16.11 Третья сторона должна разрешить BT установить защитное программное обеспечение, соответствующее спецификации BT, в любой виртуальной инфраструктуре третьей стороны (включая виртуальные машины и контейнеры) или установленной третьей стороной операционной системе, работающей в сетях BT.

16.12 Третья сторона должна обеспечивать установку последних обновлений и исправлений безопасности для систем, активов, сетей и приложений и должна гарантировать, что:

Третья сторона развертывает исправления как можно скорее и прилагает все усилия, чтобы развернуть их в следующие сроки после выпуска исправления:

	Активно используемые для проведения атак	**Высокий показатель EPSS** Уязвимость CVSS: > 8,0 (высокий + критический) EPSS: ≥ 70 % (Сетевой вектор атаки — см. раздел «Определения»)	**Низкий показатель EPSS** Уязвимость CVSS: > 8,0 (высокий + критический) EPSS: < 70 % (Сетевой вектор атаки — см. раздел «Определения»)	**Другое** (несетевой вектор атаки)
Внешний интерфейс	7 дней	14 дней	30 дней	90 дней
Внутренний интерфейс	7 дней	14 дней	30 дней	90 дней/BAU

- третья сторона использует исправления, полученные от поставщиков непосредственно для конкретных систем, и исправления, которые (i) имеют цифровую подпись или (ii) проверены с использованием хеш-кода поставщика (не следует использовать хеши MD5) для пакета обновления. Должно быть подтверждено, что эти исправления получены от авторитетной организации технической поддержки программного обеспечения с открытым исходным кодом;
- третья сторона тестирует все исправления в системах с конфигурацией, аналогичной конфигурации целевых производственных систем, перед их установкой в производственных системах, а после установки проверяется правильность работы затронутых служб;
- предупреждения об уязвимостях отслеживаются у всех поставщиков и во всех источниках информации;

- в случае невозможности установки исправлений применяются необходимые меры реагирования;
- Третья сторона будет поставлять критические исправления безопасности отдельно от функциональных обновлений, чтобы максимально ускорить развертывание исправлений, и по возможности будет отдавать приоритет критическим исправлениям безопасности, а не обновлениям функциональности.

Закон «О безопасности телекоммуникаций» 2021 года (TSA)

Если третья сторона поставляет или предоставляет товары, услуги или средства для использования в связи с общедоступной сетью или службой электронных коммуникаций Великобритании, применяются следующие меры безопасности.

16.13 Если третья сторона оказывает поддержку более чем одному оператору, должны быть внедрены меры контроля, чтобы предотвратить негативное влияние одного оператора или его сети на любого другого оператора или его сеть.

16.14 Если третья сторона работает в качестве администратора третьей стороны для более чем одного оператора, применяются следующие правила:

- внедрение логического разделения в сети третьей стороны для разделения данных и сетей клиентов;
- внедрение разделения между средами управления третьей стороны, используемыми для сетей разных операторов;
- внедрение и выполнение функций по обеспечению безопасности на границе между сетью третьей стороны и сетью оператора;
- внедрение технических средств контроля для ограничения возможностей пользователей или систем оказывать негативное воздействие более чем на одного оператора;
- внедрение физически и логически независимых рабочих станций с привилегированным доступом для каждого оператора;
- внедрение независимых административных доменов и учетных записей для каждого оператора.

16.15 При предоставлении сетевого оборудования третьи стороны должны предоставить BT декларацию безопасности о том, как производится безопасное оборудование и как обеспечивается безопасность оборудования в течение всего срока его службы. Эта декларация безопасности должна охватывать требования оценки безопасности поставщика, опубликованной в Приложении B Правил безопасности телекоммуникаций, и должна быть утверждена на соответствующем уровне руководства, согласованном с BT.

16.16 Если третья сторона предоставляет сетевое оборудование, то применимы следующие меры контроля:

- третья сторона гарантирует, что она будет придерживаться стандарта не ниже, чем ее опубликованная «декларация безопасности»;
- третья сторона предоставит актуальное руководство по безопасному развертыванию оборудования;

- третья сторона будет поддерживать все оборудование и все программные и аппаратные субкомпоненты в течение всего срока действия контракта;
- третья сторона предоставит подробную информацию обо всех основных компонентах сторонних производителей и зависимостях, включая продукт и версию, компоненты с открытым исходным кодом, уровень и период поддержки;
- третья сторона устранит все проблемы безопасности, представляющие риск безопасности для сети или услуг BT, обнаруженные в продуктах, в течение разумного времени после получения уведомления, предоставляя регулярные обновления о прогрессе в промежуточный период. Такое время должно быть надлежащим образом согласовано между BT и третьей стороной. Речь идет обо всех продуктах, на которые влияет уязвимость, а не только о продукте, в котором она была обнаружена.
- Третья сторона либо удалит, либо изменит пароли по умолчанию и учетные записи по умолчанию или жестко закодированные, либо обеспечит, чтобы сетевое оборудование было настроено таким образом, чтобы сотрудники BT могли это сделать.
- Третья сторона по возможности отключит незашифрованные протоколы управления и, если это невозможно, определит наличие таких протоколов для BT, чтобы их использование было ограничено.

16.17 Если третья сторона получила международно признанные оценки безопасности или сертификаты для оборудования (например, Common Criteria или NESAS), она обязана предоставить BT полную информацию о результатах, подтверждающих эту оценку или сертификат.

