

Приложение 1 - "Классификация информации"

Введение

В ВТ все данные и информация имеют ответственного за бизнес ВТ, который отвечает за классификацию документов или данных.

Данные и информация должны защищаться всеми пользователями, которые имеют с ними дело. Будучи пользователем Информации ВТ, вы несете ответственность за выполнение требований, предусмотренных средствами контроля классификации безопасности согласно настоящему документу, а также любыми конкретными требованиями проектов, которые определит ВТ. Вы должны использовать документ или данные исключительно по их предназначению и получить разрешение от ответственного за данные, если вы хотите предоставить доступ к ним дополнительным лицам.

Если вы получили Информацию ВТ, которая не классифицирована, вам необходимо обратиться к отправителю или своему руководителю ВТ для подтверждения классификации; в противном случае обратитесь в Службу безопасности ВТ в соответствии с Приложением 3 к Требованиям безопасности.

Примечание. Если у вас имеется доступ к локальной сети ВТ Greenside, или если вы обязаны создавать для ВТ документы, которые включают любую Информацию ВТ, вам необходимо обратиться к [Политике безопасности 4](#), в противном случае применяются следующие положения

Классификация информации

Существуют 4 класса информации:

- Общедоступная
- Для внутреннего пользования
- Конфиденциальная
- Строго конфиденциальная

Общедоступная

Общедоступная информация не требует контроля или предназначена для использования неограниченным кругом лиц.

Для внутреннего пользования

Информация для внутреннего пользования доступна сотрудникам ВТ и иным лицам, у которых имеется доступ к информационной сети ВТ, причем в случаях, когда такой доступ связан с незначительным коммерческим риском для ВТ.

Конфиденциальная

Конфиденциальная информация имеет конкретную аудиторию: строго соблюдается принцип служебной необходимости (средства контроля доступа). Неразрешенное раскрытие Конфиденциальной информации может повлиять на репутацию ВТ или причинить вред людям.

В числе примеров:

- Персональная информация о физических лицах, будь то сотрудниках ВТ, третьих сторонах или клиентах;

общественного

- Данные системных журналов;
- Данные о продажах и маркетинговые данные;
- Местные бизнес-планы;
- Данные о рисках;
- Пароли;
- Информация, которая является конфиденциальной по закону

Собрание нескольких Конфиденциальных документов

Если у вас на одном объекте имеется собрание Конфиденциальных документов, может потребоваться повышение уровня классификации, и это может привести к переклассификации отдельных документов как Строго конфиденциальных или потребовать принятия дополнительных мер безопасности для защиты объекта, если:

- В совокупности они могут нанести ВТ исключительный ущерб, если будут раскрыты;
- При использовании с иными сочетаниями элементов данных, например, именем и адресом и/или в случае если в системе имеется несколько записей с банковскими реквизитами, они могут быть привлекательной целью.

Если у вас имеются опасения относительно информации, которой вы владеете, обратитесь к своему контактному лицу ВТ.

Строго конфиденциальная

Строго конфиденциальная информация или данные предназначены для предоставления определенному и небольшому кругу лиц; строго соблюдается принцип служебной необходимости (следует знать, у кого имеются копии и у кого имеется доступ). Несанкционированное раскрытие может нанести ВТ исключительный ущерб. Вы должны тщательно оценить, является ли информация Строго конфиденциальной, так как она требует принятия наиболее жестких мер безопасности.

Меры безопасности

Определяемые термины:

Шифрование

Минимальные требования

- Используется шифрование AES 256-бит.
- Длина симметричных ключей должна быть не менее 256 бит.
- Длина несимметричных ключей (например, RSA) должна быть не менее 2 048 бит.
- Используются только известные и доверенные криптографические шифры.
- Использование самозаверяющих сертификатов не допускается.

Пароли/парольные фразы - (для шифрования)

Не должны легко угадываться (например, должны быть как можно более рандомизированными, не связанными с пользовательским идентификатором, пользователями, идентификационными данными, датой и т.п.) и не должны раскрываться с использованием словарей часто используемых паролей. Тем не менее, они, как минимум, должны быть:

- Длиной не менее 8 символов.
- Содержать не менее двух из следующих символов

общественного

- Не алфавитно-цифровые символы, например, (!, £, ", \$, %, ^, &, *, (,), -, _ , +, =, :, ', @, ~, #, ?, <, >,)
- Десятичное число: (0... 9)
- Прописная буква: (A... Z)
- Частные ключи должны быть защищены парольной фразой с использованием комбинации алфавитно-цифровых символов и знаков, как определено выше.

Примечание. Во избежание сомнений, любые специфичные для клиента договорные требования, содержащиеся в контракте с Клиентом, которые требуют более высокого уровня безопасности, имеют приоритет над следующими мерами.

