Public (Общедоступная)

ЗАЩИТА ИНФОРМАЦИИ "BT"

Наш стандарт контроля для третьих сторон

Редакция: 1.1 **Владелец:** Mark Tilston

В настоящем стандарте определены основные требования безопасности для третьих сторон, сотрудничающих с нашей компанией.

Он публикуется и доводится до сведения всех сотрудничающих сторон, а также будет являться собственностью и проверяться «Экспертом в конкретной предметной области» по крайней мере ежегодно, чтобы гарантировать его соответствие требованиям заинтересованных сторон и бизнес-целям, указанным в СМИБ компании "BT".

Это относится ко всем сторонним организациям, работающим на или от имени группы компаний " BT Group ", включая компании " Openreach", "EE" и " PlusNet ".

Для простоты в остальной части документа мы будем употреблять название "BT".

Если работа должна выполняться заинтересованной стороной "BT", такие требования будут выделены серым цветом.

Вводная часть

"ВТ" стремится обеспечить безопасные условия работы для своих заказчиков и сотрудников. Наша цель — защитить всю нашу информацию и системы от случайного или злонамеренного уничтожения, повреждения, изменения или разглашения. Это подтверждается тем, что мы реализуем эффективные меры по контролю третьих сторон для защиты конфиденциальности, целостности и надёжности нашей информации и систем.

Кого касается настоящий стандарт?

Данный стандарт касается третьих сторон, которые работают на или от имени компании "ВТ", а также получают доступ, обрабатывают, хранят или распространяют информацию и данные "ВТ". Этот стандарт может время от времени изменяться после проведения необходимых внутренних консультаций.

Определение терминов:

Термин	Значение
" Должен"	Это слово и слова «ТРЕБУЕТСЯ» или «ОБЯЗАН» указывают на абсолютное требование.
" Не Должен"	Эта фраза и фраза «НЕ МОЖЕТ» указывают на абсолютный запрет.
"может"	Это слово и прилагательное "НЕОБЯЗАТЕЛЬНЫЙ" указывают на то, что требование действительно необязательно.
" Следует"	Это слово и прилагательное «РЕКОМЕНДУЕМЫЙ» указывают на то, что в определённых ситуациях есть веская причина игнорировать конкретное требование, но перед Выбором другого решения нужно тщательно обдумать последствия.
" Не Следует"	Эта фраза и фраза «НЕ РЕКОМЕНДУЕТСЯ» указывают на то, что будут приложены все усилия для Выполнения конкретного требования, но не всегда и не во всех случаях возможно избежать описываемого действия. Если конкретная мера безопасности не может быть соблюдена, последствия будут оценены и полностью поняты.

Область применения

В этом документе описываются минимальные меры безопасности Высокого уровня в цепочке поставок третьей стороны для компании "ВТ".

Персонал "ВТ" может ознакомиться с сопутствующими стандартами, исходными данными, рабочими документами и указаниями по реализации мер безопасности, дополняющими этот стандарт, на веб-сайте по безопасности.

Заинтересованные стороны "ВТ", которым необходимы льготы для третьих сторон, которых касается этот стандарт, должны делать запрос, используя процедуру предоставления льгот

Что включено в этот документ?

1. Роли и обязанности

Каждая третья сторона должна знать и понимать настоящий стандарт и следить за тем, чтобы все лица, участвующие в предоставлении услуг "ВТ", Выполняли его соответствующие требования.

Заинтересованные стороны "ВТ" обязаны контролировать соблюдение настоящего стандарта и работать со своей третьей стороной для лучшего Выполнения требований и реализации мер по смягчению последствий в случае обнаружения проблем.

Руководители "ВТ" обязаны следить за тем, чтобы их сотрудники были знакомы и соблюдали требования настоящего стандарта, а также связанных с ним политик и стандартов.

2. Система контроля

2.1. Третья сторона должна иметь организованную и согласованную отраслевую структуру информационной и кибербезопасности, включающую следующие компоненты:

- соответствующие политики и процедуры информационной и кибербезопасности, утверждённые и доведённые до сведения сотрудников;
- стратегия информационной безопасности;
- соответствующие правоВые и нормативные требования информационной и кибербезопасности (включая конфиденциальность), которые понятны и Выполнимы;
- процессы контроля и управления рисками в сфере информационной и кибербезопасности.

2.2. 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, комиссия 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 чёткими полномочиями и обязанностями.

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

2.4. Третья сторона должна уведомлять (в письменном виде) "ВТ", как только на это появятся законные основания, о своём слиянии, приобретении или изменении формы собственности.

3. Управление инцидентами

3.1. 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;
- Отчёт об инцидентах в соответствии с установленными критериями;
- Понимание последствий инцидента;

- Судебная экспертиза своими силами или с помощью приглашённого специалиста;
- Эффективная практическая реализация уроков произошедших инцидентов;
- Обеспечение конфиденциальности информации об инцидентах, могущей нанести ущерб "ВТ".