16.18 Если собственная сеть третьей стороны потенциально может повлиять на сети BT, третья сторона, по рекомендации BT, должна пройти такой же уровень тестирования, какой BT применяет к сетям BT, и устранить выявленные уязвимости, как согласовано обеими сторонами.

16.19 Третья сторона уполномочивает BT предоставлять информацию о проблемах безопасности, если это необходимо в целях обеспечения безопасности сети.

16.20 Инфраструктура и системы, используемые для обслуживания сетей BT, должны находиться на территории Великобритании.

16.21 Если третья сторона выполняет функции BT по надзору за сетью, оборудование, используемое для этой функции, должно быть расположено в Великобритании и эксплуатироваться персоналом, находящимся в Великобритании.

16.22 Если третья сторона отвечает за безопасность сети и журналы аудита, они должны храниться в Великобритании и защищаться в соответствии с законодательством Великобритании.

16.23 Если третья сторона работает в качестве администратора третьей стороны, BT сохраняет право определять разрешения учетных записей, используемых третьей стороной для доступа к своей сети, и требовать все журналы, относящиеся к безопасности сети третьей стороны, в той степени, в которой эти журналы относятся к доступу в сеть BT. Третья сторона должна контролировать и проверять деятельность своего персонала при доступе к сети BT.

17. Безопасность сети третьей стороны

17.1 Третья сторона должна гарантировать, что целостность сети сохраняется и поддерживается следующими действиями, и уведомлять BT в тех случаях, когда это технически невозможно:

- Внешние подключения к сети документируются, защищаются брандмауэром, проверяются и утверждаются до установления подключения для предотвращения нарушения безопасности данных.
- Сеть должным образом спроектирована с использованием принципов «глубокой защиты», чтобы свести к минимуму нарушения кибербезопасности посредством соответствующих средств контроля, предотвращающих любую целенаправленную атаку, такую как «сегментация сети».
- Структура и оснащение сети пересматриваются по крайней мере ежегодно.
- Весь беспроводной доступ к сети защищен протоколами авторизации, аутентификации, сегментации и шифрования для предотвращения нарушений безопасности.
- Используются защищенные каналы связи между устройствами и станциями управления.
- Используются безопасные каналы связи между устройствами в соответствии с требованиями, включая шифрование всех операций доступа администратора, осуществляемых не с консолей управления.
- Используется надежная многоуровневая и зонированная архитектура с эффективным управлением идентификаторами и конфигурацией операционной системы, которая должна быть соответствующим образом защищена и задокументирована.
- Отключены (где это возможно) службы, приложения и порты, которые не будут использоваться.
- Отключены или удалены гостевые учетные записи.
- Исключены доверительные отношения между серверами.
- Для выполнения операций используется передовой принцип безопасности «наименьшие привилегии».
- Принимаются надлежащие меры для обнаружения вторжений и/или защиты от них.
- Обеспечивается необходимый контроль целостности файлов для обнаружения любых добавлений, изменений или удалений критических системных файлов или данных.
- Меняются все пароли по умолчанию и пароли поставщика перед вводом компонентов сети в эксплуатацию.
- Отключаются незашифрованные протоколы управления, если это технически возможно.

17.2 Третья сторона в работе с сетями должна соответствовать всем законодательным и нормативным требованиям, а также:

- прилагать все усилия для предотвращения доступа посторонних лиц (например, хакеров) к сетям третьей стороны;
- прилагать все усилия для снижения риска неправомерного использования сетей третьей стороны лицами, имеющим доступ к ней;
- прилагать все усилия для выявления любых нарушений безопасности и обеспечения быстрого устранения любых нарушений, а также идентификации лиц, которые получили доступ к сети, и определения того, как они его получили.

Закон «О безопасности телекоммуникаций» 2021 года

17.3 Если третья сторона поставляет или предоставляет товары, услуги или средства для использования в связи с общедоступной сетью или службой электронных коммуникаций Великобритании, применяются следующие дополнительные меры безопасности.

- Внешние системы, за исключением оборудования в помещениях заказчика (CPE), проверяются на безопасность каждые два года или при значительных изменениях.
- Наборы конфиденциальных данных и конфиденциальные или критически важные функции не размещаются на оборудовании на открытой границе сети.
- Если они не защищены криптографически, между открытой границей и конфиденциальными или критическими функциями должно быть реализовано физическое и логическое разделение.
- Разделение безопасности с использованием функций, обеспечивающих безопасность, должно быть реализовано между открытой границей и конфиденциальными или критическими функциями.

18. Облачная информационная безопасность

18.1 Третья сторона должна быть сертифицирована в соответствии с последней версией ISO27017 или иметь организованную и согласованную систему, чтобы гарантировать, что любое использование облачной технологии и конфиденциальных данных, хранящихся в облаке, одобрено и контролируется согласно требованиям последней версии Матрицы средств контроля облачных вычислений (CCM) Альянса безопасности облачных вычислений.

18.2 В соглашениях об инфраструктурном и сетевом обслуживании (внутреннем и стороннем) должны четко указываться общие обязанности, меры безопасности, объем и уровни обслуживания, а также требования бизнеса или клиента.

18.3 Третья сторона должна применять меры безопасности по всем аспектам предоставляемой услуги, защищая конфиденциальность, надежность, качество и целостность систем, минимизируя возможности несанкционированного доступа к информации BT и услугам для BT (например, другими пользователями облачной сети).