	Меры безопасности	Для внутреннего пользования	Конфиденциальная	Строго конфиденциальная
1	Национальное законодательство о защите данных - Персональные и закрытые личные данные	Не должны рассматриваться как данные для внутреннего пользования. Защита отдельных записей как Конфиденциальной информации.	Защита отдельных записей как Конфиденциальной информации.	Защита комплекса записей как Строго конфиденциальной информации.
2	Контроль распространения и отслеживание перемещения деловых документов (Word, Excel и т.п.)	Контроль и отслеживание не требуется. На каждой странице указывается "ДЛЯ ВНУТРЕННЕГО ПОЛЬЗОВАНИЯ В ВТ" или "ДЛЯ ВНУТРЕННЕГО ПОЛЬЗОВАНИЯ В OPENREACH" , если документ будет совместно использоваться только в Openreach.	На каждой странице указывается "КОНФИДЕНЦИАЛЬНО" , а также необходимо гарантировать следование принципу служебной необходимости и рассмотреть возможность использования списка рассылки . Требуется шифрование в соответствии с определяемыми терминами "Шифрование" и "Пароль/парольная фраза" выше по тексту.	На каждой странице документа указывается "СТРОГО КОНФИДЕНЦИАЛЬНО" . В документ включается список рассылки . Ответственное лицо обязано удостовериться в соблюдении принципа служебной необходимости . До начала хранения требуется шифрование с использованием программного обеспечения, которое соответствует определяемым терминам "Шифрование" и "Пароль/парольная фраза" выше по тексту, если данные не хранятся на предоставленном ВТ ПК/переносном компьютере с

общественного

				шифрованием жесткого диска, т.е. на съемном носителе. То же самое применимо в случае если вы отправляете документ по электронной почте - будь то в ВТ или за ее пределами.
3	Безопасное хранение: на переносном компьютере и ПК	Необходимо безопасное хранение, например, с использованием PGP, WinZip 9.	Шифрование всего диска в соответствии с определяемыми терминами "Шифрование" и "Пароль/парольная фраза" выше по тексту.	Шифрование всего диска в соответствии с определяемыми терминами "Шифрование" и "Пароль/парольная фраза" выше по тексту.
4	Безопасное хранение на сервере и в базах данных (фиксированное - диск/лента)	Безопасное хранение не требуется, если выполнены все физические требования, в противном случае требуется безопасное хранение, например, с использованием PGP, WinZip 9.	Информация ВТ должна быть зашифрована в соответствии с определяемыми терминами "Шифрование" и "Пароль/парольная фраза" выше по тексту.	Информация ВТ должна быть зашифрована в соответствии с определяемыми терминами "Шифрование" и "Пароль/парольная фраза" выше по тексту.
5	Безопасное хранение на устройствах Blackberry, Windows Mobile, иных КПК, планшетах (iPad и т.п.), мобильных телефонах и MP3-плеерах	На таких устройствах запрещается хранить информацию для внутреннего пользования, за исключением случаев, когда устройство предоставляет ВТ или исключение одобрено Службой безопасности ВТ. Такие устройства запрещается конфигурировать для получения доступа к учетным записям электронной почты ВТ.com (доступ к электронной почте bt.com через почтовый веб-интерфейс допускается).	На таких устройствах запрещается хранить Конфиденциальную информацию, за исключением случаев, когда устройство предоставляет ВТ или исключение одобрено Службой безопасности ВТ. Такие устройства запрещается конфигурировать для получения доступа к учетным записям электронной почты ВТ.com (доступ к электронной почте bt.com через почтовый веб-интерфейс допускается).	На таких устройствах запрещается хранить Строго конфиденциальную информацию.
6	Безопасное хранение на: Съемных носителях, таких как карты Memory Stick, флэш-память, CD/DVD-	Информация ВТ должна быть зашифрована при хранении на таких устройствах в соответствии с определяемыми терминами "Шифрование" и	Информация ВТ должна быть зашифрована при хранении на таких устройствах в соответствии с определяемыми терминами	На таких устройствах запрещается хранить Строго конфиденциальную информацию.

общественного

	диски, жесткие диски с USB-интерфейсом, карты Secure Digital, дискеты и иные аналогичные устройства.	"Пароль/парольная фраза" выше по тексту.	"Шифрование" и "Пароль/парольная фраза" выше по тексту.	
7	Веб-хранилище/онлайн новое хранилище или любая система хранения данных в Интернете	Запрещено	Запрещено	Запрещено
8	Совместная работа со сторонними лицами с использованием Веб-средств	Любая платформа MS LiveMeeting или Webjoin	Запрещено	Запрещено
9	Отправка по электронной почте	Шифрование не требуется.	Шифрование для получателей (в случае когда пункт назначения отличается от адреса электронной почты bt.com) в соответствии с определяемыми терминами "Шифрование" и "Пароль/парольная фраза" выше по тексту.	Требуется шифрование в соответствии с определяемыми терминами "Шифрование" и "Пароль/парольная фраза" выше по тексту.
10	Автоматическая пересылка по электронной почте	Запрещено	Запрещено	Запрещено
11	Передача по сети	Шифрование не требуется.	Шифрование для внешней и внутренней передачи в соответствии с определяемыми терминами "Шифрование" и "Пароль/парольная фраза" выше по тексту.	Шифрование для внешней и внутренней передачи в соответствии с определяемыми терминами "Шифрование" и "Пароль/парольная фраза" выше по тексту.
12	Передача файлов	Используется протокол безопасной передачи данных, например SFTP, XFB.	Используется протокол безопасной передачи данных, например SFTP, XFB.	Используется протокол безопасной передачи данных, например SFTP, XFB.
13	Стирание/удаление данных	Используются средства удаления в приложении или операционной системе.	Удаление данных без возможности восстановления путем перезаписи каждого сектора случайными бинарными данными не менее одного раза с использованием программного	Удаление данных без возможности восстановления путем перезаписи каждого сектора случайными бинарными данными не менее одного раза с