3.2. Третья сторона должна назначить квалифицированных специалистов для обращения к ним в случаях угроз безопасности, для урегулирования инцидентов и контроля соблюдения соответствующих норм. Третья сторона должна сообщать заинтересованному лицу "ВТ" контактные данные ответственных лиц и о любых их изменениях. Контактные данные должны включать:
ФИО, обязанности, должность, рабочие адреса электронной почты и/или номера телефона.

3.3. Третья сторона должна в разумные сроки информировать заинтересованное лицо "ВТ" о любом ставшем ей известным инциденте, влияющем на обслуживание "ВТ" или её информацию, не позднее двенадцати (12) часов с момента получения информации об инциденте третьей стороной.

3.4. Третья сторона должна своевременно устранять риски, способствовать смягчению серьёзности и последствий инцидентов и уменьшению их продолжительности.

3.5. Третья сторона должна уведомлять заинтересованное лицо "ВТ" о любых инцидентах, влияющих на обслуживание "ВТ" или её информацию, с указанием, как минимум, следующих данных:

- дата и время,
- место,
- характер инцидента,
- последствия,
- классификация затронутой информации (см. Стандарт по классификации и обращению с информацией третьей стороной)
- текущее положение,
- результаты действий (включая любые рекомендации по разрешению проблемы или принятые меры).

3.6. Если для хранения и обработки информации "ВТ" привлекается четвёртая сторона, третья сторона должна получить разрешение и разъяснения от заинтересованного лица "ВТ" того, какую информацию можно предоставлять. Третья сторона должна установить договорные отношения с четвёртой стороной и гарантировать, что та располагает стандартной отраслевой системой безопасности.

4. Управление изменениями

4.1. Третья сторона должна обеспечить согласование, регистрацию и тестирование всех изменений IT, отбракоВывание неудачных с целью предотвращения сбоев в обслуживании и нарушений безопасности, а также управляемую процедуру экстренных обновлений.

4.2. Третья сторона должна обеспечить отражение изменений в производстве и при аварийном восстановлении.

4.3. Третья сторона должна немедленно уведомлять "ВТ" о любых существенных изменениях в обслуживании, и среди всего прочего, изменениях доступа через брандмауэры, включая

трансляцию сетеВых адресов.

4.4. Третья сторона должна обеспечить Выполнение и регистрацию технического обслуживания и ремонта ресурсов организации с использованием согласованных и управляемых инструментов.

4.5. Третья сторона должна обеспечить согласование, регистрацию и Выполнение дистанционного обслуживание ресурсов организации без риска несанкционированного доступа.

5. Управление киберрисками и киберугрозами

5.1. Третья сторона должна обеспечить наличие постоянной системы оценки рисков и угроз, гарантирующей, что кибербезопасность подразделений, ресурсов и территорий организации и её сотрудников понимается и контролируется посредством:

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

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

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

6. Управление идентификационными данными и контроль доступа

6.1 Третья сторона должна иметь организованную и согласованную систему безопасного управления идентификационными и регистрационными данными уполномоченным персоналом:

- Предоставление, повторное предоставление, изменение и лишение прав доступа только на основе документированных и санкционированных разрешений.
- Блокировка неактивных учётных записей.
- Отключение учётных записей уволенного/уволившегося персонала.
- Периодическая проверка доступа на предмет соответствия цели.
- Для учётных записей пользователей предусмотрена возможность повторной сертификации по крайней мере раз в год, а для привилегированных учётных записей - ежеквартально.

6.2 Третья сторона должна обеспечить управление удалённым 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 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 вашей политике информационной безопасности.

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

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

6.4 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.

6.5 Третья сторона должна гарантировать всю аутентификацию соразмерно с рискованностью транзакций, то есть с использованием пароля соответствующей длины и сложности, разной частоты смены паролей, многофакторной аутентификации, безопасного управления регистрационными данными или других средств.

6.6 Должны быть предусмотрены необходимые средства контроля неудачных аутентификаций, включая всплывающие уведомления, журнал сбоев и блокировку пользователей.

6.7 Должны быть предусмотрены процессы и средства для управления и авторизации гостеВых и служебных учётных записей.

7. Управление информационными активами

7.1. Третья сторона должна иметь перечень информационных активов, при необходимости включающий любое оборудование "ВТ", размещённое в помещениях третьей стороны) и обеспечивать ежегодное проведение не менее одной проверки этого перечня на предмет актуальности, полноты и точности.

7.2. Третья сторона должна внести в перечень 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 "ВТ" или клиентов "ВТ".

8. Доступ к системам "ВТ".

8.1 Третья сторона обязана соблюдать все предоставленные ей инструкции доступа и использования систем "ВТ".

8.2 Третья сторона обязана в течение 24 часов уведомить "ВТ" об отпавшей необходимости доступа для её работника.

8.3 Третья сторона должна гарантировать использование идентификационных данных пользователя, паролей, PIN-кодов, токенов и доступа к конференциям только своим персоналом. Данные доступа должны храниться безопасно и отдельно от используемого устройства. Если пароль становится известным посторонним людям, он должен быть немедленно изменён.

Межсистемные соединения

8.4 Междоменное соединение с системами "ВТ" недопустимо без специального согласования и разрешения "ВТ".

8.5 Третья сторона должна принимать все необходимые меры против попадания вирусов и вредоносных кодов (в смысле, определяемом компьютерной терминологией) в системы "ВТ".