18.4 В той степени, в которой третья сторона предоставляет BT размещенные приложения или услуги, как одноарендные, так и мультиарендные, включая

программное обеспечение как услугу, платформу как услугу, инфраструктуру как услугу и подобные предложения, для сбора, передачи, хранения или иной обработки конфиденциальных данных, третья сторона должна предоставить BT возможность:

- изолировать такие конфиденциальные данные логически от данных других клиентов третьей стороны;
- ограничивать, регистрировать и контролировать доступ к таким конфиденциальным данным в любое время, включая доступ персонала третьей стороны;
- создавать, включать, отключать и удалять наивысший ключ шифрования (также называется «управляемый ключ клиента»), используемый для шифрования и расшифровки последующих ключей, включая самый нижний ключ шифрования данных;
- ограничивать, регистрировать и отслеживать доступ к управляемому ключу клиента в любое время. Ни при каких обстоятельствах никакой последующий ключ шифрования, ключ шифрования в иерархии ключей ниже, чем управляемый ключ клиента, не должен храниться в той же системе, что и конфиденциальные данные, если он не зашифрован управляемым ключом клиента (что также называют «обертыванием» управляемым ключом клиента).

19. SIM-карты

19.1 Если третья сторона предоставляет SIM-карты, то применимы следующие меры контроля.

- Для SIM-карт с фиксированным профилем третья сторона должна обеспечить надлежащую защиту конфиденциальных данных SIM-карты производителем SIM-карты.
- Для SIM-карт с фиксированным профилем третья сторона должна обеспечить защиту конфиденциальности, целостности и доступности закрытых данных SIM-карты, передаваемых производителю SIM-карты, на каждом этапе их срока службы.

20. Информация, классифицируемая правительством Его Величества как «СЛУЖЕБНАЯ» или выше

20.1 К каждой третьей стороне, занимающейся хранением, обработкой или передачей информации, классифицируемой как «СЛУЖЕБНАЯ» в соответствии с регулярно обновляемой Системой классификации безопасности правительства Его Величества, будут применяться дополнительные требования к безопасности, изложенные в Приложении 1 к настоящим Требованиям к безопасности.

21. Термины и их толкование

21.1 Если иное не указано ниже, слова и выражения, используемые в настоящих Требованиях к безопасности, имеют то же значение, что и в контракте.

Доступ и **получение доступа** — обработка, хранение информации BT или операции с такой информацией, полученной с использованием одного или нескольких из следующих способов:

a. посредством подключения к системам BT,

b. в бумажном или неэлектронном формате,

c. информации BT в системах поставщика,

d. через мобильные средства передачи информации;

и/или доступ в помещения BT для предоставления услуг, исключая доставку аппаратных средств и присутствие на совещаниях.

Информация BT — вся информация, касающаяся BT или клиента BT, предоставленная Поставщику, и вся информация, которая обрабатывается Поставщиком от имени BT или клиента BT по контракту.

Заинтересованная сторона BT — представитель BT, ответственный за объем работ, которые выполняет третья сторона.

Системы BT — услуги и компоненты услуг, продукты, сети, серверы, процессы, печатные системы или ИТ-системы (полностью или частично), принадлежащие и/или управляемые BT, или другие системы, которые могут быть размещены в помещениях BT.

Сети BT — любая общедоступная сеть электронных коммуникаций, управляемая BT, как определено в разделе 32 закона «О коммуникациях» 2003 года.

BYOD — концепция использования собственных устройств сотрудников.

Контракт — контракт, заключенный сторонами на поставку товаров, программного обеспечения или услуг, в котором есть ссылки на настоящие Требования к безопасности.

Оборудование в помещениях заказчика — оборудование, предоставляемое клиентам поставщиком услуг и управляемое им, которое используется или предназначено для использования в качестве части сети или услуги. Сюда не входят потребительские электронные устройства, такие как мобильные телефоны и планшеты, но включены такие устройства, как пограничные брандмауэры, оборудование программно-определяемой глобальной компьютерной сети (SD-WAN) и комплект фиксированного беспроводного доступа. “”

Cyber Essentials Plus — поддерживаемая правительством Великобритании система, помогающая организациям защитить себя от распространенных кибератак.

Кибербезопасность — это методы и процедуры, с помощью которых люди и организации снижают риск кибератак. Основная функция кибербезопасности — защита устройств, которыми мы все пользуемся (смартфоны, ноутбуки, планшеты и компьютеры), и услуг, к которым мы получаем доступ, как онлайн, так и на работе, от кражи или повреждения.

EPSS — Exploit Prediction Scoring System.

Эскроу — соглашение об условном депонировании исходного кода, заключенное в соответствии с контрактом, для использования, копирования, сохранения и изменения такого исходного кода в коммерческих целях BT (включая право на компиляцию такого исходного кода).

Открытая граница — оборудование, которое либо находится в помещении заказчика, либо напрямую доступно с оборудования заказчика/пользователя, либо физически уязвимо. Физически уязвимое оборудование включает оборудование в придорожных шкафах или прикрепленное к уличному оборудованию. К открытой границе относятся CPE, оборудование базовых станций, оборудование OLT и оборудование MSAN/DSLAM.

Установившаяся в отрасли практика обеспечения безопасности — в отношении любых взятых обязательств и обстоятельств означает реализацию мер безопасности, политик, стандартов и инструментов, которую следует обычно и обоснованно ожидать от квалифицированного и опытного человека, занимающегося тем же видом деятельности при тех же или аналогичных обстоятельствах.