общественного

			продукта, например, Blanco HMG Edition или Blanco Version 5 - при использовании твердотельных устройств.	использованием программного продукта, например, Blanco HMG Edition или Blanco Version 5 - при использовании твердотельных устройств.
14	Утилизация или повторное использование ИТ-оборудования (на котором хранится Информация ВТ) Включает, помимо прочего: - Утилизацию отдельных деталей - Уничтожение оборудования Поставщика - Требования к уничтожению резервных копий - Детали серверов, которые отправляются производителю для ремонта	Используется поддающееся проверке и испытанное программное решение для стирания, в котором для подтверждения стирания оформляется официальный сертификат. Любое оборудование, которое не поддается стиранию, должно быть уничтожено с получением/предоставлением официального сертификата, содержащего, как минимум серийный номер оборудования в качестве подтверждения утилизации. Вышеуказанное решение не может использоваться с твердотельными дисками (SSD), которые должны уничтожаться с получением/предоставлением официального сертификата. Дополнительная информация приведена в документе BS EN 17513.	Диски (или иные информационные носители включая, помимо прочего, карты Compact Flash и твердотельные устройства) должны стираться без возможности восстановления путем перезаписи каждого сектора случайными бинарными данными не менее одного раза с использованием программного продукта, например, Blanco HMG Edition или Blanco Version 5 - при использовании твердотельных устройств. Если стирание без возможности восстановления невозможно или нецелесообразно, диск (или иные информационные носители, включая, помимо прочего, карты Compact Flash и твердотельные устройства) должны уничтожаться с использованием средства уничтожения дисков. Для подтверждения стирания или уничтожения должен оформляться официальный сертификат.	Диски (или иные информационные носители, включая, помимо прочего, карты Compact Flash и твердотельные устройства) должны стираться без возможности восстановления путем перезаписи каждого сектора случайными бинарными данными не менее одного раза с использованием программного продукта, например, Blanco HMG Edition или Blanco Version 5 - при использовании твердотельных устройств. Если стирание без возможности восстановления невозможно или нецелесообразно, диск (или иные информационные носители, включая, помимо прочего, карты Compact Flash и твердотельные устройства) должны уничтожаться с использованием средства уничтожения дисков. Для подтверждения стирания или уничтожения должен оформляться официальный сертификат.
15	Печать	Используется принтер, подключенный к ПК, или необходимо личное присутствие рядом с сетевым принтером во	Используется принтер с доступом по PIN-коду, принтер, подключенный к ПК или принтер в	Используется принтер с доступом по PIN-коду, принтер, подключенный к ПК

общественного

		время печати.	помещении с контролируемым доступом. Необходимо перепроверить, на какой из принтеров отправлен документ; запрещается оставлять документы в лотке принтера.	или принтер в помещении с контролируемым доступом. При печати следует быть внимательным. Необходимо перепроверить, на какой из принтеров отправлен документ; запрещается оставлять документы в лотке принтера.
16	Почтовые/курьерские услуги между ВТ и Поставщиком.	Одиночный конверт.	Используются двойные конверты; отправка заказным пакетом для вручения только адресату; на 1-м конверте запрещается указывать "Конфиденциально".	Используется двойной конверт; отправка заказным пакетом для вручения только адресату; на 1-м конверте запрещается указывать "Строго конфиденциально".
17	Раскрытие сторонним лицам	Необходимо обратиться за разрешением к Контактному лицу ВТ в области безопасности. См. Приложение 3.	Необходимо обратиться за разрешением к Контактному лицу ВТ в области безопасности. См. Приложение 3.	Необходимо обратиться за разрешением к Контактному лицу ВТ в области безопасности. См. Приложение 3.
18	Использование в процессе обучения, разработки или тестирования	Необходима анонимность со стороны ВТ и выполнение требований Руководства ВТ по передовым методикам анонимности данных ВР001.	Необходима анонимность со стороны ВТ и выполнение требований Руководства ВТ по передовым методикам анонимности данных ВР001.	Запрещено
19	Утилизация бумаги	Измельчение в shreddерах с поперечной резкой.	Измельчение в shreddерах с поперечной резкой.	Измельчение в shreddерах с поперечной резкой до частиц размером 4 x 15 мм.
20	Общественные зоны	Запрещается обсуждать информацию для внутреннего пользования на публике.	Запрещается обсуждать Конфиденциальную информацию на публике. Запрещается работать с документами в местах общего пользования, где ваши действия можно подсмотреть.	Запрещается обсуждать Строго конфиденциальную информацию на публике. Запрещается работать с документами в местах общего пользования.