8.6 Системы третьей стороны должны подключаться к системам "ВТ" через защищённые каналы, данные должны защищаться шифрованием согласно требованиям **раздела 11 «Криптография»**.

8.7 Третья сторона обязана использовать системы и инфраструктуры в Выделенной логической сети. Такая сеть должна состоять только из систем, образующих защищённый комплекс обработки данных клиентов.

9. Физическая безопасность в помещениях 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 "ВТ". Метод доступа должен включать один или более из следующих элементов:

- Действительная идентификационная карточка работника третьей стороны с чётко распознаваемой и узнаваемой фотографией.
- Действительная электронная карта доступа в соответствующие помещения.
- Клавишная система защищённого доступа с возможностью авторизации, простых и целеВых изменений кода (по крайней мере ежемесячно).
- Биометрическое распознавание.

9.2 Третья сторона должна иметь методики и процедуры контроля и мониторинга посетителей, включая работников третьей стороны с правом доступа в режимные зоны, а также работников служб экологии, систем сигнализации и уборщиков помещений.

9.3 Режимные зоны третьей стороны, используемые для обеспечения услуг (например, помещения для сетевой передачи данных), должны отделяться от общих территорий 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 скрытого видеонаблюдения в местах хранения и обработки информации "ВТ".

9.5 Записи CCTV-камер должны храниться не менее 20 дней. Однако этот период может быть продлён в следующих ситуациях:

- Необходимость видео доказательства при расследовании инцидента или уголовного дела; или
- Требование законодательства.

9.6 Все записи CCTV-камер и записывающие устройства должны размещаться в защищённых местах во избежание изменения, удаления или «случайного» просмотра видеоматериалов, при этом доступ к записям должен контролироваться и ограничиваться только уполномоченными лицами.

9.7 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);
- Содержать контрольное оборудование, в частности, системы кондиционирования воздуха и обнаружения протекания воды;
- Предотвращение повреждения водой, размещение ёмкостей для воды, труб и т.д. вне помещений.

9.8 Третья сторона должна обеспечивать физический доступ в зоны хранения информации "ВТ" с помощью смарт-карт или бесконтактных карт (а также равноценных или более совершенных систем безопасности). Третья сторона также должна проводить ежемесячные проверки, гарантирующие доступ только уполномоченным лицам.

9.9 Третья сторона должна препятствовать фотографированию и захвату изображения любой информации "ВТ". При необходимости в захвате таких изображений следует получить письменное разрешение у заинтересованного лица "ВТ".

Предоставление помещений для размещения оборудования "ВТ"

9.10 Там, где на территории третьей стороны безопасно размещено оборудование "ВТ" или клиентов "ВТ", третья сторона должна:

- Предоставить "ВТ" план этажа с Выделенным местом в безопасной зоне.
- Гарантировать, что системные блоки "ВТ" и клиентов "ВТ" в помещениях заперты и доступны только уполномоченным работникам и представителям "ВТ" и третьей стороны.
- Внедрить безопасный процесс управления ключами.

9.11 "ВТ" предоставляет третьей стороне:

- Перечень физических активов "ВТ" и клиентов "ВТ", находящихся в помещениях третьей стороны;
- Сведения о сотрудниках, субподрядчиках и агентах "ВТ", которым необходим доступ в помещения третьей стороны (на постоянной основе).

10.Классификация и защита данных

10.1 Третья стороны должна иметь организованную и согласованную систему классификации и обработки информации (в соответствии с добросовестной отраслевой практикой/требованиями "ВТ"), которые предусматривают следующее:

- Указания по обработке информации;
- Защиту информации в зависимости от уровня конфиденциальности;
- Знание сотрудниками того, что информация "ВТ" должна использоваться только для тех целей, для которых она была предоставлена;
- Обработку информации "ВТ" в соответствии со Стандартом по классификации и обращению с информацией для третьих сторон.

11. Криптография

11.1 Третья сторона должна гарантировать, что там, где уровень риска требует шифрования, данные должным образом зашифрованы (при передаче и хранении), а при использовании криптографических ключей — что такие ключи разработаны и реализованы согласно требованиям безопасности по стандарту NIST FIPS 140 -2 для уровня 2 или Выше.

11.2 Длина криптографических ключей должна соответствовать или преВышать следующие значения:

- Симметричные ключи (например, AES) должны иметь длину не менее 256 бит.
- Асимметричные ключи (например, RSA) должны иметь длину не менее 2048 бит.
- Ключи эллиптической кривой должны иметь длину не менее 224 бит.

11.3 После объявления NIST о том, что криптоалгоритм больше не безопасен, его нельзя использовать для новых развертываний. Для существующих развернутых систем необходимо пересмотреть дальнейшее использование устаревших криптоалгоритмов и предложить план перехода от устаревших криптоалгоритмов к чему-то более безопасному.

11.4 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.

11.5 Для защиты хранимых данных, то есть паролей, необходимо использовать "солёное" 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.