NDA означает соглашение о неразглашении. Это обязательный договор между двумя или более сторонами, который предотвращает передачу конфиденциальной информации другим лицам.

NESAS — схема обеспечения безопасности сетевого оборудования Ассоциации GSM.

Сетевой актив — элемент, который является частью совокупности взаимосвязанных компонентов, таких как компьютеры, маршрутизаторы, концентраторы, кабели и телекоммуникационные контроллеры, которые составляют сеть.

Сетевой вектор атаки означает, что уязвимый компонент связан с сетевым стеком и набор возможных злоумышленников выходит за рамки других вариантов, перечисленных ниже, вплоть до всей сети Интернет. Такую уязвимость часто называют «удаленно эксплуатируемой», и ее можно представить как атаку, которую можно использовать на уровне протокола на расстоянии одного или нескольких сетевых хопов (например, через один или несколько маршрутизаторов). Примером сетевой атаки может служить злоумышленник, вызывающий отказ в обслуживании (DoS) путем отправки специально созданного TCP-пакета через глобальную сеть (например, CVE 2004 0230).

Функция надзора за сетью — компоненты сети BT, которые осуществляют надзор и контроль критически важных функций безопасности, что делает их жизненно важными для общей безопасности сети. Они необходимы BT для понимания сети, обеспечения ее безопасности или восстановления.

Безопасность сетей — безопасность взаимосвязанных каналов и узлов связи, которые логически соединяют технологии конечного пользователя вместе, а также связанных систем управления.

NIST — это Национальный институт стандартов и технологий, подразделение Министерства торговли США. Ранее известный как Национальное бюро стандартов, NIST продвигает и поддерживает стандарты измерений. Институт также осуществляет активные программы по поощрению и оказанию помощи промышленности и науке в разработке и использовании этих стандартов.

Заявление в отношении конфиденциальной служебной информации — письменное заявление, которое должно делаться Поставщиком в отношении ролей с доступом к информации, классифицированной как «служебная и конфиденциальная», или дающих высокие привилегии доступа к инфраструктуре хранения, обработки или

передачи информации, классифицированной как «служебная и конфиденциальная», форма которого приведена в Приложении 1.

Рабочая станция с привилегированным доступом (PAW) — рабочие станции, через которые возможен привилегированный доступ.

Критическая функция безопасности — любая функция сети или услуги BT, работа которой может оказать существенное влияние на надлежащую работу всей сети или услуги или их существенной части.

Требования к безопасности — это настоящий документ с периодическими обновлениями.

SIM — уникальный аппаратный компонент или маркер, а также связанное с ним программное обеспечение, используемое для аутентификации доступа абонента к сети. В данном документе термин SIM включает в себя средства технического обеспечения UICC/eUICC, приложения SIM/USIM/ISIM, функциональность eSIM и RSP, а также любые утилиты SIM.

Субподрядчик — субподрядчик поставщика, который предоставляет или участвует в предоставлении услуг или который нанимает или привлекает лиц, занимающихся предоставлением услуг.

Услуга — все **товары**, **программное обеспечение** или **услуги**, определенные в контракте.

Транзакция — транзакционные данные/информация, получаемые из транзакций, т. е. данные, генерируемые различными приложениями в ходе выполнения или поддержки повседневных бизнес-процессов.

Доверенный платформенный модуль — технология, предназначенная для выполнения аппаратных функций, связанных с безопасностью. Чип TPM — это защищенный криптопроцессор, предназначенный для выполнения криптографических операций. Чип оснащен множеством физических механизмов защиты, что делает его устойчивым к взлому, а вредоносное программное обеспечение не может вмешаться в функции безопасности TPM. Наиболее распространенные функции TPM используются для определения целостности системы, а также для создания и использования ключей. В процессе загрузки системы загружаемый код (включая микропрограмму и компоненты операционной системы) может измеряться и записываться в TPM. Измерения целостности можно использовать в качестве доказательства того, как система запускалась, и убедиться, что ключ на базе TPM использовался, только когда для загрузки системы применялось правильное программное обеспечение.

Третья сторона — поставщик BT.

Администратор третьей стороны означает поставщика управляемых услуг, поставщика групповых функций или внешней поддержки оборудования поставщика третьей стороны (например, функция поддержки третьей линии)

Персонал третьей стороны — любые лица, привлеченные поставщиком или его субподрядчиками к выполнению обязательств поставщика по контракту.

Сеть третьей стороны — любая сеть поставщика.

Система третьей стороны — любые принадлежащие поставщику компьютерные, программные или сетевые системы, используемые для доступа, хранения или обработки информации BT или задействованные в предоставлении услуг.

Толкование словесных выражений

21.2 Любые слова, следующие за словами «включая», «включает», «в частности», «например» или любыми аналогичными выражениями, должны толковаться как пояснительные и не ограничивать смысл слов, описаний, определений, фраз или терминов, стоящих перед такими выражениями.

21.3 Если обязательство или право Стороны выражается в виде обязательства или права, которое она «**может**» осуществить или реализовать, принятие решения в отношении такого осуществления или реализации остается на усмотрение этой Стороны.

21.4 Там, где в документе приведена какая-либо гиперссылка (**URL-адрес**), она подразумевает онлайн-ресурс, который доступен по этому URL-адресу или другому заменяющему его URL-адресу, периодически сообщаемому соответствующей Стороне.

