Положения о классификации и обращении с информацией сторонних лиц

Введение

Не вся информация обладает одинаковой ценностью или степенью секретности. Классификация информации дает возможность понять, как ее следует защитить; демонстрирует наше стремление к обеспечению ее защиты и способствует эффективному обращению с ней.

Существует четыре уровня классификации информации:

- Общедоступная
- Внутренняя
- «Конфиденциально»
- «Совершенно конфиденциально»

В приведенной ниже таблице представлено краткое пояснение типов информации, которые принадлежат каждой из этих четырех категорий.

По умолчанию любая информация компании BT классифицируется как информация под грифом «Конфиденциально», если не указано иное.

Если вы не уверены, к какой категории отнести информацию, обратитесь за помощью к представителю службы безопасности BT.

Классификация	Общее описание	Примеры
Общедоступная — категория 1	Общедоступная информация — это информация, которая доступна как сотрудникам BT, так и сторонним лицам.	• Рекламные кампании. • Общие сообщения, доступные из открытых источников (например, заявления службы по связям с общественностью (PR), общедоступные статьи о компании BT). • Общественно доступная коммерческая информация, такая как объявленные цены или деловые предложения.
Внутренняя — категория 2	Информация BT, которая доступна для сотрудников BT и лиц, имеющих доступ к информационной сети BT, когда такой доступ несет минимальный деловой риск для BT. Внутренняя информация может включать информацию, которая подпадает под действие общих положений конфиденциальности (например, обычные электронные сообщения, отчеты или контрактная документация), при условии, что эта информация не обладает достаточной степенью коммерческой секретности, чтобы для нее потребовались усиленные защитные меры, описанные ниже.	• Внутренняя информационная рассылка, такая как Новости BT. • Статьи FixIt. • Общие не секретные электронные сообщения (например, некоммерческая информация или персональные данные с ограниченным доступом, что указывается в левой колонке, находящейся в теле электронного сообщения).

«Конфиденциально» — категория 3	Информация под грифом «Конфиденциально» — это информация, к которой должен иметь доступ ограниченный круг лиц. Несанкционированное раскрытие этой информации может нанести ущерб репутации компании BT, или ее раскрытие может потенциально повредить лицам, которых касается эта информация (например, наиболее персональные данные о сотрудниках или клиентах). К информации под грифом «Конфиденциально» должен применяться принцип необходимого знания (need-to-know). **Группа из нескольких документов под грифом «Конфиденциально»** Если группа документов под грифом «Конфиденциально» находится в одном месте, может потребоваться усовершенствование классификации, что может привести к переклассификации отдельных документов с присвоением им статуса «Совершенно конфиденциально», или могут потребоваться дополнительные меры безопасности для защиты места их хранения, если: • совместно они могут стать причиной нанесения исключительного вреда компании BT в случае утечки; или • при использовании с комбинацией других элементов данных они могут стать привлекательной целью для мошенников.	• Данные системного журнала. • Данные по коммерческим секретным операциям и рыночные данные. • Региональные коммерческие планы; • Наиболее персональные данные; и • Данные о рисках. • Все персональные данные (определенные в Положении «**Защита информации**»), кроме случаев, когда они относятся к категории «Совершенно конфиденциально», описанной ниже.
«Совершенно конфиденциально» — категория 4	Информация или данные под грифом «Совершенно конфиденциально» должна иметь определенное и минимальное обращение; должен быть ужесточен принцип необходимого знания (необходимо знать лиц, имеющих копии и обладающих доступом к информации).	• Подробная информация о банковских счетах • Данные для аутентификации должны рассматриваться как данные под грифом «Совершенно конфиденциально». • Пароли от компьютеров; пароли должны храниться и быть защищены

	Несанкционированное раскрытие информации может причинить исключительный вред ВТ. Следует провести тщательный анализ на предмет того, принадлежит ли информация к категории «Совершенно конфиденциально», поскольку для нее предписаны самые жесткие меры контроля за безопасностью.	в соответствии с Положениями о криптографии ВТ. • Данные финансового учета под запретом до публикации ежегодного отчета. • Стратегические бизнес-планы, конкурентная стратегия, новые стратегические продукты и новая политика в области сбыта. • Совершенно секретный анализ конкурентов, партнеров или подрядчиков. • Секретная информация отдела кадров (HR), которая может негативно повлиять на доверие существенного количества сотрудников. • Подробная информация о крупных приобретениях, объединении, изъятии инвестиций и планах слияния. • Подробная информация о существенных уязвимостях сети. • Подробная информация о кодах безопасности клиентов, основных шифрах, вычислении ключей, транзакциях, счетах или результаты аудита; подробная информация о кодах безопасности клиентов, основных шифрах, вычислении ключей, транзакциях, счетах или результаты аудита. • Аудиторские заключения или наблюдения аудита, содержащие подробную информацию о недостатках/уязвимостях в технологиях или процессах ВТ.