11.6 Управление ключами — создание и использование

- Ключи сеанса и случайные числа должны создаваться с использованием безопасного генератора псевдослучайных чисел. Они должны быть заполнены, по крайней мере,

таким количеством битов энтропии или неожиданности сообщения, которое соответствует количеству эффективных битов безопасности, обеспечиваемых алгоритмом, который будет использовать ключ.

- Использование более короткого ключа из 64 бит и комбинирование некриптографическим способом с одним и тем же ключом из 64 битов для получения 128 бит запрещено.
- В алгоритме должны быть задействованы все биты ключа.
- Дополнение пробелами или другие биты, используемые алгоритмом, не должны учитываться при расчете длины ключа.

11.7 Управление ключами — степень случайности

- При создании сеансовых ключей в симметричных частях гибридной криптографии или для создания "солей" или векторов инициализации должен применяться надёжный источник случайных данных.
- Можно использовать генераторы псевдослучайных чисел (PRNG), но для того, чтобы считаться защищённым, PRNG не должен позволять злоумышленнику:
  - Угадывать будущий результат генератора, если известен предыдущий результат;
  - Рассчитать предыдущие состояния генератора, если известно его текущее состояние;
  - Отличать псевдослучайные числа от по-настоящему случайных. (Использование случайных чисел () не допускается).

11.8 Управление ключами — обмен ключами

- Обмен сеансовыми ключами, сгенерированными для использования с симметричным алгоритмом, должен осуществляться с использованием протокола безопасного обмена ключами.

11.9 Управление ключами — хранение ключей

- Если ключи используются для защиты хранимых данных, ключ шифрования данных (DEK) должен быть защищён с использованием ключа шифрования ключей (KEK), который должен храниться на отдельном сервере или в доверенном платформенном модуле (TPM).
- Если KEK хранится на отдельном сервере, он должен быть защищён при передаче на сервер хранения данных.

11.10 Управление ключами — Ротация (регенерация) ключей

- Должна быть возможность регенерации ключа в соответствии с передовой отраслевой практикой в течение срока его службы.
- Должна быть возможность повторного шифрования данных, защищаемых с помощью регенерированного ключа.
- Должна быть возможность специальной регенерации ключа и повторного шифрования данных при подозрении, что исходный ключ шифрования был взломан.
- Для AES GCM вероятность того, что функция аутентифицированного шифрования когда-либо будет активироваться с одним и тем же IV и одним и тем же ключом для двух (или более) различных наборов входных данных, не должна превышать 232.

11.11 Управление ключами — аппаратные модули безопасности (HSM)

- Криптографические ключи должны загружаться в HSM с помощью смарт-карт.
- Для доступа к смарт-картам должен использоваться PIN-код.
- PIN-коды должны Выбираться в соответствии с политикой контроля доступа.

- PIN-коды и смарт-карты должны храниться в сейфе, проверенном службой информационной безопасности.
- Должна быть исключена возможность извлечения криптографических ключей из HSM.
- Необходимо обеспечить уничтожение криптографических ключей при попытке вскрытия корпуса аппаратного модуля безопасности.
- Для HSM с ключами Высокого уровня конфиденциальности защитные PIN-коды и смарт-карты должны конфигурироваться и храниться только сотрудниками службы технической безопасности.
- Там, где HSM будут использоваться для защиты Высококонфиденциальных данных, при внесении изменений в HSM необходимо предусмотреть использование 2 смарт-карт (кворум) и связанных с ними PIN-кодов. Элементы кворума должны проверяться с особой тщательностью.

11.12 ЦифроВые сертификаты

- Для сертификатов должен быть установлен атрибут "Точка распространения списка отзыва сертификатов" (CDP).
- Для определения статуса сертификата должен использоваться онлайноВый протокол статуса сертификата (OCSP) или список отзыва сертификатов (CRL).
- Владельцы сертификатов должны отслеживать их действительность и срок действия во избежание системных сбоев при их истечении.
- Потребители сертификатов (клиенты) должны отслеживать их действительность и срок действия во избежание системных сбоев при их истечении.
- Срок действия сертификата должен соответствовать его назначению.
- Срок действия сертификата должен устанавливаться до его Выдачи.
- Использование стандартной идентификационной информации (клиент, сервер) 1024 не допускается.

11.13 Транзит данных

- Шифрование данных при транзите обычно Выполняется с использованием транспортного или транзитного шифрования (сообщения или Выборочного поля). Механизмы транспортного шифрования, включают, в частности:
- Безопасность на транспортном уровне (TLS);
- Безопасное туннелирование (IPSec);
- Протокол безопасной оболочки (SSH).
- Для транспортного шифрования симметричный компонент должен соответствовать разделу 12.14 настоящего стандарта.
- Транспортные протоколы безопасности должны быть настроены для предотвращения взаимодействия более слабых алгоритмов и/или более коротких ключей, когда обе конечные точки поддерживают более безопасный вариант.
- Протокол SSL не должен использоваться ввиду нескольких известных уязвимостей.
- Векторы инициализации для поточного шифрования и AES в режиме CBC не должны быть предсказуемыми.
- IV / случайное число в AES GCM должны соответствовать следующим требованиям «уникальности»:
  - Соблюдение этих требований имеет решающее значение для безопасности GCM.
  - Транспортные протоколы безопасности должны быть сконфигурированы (например, с использованием разрядов направления) для предотвращения атак на основе открытых текстов, основанных на возвращаемых известных сообщениях типа "никаких изменений".
  - При настройке транзита должна Выполняться взаимная проверка подлинности.