Версия	Описание	Автор	Дата
5.0	Закон «О безопасности телекоммуникаций» (TSA) 2021 года и принятие компанией BT CIS	Джемма Тернер	25/10/22
5.1	Поправка к пункту 14.9 TLS	Джемма Тернер	17/04/23
5.2	Изменения в различных пунктах для учета TSA и уязвимостей	Джемма Тернер	30/11/23

ПРИЛОЖЕНИЕ 1. Дополнительные требования к безопасности

Если от третьей стороны потребуется обеспечить хранение, обработку или передачу информации, классифицированной как «СЛУЖЕБНАЯ» или строже, или доступ к ней, третья сторона будет соблюдать требования безопасности BT и дополнительно требования, изложенные в данном Приложении 1. Во всех случаях контроль на высшем уровне будет иметь приоритет над требованиями, задокументированными в других разделах настоящих Требований безопасности.

1. РАБОТНИКИ

1.1 Весь персонал третьей стороны, имеющий доступ к информации, классифицированной как «СЛУЖЕБНАЯ» или строже, или обладающий повышенными привилегиями к инфраструктуре, хранящей, обрабатывающей или передающей информацию, классифицированную как «СЛУЖЕБНАЯ» или строже:

1.1.1 Должен пройти предварительный отбор на работу в соответствии с базовым стандартом безопасности персонала (BPSS).

1.1.2 Должен подписать личную декларацию по закону «О государственной тайне».

1.1.3 Должен быть лишен доступа к информации или системам, если у него нет необходимых допусков по безопасности, как указано в соответствующем контракте.

2. ИНСТРУКТАЖ ПО БЕЗОПАСНОСТИ

2.1 Третья сторона обязуется проводить обучение по безопасности при приеме на работу и не реже одного раза в год для всего персонала, имеющего доступ к информации, классифицированной как «СЛУЖЕБНАЯ» или строже, или обладающего повышенными привилегиями к инфраструктуре, хранящей, обрабатывающей или передающей информацию, классифицированную как «СЛУЖЕБНАЯ» или строже. Это обучение должно охватывать требования по работе с информацией в соответствии с требованиями Системы классификации безопасности правительства Его Величества, как подробно описано в Руководстве BT по защите информации правительства Его Величества для третьих сторон, которое должно быть предоставлено третьей стороне компанией BT.

2.2 Третья сторона будет обновлять должностные инструкции для всего персонала, имеющего доступ к информации, классифицированной как «СЛУЖЕБНАЯ» или строже, или обладающего повышенными привилегиями к инфраструктуре, хранящей, обрабатывающей или передающей информацию, классифицированную как «СЛУЖЕБНАЯ» или строже, и будет обязывать пройти обучение, описанное в пункте 2.1 выше. Третья сторона будет вести журнал инструктажа и предоставлять его BT по запросу.

3. КОНТРОЛЬ ДОСТУПА

3.1 При отзыве или изменении ролей сотрудников их права доступа к системам третьей стороны должны отзываться в течение одного (1) рабочего дня.

3.2 Если работники третьей стороны, включая подрядчиков, временных сотрудников и привлеченных работников, имеют высокие привилегии доступа к инфраструктуре BT, третья сторона должна письменно уведомить BT в течение 1 рабочего дня с

момента, когда у них исчезает необходимость в доступе к системам BT (например, после увольнения или изменения роли).

3.3 Если работникам третьей стороны, включая подрядчиков, временных сотрудников и привлеченных работников, были выданы постоянные карты доступа в помещения BT, третья сторона должна письменно уведомить BT в течение 1 рабочего дня с момента, когда исчезает необходимость в их доступе в помещения BT (например, после увольнения или изменения роли).

4. ОЦЕНКА И КЛАССИФИКАЦИЯ АКТИВОВ

4.1 Третья сторона должна ввести дополнительные процедуры для выполнения требований к обращению с информацией в соответствии с периодически обновляемой Системой классификации безопасности Правительства Его Величества.

5. РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ И ОТЧЕТНОСТЬ ПО НИМ — СОГЛАШЕНИЯ ОБ УРОВНЕ ОБСЛУЖИВАНИЯ

5.1 Третья сторона будет уведомляться о необходимости заключения отдельных соглашений об уровне обслуживания для поддержки процесса реагирования на инциденты. Они могут заменять любое предыдущее соглашение, указанное в настоящих Требованиях к безопасности.

6. АУДИТ, ТЕСТИРОВАНИЕ И МОНИТОРИНГ

6.1 Третья сторона будет осуществлять круглосуточный мониторинг безопасности, если это определено BT, для инфраструктуры третьей стороны, которая поддерживает обработку, хранение или передачу информации, классифицированной как «СЛУЖЕБНАЯ» или строже.

7. НЕПРЕРЫВНОСТЬ РАБОТЫ И ПОСЛЕАВАРИЙНОЕ ВОССТАНОВЛЕНИЕ

7.1 Третья сторона подготовит план обеспечения непрерывности своей работы и послеаварийного восстановления в соответствии со стандартом BS ISO 22301 в течение 30 дней после подписания контракта.

8. МЕСТОНАХОЖДЕНИЕ

8.1 Если иное не указано BT, услуги должны предоставляться в пределах физических границ Великобритании или, если применимо, ЕЭЗ. Любая удаленная поддержка услуги и/или управление ею поставщиком из-за границы должны осуществляться только в соответствии с процессом утверждения, изложенным в соответствующем контракте между BT и соответствующим государственным учреждением.