- Для конфиденциальных коротких данных, требующих использования транзитного шифрования (ключи шифрования, пароли, данные платёжной карты), используйте асимметричное шифрование. При этом минимальная длина ключей и алгоритмы должны соответствовать описанным в настоящем документе.
- При транзите данных управления системой они должны быть зашифрованы.
- Не допускаются следующие варианты TLS: TLS версия 1.0, TLS версия 1.2, версия 6.0, TLS версия 6.1 и SSL (все версии).
- Не допускаются следующие варианты SSH (SFTP): SSH версия 1.
- Не допускаются следующие варианты IPSec: IKE версия 1.

11.14 Данные "в местах хранения"

- Данные в "местах хранения" включают данные, хранящиеся в файлах (временных, файлах подкачки и т.д.), базах данных и на любом устройстве, в частности, ПК, ноутбуках и других портативных устройствах, серверах, магнитных лентах, SAN, USB, CD, DVD, дискетах и других съёмных носителях.
- Конфиденциальные или более секретные данные, хранимые в энергонезависимой памяти на любом устройстве, должны зашифроваться.
- Информация о платёжных картах на любом устройстве в энергонезависимой памяти должна зашифроваться.
- Если данные симметричного ключа защищены асимметричным ключом, асимметричный ключ должен обеспечивать равную надёжность, измеряемую в битах защиты симметричного ключа.
- Системная документация должна содержать классификацию данных и указание их объёма в системе.
- Ключи дешифрования не должны храниться или резервироваться с данными, для дешифровки которых они используются. Программное обеспечение должно быть полностью протестировано перед развёртыванием в производственных системах.

12. Предотвращение утечки данных

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

- Электронную почту,
- Интернет-шлюзы (включая хранилища данных постоянной готовности и веб-почту),
- USB, оптические и другие типы портов/ портативных устройств хранения и т.д.,
- Мобильные компьютерные среды и BYOD,
- Службы удалённого доступа,
- Средства совместного использования файлов и социальные сети.

ОБРАТИТЕ ОСОБОЕ ВНИМАНИЕ! Съёмные носители/ портативные устройства должны быть по умолчанию отключены и включаться только для законных служебных целей. Любые данные на съёмных носителях и переносных устройствах должны шифроваться соразмерно риску. Использование несанкционированных устройств для подключения к сети (корпоративной сети поставщика или системам/ сетям "BT") или доступа к закрытой информации не допускается. Более подробная информация по работе со съёмными носителями приведена в Стандарте по классификации и обработке информации третьими сторонами .

13. PCI DSS

13.1 Третья сторона, работающая с данными платёжных карт, должна соответствовать требованиям PCI-DSS.

14.Облачные / сетеВые Вычисления

14.1. 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.

14.2. В соглашениях об инфраструктурном и сетевом обслуживании (внутреннем и стороннем) должны чётко указываться меры безопасности, объём и уровни обслуживания, а также требования бизнеса или клиента.

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

15. Социальные сети

15.1. Третья сторона должна иметь организованную и согласованную систему пригодную для частных и корпоративных социальных сетей со следующими возможностями:

- Препятствование публикации сотрудниками клеветнических, непристойных или оскорбительных материалов об организации, её клиентах или заказчиках;
- Препятствование использованию логотипов организации или клиента без предварительного разрешения;
- Препятствование разглашению конфиденциальной информации организации или клиента без предварительного согласия;
- Препятствование публикации комментариев о компании, её клиентах или заказчиках, которые могут быть обоснованно истолкованы как официальное мнение организации или её клиентов;
- Препятствование разглашению информации "ВТ", помеченной как «Конфиденциальная» или «Строго конфиденциальная».

16.Конфигурация систем

16.1. Третья сторона должна иметь организованную и согласованную инфраструктуру для конфигурации систем (как третьей стороны, так и систем, предоставляемых "ВТ"), обеспечивающую следующее:

- Конфигурацию систем и сетеВых устройств для безопасной работы (по принципу наименьшей функциональности и отсутствия несанкционированного программного обеспечения);
- Правильную и стабильную установку времени на устройствах;
- Отсутствие вредоносного программного обеспечения в системах;
- Проверку и мониторинг целостности сборок/ устройств.

17. Разработка безопасного программного обеспечения

17.1. 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 разработках для производственной и непроизводственной сфер.

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

- Системы создаются с использованием передоВых методов разработки безопасного ПО (например, OWASP (проект по обеспечению безопасности открытых веб-приложений).
- Код хранится надёжно и проходит проверку качества.
- После тестирования и внедрения код надёжно защищён от несанкционированного изменения.

17.3. Если для защиты всех сторон требуется условное депонирование, у первой или третьей стороны (по соображениям 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 полнения условий возврата.
- Разумные условия возврата.
- Постоянные обновления, разумные тарифы и возможность пересмотра договора условного депонирования.

18. Защита от вредоносных программ

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

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

19. Управление уязвимостью

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

- Политики и процедуры процессов;
- Чётко определенные роли и обязанности;
- Необходимые инструменты, такие как системы обнаружения вторжений и системы сканирования на предмет уязвимостей;

19.2. 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.

19.3. 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 к использованию и допуску только утверждённых инструментов, технологий и пользователей.
- Минимизация или документирование Выявленных уязвимостей как общепринятых рисков.

19.4. Третья сторона должна обеспечивать своевременную установку последних патчей безопасности для систем/ активов/ сетей/ приложений и должна гарантировать что:

- Третья сторона использует патчи, полученные от поставщиков непосредственно для конкретных систем, и патчи, 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 патчи получены от авторитетной организации технической поддержки программного обеспечения с открытым исходным кодом.
- Третья сторона тестирует все патчи в системах с конфигурацией, аналогичной конфигурации целеВых производственных систем, перед их установкой в производственных системах, и каждый установленный патч проверяется на предмет корректной работы.
- Предупреждения об уязвимостях отслеживаются у всех поставщиков и во всех источниках информации.
- В случае невозможности установки патчей применяются необходимые меры реагирования.

19.5. Третья сторона должна обеспечить, по крайней мере, ежегодную независимую оценку ИТ-безопасности/ тест на проникновение для ИТ-инфраструктуры и приложений третьей стороны, используемых для предоставления услуг, включая узлы аварийного восстановления, для Выявления уязвимостей, которые могут быть использованы для взлома данных/ служб. Кроме того, должна быть предусмотрена защита от любых нарушений системы безопасности посредством кибер-атак. Третья сторона должна по мотивированному требованию "ВТ" предоставлять ей доступ к отчётам по тестам на проникновение, относящимся к предоставляемым услугам.

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

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

19.8. Третья сторона должна гарантировать, что серверы, используемые для предоставления услуг, не развернуты в ненадёжных сетях (пределами периметра безопасности, вне административного контроля, например, подключённые к Интернету) без соответствующих мер безопасности.

20.Целостность сетей

20.1. Третья сторона должна гарантировать, что целостность сети сохраняется и поддерживается следующими действиями:

- 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 защищён протоколами авторизации, аутентификации, сегментации и шифрования для предотвращения нарушений безопасности.
- Используются защищённые 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 надёжная 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 учётные записи.
- Исключены доверительные отношения между серверами.
- Для Выполнения операций используется передовой принцип безопасности «наименьшие привилегии».
- Принимаются надлежащие меры для обнаружения и/ или защиты от вторжений.
- 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.

20.2. 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 сети(-ям) третьей стороны.
- Прилагать все усилия для снижения риска неправомерного использования сети(ей)

третьей стороны лицами, имеющим доступ к ней.

- Прилагать все усилия для Выявления любых нарушений безопасности и обеспечения быстрого устранения любых нарушений наряду с идентификацией лиц, которые получили доступ к сети, и определением того, как они его получили.

21.Защита от атак типа «отказ в обслуживании»

21.1. Третья сторона должна обеспечить защиту ключеВых систем от простых (DoS) и распределённых (DDoS) атак типа «отказ в обслуживании».

22.Непрерывная регистрация и контроль безопасности

22.1. 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, 12 месяцев. Третья сторона должна гарантировать, что журналы (если необходимо) содержат информацию о следующих событиях:

- Точки запуска и остановки зарегистрированного процесса;
- Изменения типа регистрируемых событий в соответствии с требованиями контрольного журнала (например, параметры запуска и любые их изменения);
- Запуски и Выключения системы;
- Успешные входы в систему;
- Неудачные попытки входа в систему (например, ввод неверного идентификатора пользователя или пароля);
- Создание, изменение и удаление учётных записей пользователей;
- АктиВы, к которым получал доступ пользователь (например, к данным);
- Место, откуда пользователь получал доступ к активам (например, IP-адрес);
- Время (например, метка времени).

22.2. Система аудита и управления журналами должна включать следующее:

- Проверки журналов ключеВых событий независимой стороной, по крайней мере ежемесячно, для Выявления любых несанкционированных действий, а также целей и методов атак.
- Регистрацию и расследование особых ситуаций до их разрешения.
- Сбор и сопоставление журналов из нескольких источников и датчиков, а также их надёжное хранение и защита от несанкционированного доступа для восстановления событий.
- Воздействие любых событий определяется с помощью установленных порогоВых значений для оповещения об инциденте и своевременного реагирования, зависящего от критичности аварийного сигнала.

23. Обучение и информирование

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

- Привилегированные пользователи,
- заинтересованные лица третьей стороны (например, субподрядчики, заказчики, партнёры),
- Руководители Высшего звена,
- Персонал, обеспечивающий физическую безопасность и кибербезопасность.

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

24.Право проверки

24.1. Третья сторона должна предоставлять "ВТ" возможность проверки средств контроля в местах их разработки или предоставления услуг, а также тестирования и оценки систем безопасности не реже раза в год (или сразу после инцидента).

24.2. Все расходы по устранению слабых мест системы, Выявленных "ВТ", несёт третья сторона, которая должна устранять их в течение срока, согласованного обеими сторонами.