9. ДОПОЛНИТЕЛЬНЫЕ ТРЕБОВАНИЯ ДЛЯ ИНФОРМАЦИИ КАТЕГОРИИ «СЛУЖЕБНАЯ КОНФИДЕНЦИАЛЬНАЯ» ИЛИ СТРОЖЕ

9.1 Все роли, определенные третьей стороной как имеющие доступ к информации, классифицированной как «СЛУЖЕБНАЯ КОНФИДЕНЦИАЛЬНАЯ» или строже, или обладающие повышенными привилегиями к инфраструктуре, которая хранит, обрабатывает или передает информацию, классифицированную как «СЛУЖЕБНАЯ КОНФИДЕНЦИАЛЬНАЯ» или строже, должны быть задокументированы в «Заявлении в отношении служебной конфиденциальной информации», и необходимо предоставить BT заполненное «Заявление в отношении служебной конфиденциальной информации» до подписания контракта.

9.2 Если от поставщика требуется обеспечить хранение, обработку или передачу информации, классифицированной правительством Его Величества как «СЛУЖЕБНАЯ КОНФИДЕНЦИАЛЬНАЯ» или выше, либо предоставить доступ к ней, поставщик должен провести оценку риска безопасности персонала для всех должностей, указанных в пункте 2 «Заявления в отношении конфиденциальной служебной информации», в соответствии с требованиями, изложенными в документе Национального управления по защите безопасности (NPSA) «Оценка риска безопасности персонала — руководство» (4-е издание — июнь 2013 года или позднее).

ПРИЛОЖЕНИЕ 1, ДОКУМЕНТАЛЬНОЕ ПОДТВЕРЖДЕНИЕ 1 — ОБРАЗЕЦ ДОКУМЕНТА «ЗАЯВЛЕНИЕ В ОТНОШЕНИИ КОНФИДЕНЦИАЛЬНОЙ СЛУЖЕБНОЙ ИНФОРМАЦИИ»

1. Предоставляемые системы/услуги

Перечислите системы и услуги, предоставляемые клиенту правительства Его Величества.

Система	Услуга

2. Роли третьей стороны, требующие допуска к закрытой информации.

Должность	Требуемый уровень допуска к закрытой информации
* напр. Администрирование баз данных	Доступ к секретной информации

3. Управление уязвимостями

Система	Оценка типа уязвимости	Периодичность

4. Аудит, тестирование и мониторинг

Системы с круглосуточным мониторингом согласно требованиям BT

ПРИЛОЖЕНИЕ 2. Закон «О безопасности телекоммуникаций» 2021 года. Соответствие Требований к безопасности Своду правил

Номера кодов	Требование	Положение о требованиях к безопасности BT
M1.02	Тестирование безопасности внешних систем, за исключением CPE, обычно должно проводиться не реже одного раза в два года и в любом случае сразу после значительных изменений.	17.3
M1.03	Оборудование на открытой границе не должно содержать конфиденциальных данных или критически важных для безопасности функций.	17.3
M1.04	Между открытой границей и критическими функциями безопасности должно быть реализовано физическое и логическое разделение. (Обратите внимание, что это требование может не понадобиться, если наборы данных и функции могут быть криптографически защищены от взлома.)	17.3
M1.05	Между открытой границей и критическими или конфиденциальными функциями, которые применяют защитные меры, должны существовать границы безопасности.	17.3
M2.02	Все случаи привилегированного доступа должны регистрироваться в журнале.	3.56, 3.57
M2.06	Ответственность за инфраструктуру, используемую для поддержки сети поставщика, несет сам поставщик или другая организация, соблюдающая правила, меры и механизмы надзора, применимые к поставщику (например, поставщик третьей стороны, с которым у поставщика заключены договорные отношения). Если ответственность несет поставщик или другая организация, соблюдающая правила, эта ответственность должна предусматривать сохранение надзора за управлением этой инфраструктурой (включая контроль за деятельностью по управлению, персоналом, которому предоставлен доступ к управлению, и процессами управления).	3.56, 3.57, разделы 4 и 14
M5.05	Поставщики должны проводить анализ первопричины всех инцидентов, связанных с безопасностью. Результаты этого анализа должны быть переданы на соответствующий уровень, который может включать совет директоров поставщика услуг.	3.36
M6.01	Непостоянные учетные данные (например, имя пользователя и пароль для аутентификации) должны храниться в централизованной службе с соответствующим контролем доступа на основе ролей, которые должны обновляться в	3.44