24.3. В случае серьёзного инцидента третья сторона обязуется полностью сотрудничать в любом расследовании "ВТ", любого регулирующего органа или правоохранительного органа, предоставляя по мере необходимости доступ и помощь для расследования инцидента. "ВТ" может запросить у третьей стороны изолировать любой её в целях расследования, а третья сторона не должна необоснованно отклонять такой запрос или медлить с его Выполнением.

25.Физическая безопасность — помещения "ВТ"

25.1 Весь персонал третьей стороны, работающий в помещениях "ВТ", должен иметь при себе и сразу же предъявлять идентификационную карточку, предоставленную третьей стороной или "ВТ", с фотографией, позволяющей чётко идентифицировать личность работника. "ВТ" 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.

25.2 При наличии у работника третьей стороны карты доступа, Выданной "ВТ", необходимость в которой отпадает, третья сторона должна незамедлительно или не позднее 5 рабочих дней уведомить о этом "ВТ".

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

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

25.5 Если третьей стороне разрешено предоставлять своему персоналу самостоятельный доступ в помещения "ВТ", уполномоченный представитель третьей стороны и её персонал должны

соблюдать требования документа Доступ поставщика на объекты "ВТ" — обязательное руководство по безопасности

Кроме того, уполномоченный представитель третьей стороны и её персонал должны пройти обязательную проверку перед приёмом на работу уровня L2.

26. Сетевая безопасность — собственная сеть "ВТ"

26.1 Третья сторона должна предоставить представителю службы безопасности "ВТ" имена, адреса (и другие данные по требованию "ВТ") всего персонала третьей стороны, который будет непосредственно участвовать в развёртывании, обслуживании и/ или управлении, перед тем, как этот персонал начнет осуществлять развёртывание, обслуживание и/ или управление.

26.2 Что касается деятельности в Великобритании, третья сторона должна предоставить группу специалистов по безопасности, включающую минимум одного гражданина Великобритании, которая будет доступна для связи с представителем службы безопасности "ВТ" (или кандидатами, Выдвинутыми на эту должность). Кроме того, эта группа должна присутствовать на собраниях, время от времени назначаемых представителем службы безопасности "ВТ".

26.3 Третья сторона должна предоставлять представителю службы безопасности "ВТ" перечень (обновляемый по мере необходимости) всех активных компонентов сервиса и/или сервисов и их поставщиков.

26.4 Третья сторона должна предоставлять сведения о своём персонале, который будет поддерживать связь с командой управления уязвимостью "ВТ" (CERT) по вопросам уязвимостей, Выявленных "ВТ" и третьей стороной в сервисе и/или сервисах. Третья сторона должна своевременно предоставлять "ВТ" информацию об уязвимостях и Выполнять (за свой счёт) такие обоснованные требования в отношении уязвимостей, о которых может время от времени сообщать представитель службы безопасности "ВТ". Третья сторона обязана сообщать "ВТ" о любых уязвимостях в срок достаточный для применения мер контроля и минимизации до публичного заявления третьей стороной о таких уязвимостях.

26.5 Третья сторона обязуется добиваться того, чтобы любые услуги безопасности, периодически оказываемые "ВТ" или для "ВТ" и Выполняемые за счёт третьей стороны, положительно оценивались независимыми экспертами.

26.6 Третья сторона обязуется незамедлительно и в любом случае в течение 7 рабочих дней предоставлять представителю службы безопасности "ВТ" полную информацию о любых функциях и/или функциональных возможностях любого сервиса (существующих или запланированных), о которых она периодически узнаёт,

- или
- которые представитель службы безопасности "ВТ" обоснованно считает (и об этом уведомляет третью сторону) предназначенными или возможными к использованию для законного перехвата или любого другого перехвата телекоммуникационного трафика. Информация должна быть максимально подробной, чтобы представитель службы безопасности "ВТ" мог полностью понять суть, состав и объём таких функций и/или функциональных возможностей.

26.7 Для обеспечения доступа к сетям и/или системам "ВТ" третья сторона должна немедленно уведомлять "ВТ" о любых изменениях метода доступа через брандмауэры, включая предоставление данных о трансляции сетеВых адресов.

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

26.9 Третья сторона должна гарантировать, что функции IPv6, интегрированные в операционные системы, отключены на хостах (например, устройствах или серверах конечных пользователей), которые подключаются к сети "BT", и отключены домены (там, где они не нужны).

26.10 Персонал третьей стороны, занимающийся построением, разработкой или поддержкой сетей или сетеВых активов "BT", должен пройти обязательную проверку перед приёмом на работу уровня L2. Проверки перед приёмом на работу уровня L3 необходимы для должностей, определённых представителем службы безопасности "BT". Если у третьей стороны нет собственных возможностей организации допуска персонала уровня L3, "BT" поможет получить его за счёт третьей стороны.

26.11 Третья сторона обязуется осуществлять техническое обслуживание аппаратного и программного обеспечения в соответствии со спецификациями производителей.

26.12 Третья сторона не должна использовать съёмные носители (диски, USB-накопители и т.д.), предназначенные для поддержки и обслуживания, в любых других целях.

27. Глоссарий

Термин	Определение
Двухфакторная аутентификация	Двухфакторная аутентификация или двухэтапная верификация — это процесс обеспечения безопасности, в котором пользователь использует два разных фактора аутентификации для проверки, чтобы лучше защитить как свои учётные данные, так и ресурсы, к которым он может получить доступ.
Третья сторона	Лица, Выполняющие для "BT" работу, но не являющиеся её сотрудниками.
AES	Улучшенный стандарт шифрования (AES) — это спецификация для шифрования электронных данных, созданная Национальным институтом стандартов и технологий США (NIST) в 2001 году.
ASG	Группа поддержки приложений.
BT Group ("BT Груп")	Под BT Group подразумеваются все подразделения в её составе, включая, помимо прочих, Openreach, EE и Plusnet. В данном документе они будут называться BT("BT"), если не указано иное.
заинтересованное лицо "BT"	Сотрудник "BT", который несёт ответственность за работу, Выполняемую третьей стороной.
CCTV	Замкнутая система видеонаблюдения
Администрирование баз данных	Администратор базы данных
DC	Центр данных (информационный центр)
Защита в глубину	Это подход к кибербезопасности, при котором защитные механизмы наслоены друг на друга для защиты ценных данных и информации. При обходе одного защитного механизма для отражения атаки немедленно активируется другой.
DR	Восстановление после отказа
GCM	Счётчик с аутентификацией Галуа — режим работы для криптографических блочных шифров с симметричным ключом, который получил широкое распространение благодаря своей эффективности.
HDD	Жесткий диск
HMG	Правительство Её Величества — правительственные органы в Великобритании
ISMS	Система менеджмента информационной безопасности Это система политик и процедур, которая включает в себя все юридические, физические и технические средства контроля, задействованные в процессе управления информационными рисками организации.

ISO 27001	Отраслевой стандарт для системы менеджмента информационной безопасности (ISMS).
ISO 27017	Свод практических правил контроля информационной безопасности на основе ISO/IEC 27002 для облачных сервисов.
ISO 7816	Международный стандарт, касающийся электронных идентификационных карт с контактами, особенно смарт-карт. Совместно контролируется Международной организацией по стандартизации (ISO) и Международной электротехнической комиссией (IEC).
NAS	Единое устройство хранения, которое работает с файлами данных.
NIST	Национальный институт стандартов и технологий, является лабораторией физических наук и ненормативным органом Министерства торговли США.
PCI DSS	Стандарт защиты информации в индустрии платёжных карт (PCI DSS) — это стандарт информационной безопасности для организаций, которые работают с фирменными кредитными картами основных платёжных систем.
Privileged Accounts - Привилегированные учётные записи	Привилегированный пользователь - это пользователь, имеющий административный доступ к критическим системам.
RSA	(Алгоритм Ривеста-Шамира-Эдльмана) является одной из перВых криптосистем с открытым ключом и широко используется для безопасной передачи данных.
SAN	Локальная сеть из нескольких устройств, которые работают с использованием дискоВых блоков.
SSD	Твердотельный накопитель

28.Журнал изменений

Версия №	Дата	Автор изменения	Краткое описание изменения
0.1	30.10.2017	Mark Tilston	Первоначальная версия для определения общей структуры и обновления содержания
0.2	10.04.2019	Tim Hunt	Преобразование в ноВый формат
1.0	01.05.2019	Ian Morton	Подготовлено к Выпуску
1.1	01.10.2019	Karen Tanner	Добавление дополнительных мер контроля в рамках расширения требований "BT" к безопасности

29.Утверждение документа

Должность	Дата
Mark Tilston	06.11.2019

30.Соответствие требованиям стандарта

Мы ценим профессионализм большинства сотрудников "BT" и их приверженность ценностям "BT",

но в случае неВыполнения требований настоящего стандарта "BT" может принять дисциплинарные меры в зависимости от требований местного законодательства и нормативных актов.

При неВыполнении требований этого стандарта сторонними организациями мы можем расторгнуть с ними договор на предоставление услуг.

31.Полезные ссылки и информация

Для персонала "BT":

Здесь можно ознакомиться со всеми политиками и стандартами "BT" .

Мы пересматриваем нашу политику и стандарт не реже одного раза в год. Ознакомиться с программой пересмотра можно здесь.

Чтобы сообщить об инциденте, связанном с нарушением безопасности, отправьте электронное письмо в Центр контроля за безопасностью

Если вам нужна дополнительная информация/рекомендации по этому стандарту или любой другой политике/стандарту безопасности, отправьте электронное письмо на адрес security.policy@bt.com

Для третьих сторон:

Здесь можно ознакомиться со всеми применимыми стандартами и другими документами по безопасности.

32. Право собственности и конфиденциальность

Этот документ не должен передаваться третьим лицам без письменного согласия "BT". Настоящий стандарт и любая связанная с ним документация остаются собственностью "BT" и должны быть возвращены по запросу.

Этот документ относится к категории «Для служебного пользования», однако если он скачивается третьей стороной, он должен рассматриваться как «Конфиденциальный».