	соответствии с любыми соответствующими изменениями ролей и обязанностей в организации.	
M6.02	Привилегированный доступ должен осуществляться через учетные записи с уникальным идентификатором пользователя и учетными данными аутентификации для каждого пользователя, и они не должны быть общими.	3.47
M6.04	Все учетные записи пользователей с привилегированным доступом в случае чрезвычайной ситуации должны иметь надежные уникальные учетные данные для каждого отдельного элемента сетевого оборудования.	3.48
M6.05	Учетные записи по умолчанию и жестко закодированные учетные записи должны быть отключены.	16.16
M8.05	Поставщики должны регистрировать все оборудование, развернутое в их сетях, и заблаговременно, не реже одного раза в год, оценивать свои риски, если сторонний поставщик не сможет продолжать поддержку этого оборудования.	16.16, 16.5
M8.06	Поставщики должны удалить или изменить пароли и учетные записи по умолчанию для всех устройств в сети и отключить незашифрованные протоколы управления. Если отключить незашифрованные протоколы управления невозможно, поставщики должны по возможности ограничить и минимизировать использование этих протоколов.	16.16 и 17.1
M8.07	Поставщики должны обеспечить, чтобы на всем сетевом оборудовании были активированы все журналы, относящиеся к безопасности, и отправлены в сетевые системы регистрации.	16.5
M8.08	Поставщики должны по возможности отдавать приоритет критическим исправлениям безопасности, а не обновлениям функциональности.	14.1 и 16.12
M8.12	Для SIM-карт с фиксированным профилем поставщик должен обеспечить надлежащую защиту конфиденциальных данных SIM-карт на протяжении всего их срока службы как со стороны поставщика SIM-карт, так и в сети оператора, учитывая риск для устойчивости сети и конфиденциальности в случае потери этой информации.	19.1
M8.13	Для SIM-карт с фиксированным профилем конфиденциальность, целостность и доступность конфиденциальных данных SIM-карты, передаваемых поставщику SIM-карты, должны быть защищены на каждом этапе их срока службы.	19.1
M10.04	В процессе управления инцидентами поставщика и его сторонних поставщиков должна обеспечиваться взаимная поддержка в разрешении инцидентов.	3.31-3.36

M10.06	Поставщик должен определить, какая информация будет доступна любому стороннему поставщику, гарантируя, что она является минимально необходимой для выполнения его функций. Поставщики должны установить контроль над этой информацией и ограничить доступ третьих сторон до минимума, необходимого для выполнения рабочих функций.	3.44
M10.09	Если сетевые или пользовательские данные выходят из-под контроля поставщика, он должен в соответствии с договором требовать и проверять, чтобы эти данные были надлежащим образом защищены. Сюда входит оценка средств контроля стороннего поставщика для обеспечения того, чтобы данные поставщика были видны или доступны только соответствующим сотрудникам и из соответствующих мест.	3.44–3.50 и разделы 14, 15, 17 и 18
M10.11	Поставщики должны на договорной основе обязать сторонних поставщиков уведомлять поставщика в течение 48 часов после того, как им стало известно о любых инцидентах безопасности, которые могли привести или привели к возникновению угрозы безопасности, или когда они выявили повышенный риск возникновения такой угрозы. Это касается, в частности, инцидентов в сети разработки поставщика или в его корпоративной сети.	3.33
M10.12	Поставщики должны на договорной основе требовать от сторонних поставщиков поддержки поставщика в расследовании инцидентов, которые привели к возникновению или способствовали возникновению нарушения безопасности в отношении основного поставщика, или повышенного риска возникновения такого нарушения.	3.31-3.36
M10.13	Поставщики должны на договорной основе требовать от сторонних поставщиков в течение 30 дней найти первопричину любого инцидента безопасности, который может привести к нарушению безопасности в Великобритании, сообщить о такой первопричине и устранить все обнаруженные нарушения безопасности.	3.35
M10.16	Поставщики должны на договорной основе требовать от сторонних поставщиков поддержки, насколько это уместно, любых аудитов, оценок или тестирования безопасности, необходимых поставщику в отношении безопасности собственной сети поставщика, включая те, которые необходимы для оценки требований безопасности в данном документе.	5.1-5.2, 6.1-6.3
M10.18	Поставщик сохраняет за собой право определять разрешения учетных записей, используемых для доступа к его сети администраторами третьих лиц.	16.23
M10.21	Поставщики должны иметь договорное право контролировать членов персонала администраторов третьих сторон, участвующих в предоставлении услуг администраторов третьих сторон, включая требование к	13.1

	администраторам третьих сторон обеспечить, чтобы любой член персонала больше не имел доступа к сети.	
M10.24	Поставщики должны на договорной основе требовать от администраторов третьей стороны внедрения технических средств контроля для предотвращения негативного влияния одного поставщика или его сети на любого другого поставщика или его сеть.	16.13
M10.25	Поставщики должны на договорной основе требовать, чтобы администраторы третьей стороны осуществляли логическое разделение в сети администратора третьей стороны для разделения данных и сетей заказчиков.	16.14
M10.26	Поставщики должны на договорной основе требовать, чтобы администраторы третьей стороны осуществляли разделение между средами управления администраторов третьей стороны, используемых для различных сетей поставщиков.	16.14
M10.27	Поставщики должны на договорной основе требовать, чтобы администраторы третьей стороны внедряли и применяли функции обеспечения безопасности на границе между сетью администратора третьей стороны и сетью поставщика.	16.14
M10.28	Поставщики должны на договорной основе требовать от администраторов третьей стороны внедрения технических средств контроля для ограничения возможности пользователей или систем негативно влиять на более чем одного поставщика.	16.14
M10.29	Поставщики должны на договорной основе требовать от администраторов третьей стороны внедрения логически независимых рабочих станций привилегированного доступа для каждого поставщика.	16.14
M10.30	Поставщики должны на договорной основе требовать, чтобы администраторы третьей стороны внедряли независимые административные домены и учетные записи для каждого поставщика.	16.14
M10.33	Поставщик должен на договорной основе потребовать от администратора третьей стороны осуществлять мониторинг и аудит действий персонала администратора третьей стороны при доступе к сети поставщика.	3.56, 3.57
M10.34	Поставщик должен на договорной основе требовать от администратора третьей стороны все журналы, относящиеся к безопасности сети администратора третьей стороны, в той степени, в которой эти журналы относятся к доступу в сеть поставщика.	3.56, 3.57 и 16.23
M10.35	Поставщики должны требовать, чтобы сети администраторов третьей стороны, которые могут повлиять на поставщика, проходили такой же уровень тестирования, который поставщик применяет к себе (например, периодическое	16.18

	тестирование TBEST, установленное для поставщика услуг Ofcom).	
M10.36	Поставщики должны на договорной основе требовать от поставщиков сетевого оборудования предоставить им декларацию безопасности о том, как они производят защищенное оборудование и обеспечивают его безопасность в течение всего срока службы. Рекомендуется, чтобы любая такая декларация охватывала все аспекты, описанные в оценке безопасности поставщика (VSA) (см. Приложение B), а поставщики должны поощрять своих поставщиков публиковать ответ на VSA.	16.15
M10.38	Поставщики должны обеспечить, в соответствии с контрактными договоренностями, чтобы декларация безопасности поставщика сетевого оборудования была подписана на соответствующем уровне управления.	16.15
M10.39	Если поставщик сетевого оборудования утверждает, что получил какие-либо международно признанные оценки или сертификаты безопасности своего оборудования (например, Common Criteria или NESAS), поставщики должны на договорной основе потребовать от поставщиков оборудования предоставить им полные результаты, подтверждающие эту оценку или сертификат.	16.17
M10.40	Поставщики должны на договорной основе требовать от поставщиков сетевого оборудования соблюдения стандарта не ниже, чем декларация безопасности поставщика сетевого оборудования.	16.16
M10.41	Поставщики должны на договорной основе требовать от поставщиков сетевого оборудования предоставления актуального руководства по безопасному развертыванию оборудования.	16.16
M10.42	Поставщики должны на договорной основе требовать от поставщиков сетевого оборудования поддержки всего оборудования и всех программных и аппаратных субкомпонентов в течение всего срока действия контракта. Период поддержки как аппаратного, так и программного обеспечения должен быть прописан в контракте.	16.16
M10.43	Поставщики должны на договорной основе требовать от поставщиков сетевого оборудования предоставления подробной информации (продукт и версия) об основных компонентах сторонних производителей и зависимостях, включая компоненты с открытым исходным кодом, а также срок и уровень поддержки.	16.16
M10.44	Если это относится к конкретному использованию оборудования поставщика, поставщики должны на договорной основе требовать от поставщиков третьей стороны устранения всех проблем безопасности, представляющих риск безопасности для сети или услуг	16.16

	поставщика, обнаруженных в их продуктах, в течение разумного времени после получения уведомления с регулярным информированием о ходе работ. Речь идет обо всех продуктах, на которые влияет уязвимость, а не только о продукте, в котором она была обнаружена.	
M10.46	Поставщики должны обеспечить, чтобы их контракты позволяли предоставлять информацию о проблемах безопасности, когда это необходимо, для поддержки идентификации и снижения рисков нарушения безопасности, возникающих в отношении сети электронных коммуникаций общего пользования или услуг электронных коммуникаций общего пользования в результате действий или бездействия сторонних поставщиков.	3.33 и 16.19
M10.47	Поставщики должны на договорной основе требовать от поставщиков сетевого оборудования поставлять критически важные исправления безопасности отдельно от функциональных обновлений, чтобы максимально ускорить развертывание исправлений.	14.1 и 16.12
M11.02	Любые постоянные учетные данные и секретные ключи (например, для доступа в случае чрезвычайной ситуации) должны быть защищены и недоступны никому, кроме ответственных лиц в случае чрезвычайной ситуации.	3.44
M11.03	Центральное хранилище для постоянных учетных данных должно быть защищено аппаратными средствами. Например, на физическом хосте диск может быть зашифрован с помощью TPM. Если для предоставления услуги централизованного хранения используется виртуальная машина (ВМ), эта ВМ и данные, содержащиеся в ней, также должны быть зашифрованы, использовать безопасную загрузку и быть настроены таким образом, чтобы обеспечить загрузку только в соответствующей среде. Это необходимо для того, чтобы исключить возможность изъятия данных из операционной среды и получения доступа к ним.	3.45
M16.12	Журналы сетевого оборудования, имеющего критически важные для безопасности функции, должны быть полностью записаны и доступны для аудита в течение 13 месяцев.	3.56, 3.57
M16.21	Признаки потенциальной аномальной активности должны быть оперативно оценены, расследованы и устранены.	3.56, 3.57
M21.02	Меры, которые должны быть приняты поставщиком услуг в соответствии с Регламентом 3(3)(f), обычно должны включать обеспечение, насколько это практически возможно, того, чтобы оборудование, выполняющее функции поставщика услуг по надзору за сетью, находилось в Великобритании и эксплуатировалось персоналом из Великобритании.	16.21
M21.03	Поставщик должен сохранить технический потенциал в Великобритании для обеспечения экспертной оценки работы	16.2, 16.20-16.22

	сетей поставщика в Великобритании и рисков для сетей поставщика в Великобритании.	
M21.04	Если данные хранятся за границей, поставщик услуг должен вести список мест, где хранятся данные. Риск, связанный с хранением данных в этих местах, включая любой риск, связанный с местным законодательством о защите данных, должен управляться в рамках процессов управления рисками поставщика услуг.	3.8