Подход к обращению с данными

С информацией необходимо обращаться в соответствии с уровнем классификации для обеспечения надлежащего уровня ее защиты, независимо от того, находится она на компьютере, передается по сети, представлена в письменной или речевой форме.

Существуют правила для обращения с данными и информацией.

- **Речевая и мультимедийная информация**: обсуждение, переписка в социальных сетях, переписка текстовыми сообщениями, переписка в Skype.
- **Документы на бумажных носителях:** печать, регистрация, уничтожение.
- **Электронные документы:** сохранение, отправка по электронной почте, передача, удаление.
- **В приложениях или системах:** центры данных.

Также предусмотрены отдельные инструкции в отношении уровня и типа шифрования, которые должны использоваться для защиты информации («Стандарт шифрования»).

Обращение с речевыми и мультимедийными данными

Код	Предполагаемое действие	Классификация	Требования к обращению	Причина
HSM10	Размещение информации в социальной сети – например, в личной учетной записи Twitter	Общедоступная	Запрещается выкладывать на сайт или оставлять сообщения, которые могут быть логически обоснованно расцениваться как взгляды компании BT, или которые дискредитируют BT и могут нанести вред бренду и репутации BT.	Несанкционированное разглашение информации или личные комментарии могут нанести ущерб нашему бренду
		Внутренняя	Не разрешается	
		«Конфиденциально»	Не разрешается	
		«Совершенно конфиденциально»	Не разрешается	
HSM20	Обсуждение или представление на рассмотрение некоторой информации путем проведения внутреннего совещания или отправки сообщений	Внутренняя	Для этой цели разрешается использование программ Live Meeting, WebEx, Webjoin и Lync/Skype для бизнеса	С внутренними данными могут быть ознакомлены лица, приглашенные на совещание
		«Конфиденциально»	Для этой цели разрешается использование программ Live Meeting, WebEx, Webjoin и Lync/Skype для бизнеса	С внутренними данными могут быть ознакомлены лица, приглашенные на совещание
		«Совершенно конфиденциально»	• Для этой цели разрешается использование программ Lync/Skype для бизнеса, размещенных на сервере BT. • Должна быть удостоверена личность присутствующих на совещании лиц. • Помещение, где проводится совещание, должно быть закрыто, чтобы исключить присутствие посторонних лиц.	Шифрование данных в программах Lync/Skype для бизнеса соответствует Стандарту шифрования, описанному ниже
HSM30	Обсуждение некоторой информации во внешнем чате онлайн-поддержки, например на сайте поддержки разработчика, такого как Cisco	Общедоступная	Обсуждение должно быть ограничено в пределах объема «общедоступной информации», находящейся в свободном доступе на нашем сайте.	Для предотвращения несанкционированного раскрытия информации
		Внутренняя	Не разрешается	
		«Конфиденциально»	Не разрешается	
		«Совершенно конфиденциально»	Не разрешается	
HSM40	Обсуждение некоторой информации с другим лицом при личном контакте/по телефону	Внутренняя	Убедитесь в том, что разговор не может подслушать любое лицо, не являющееся сотрудником BT или не действующее в интересах BT	Для предотвращения несанкционированного раскрытия информации

		«Конфиденциально»	То же, что и для «внутренней информации», а также • Перед обсуждением какой-либо конфиденциальной информации удостоверьте личность лица, с которым ведется разговор, и убедитесь в том, что это лицо подпадает под действие принципа необходимого знания. • Перед началом разговора убедитесь в наличии договора с соответствующими третьими сторонами, если данное условие применимо (Примечание: перед уступанием прав и обязанностей по всему договору или его части в пользу третьей стороны, или перед заключением субподрядного договора, необходимо получить предварительное письменное согласие BT). • Убедитесь в том, что разговор не может быть подслушан. • Запрещается оставлять информацию под грифом «Конфиденциально» на голосовой почте.	Для защиты конфиденциальной информации и ограничения ее распространения только кругом лиц, имеющих право на доступ
		«Совершенно конфиденциально»	То же, что и для информации под грифом «Конфиденциально», а также • Сократите объем информации под грифом «Совершенно конфиденциально» до абсолютного минимума	
HSM50	Отправка сообщения/информационных материалов по SMS/MMS всем сторонам (сотрудникам и сторонним лицам)	Общедоступная	Содержимое сообщения должно быть ограничено в пределах объема «общедоступной информации», которая доступна на нашем сайте	Для предотвращения несанкционированного раскрытия информации
		Внутренняя	Особые требования к обращению отсутствуют	
		«Конфиденциально»	Убедитесь в том, что сообщение отправлено только лицам, имеющим право на доступ, и что не разглашается следующее: • Информация о платежных картах. • Подробная банковская информация.	Эти три пункта принадлежат к информации под грифом «Совершенно конфиденциально»

			• Подробная информация о паролях.	
		«Совершенно конфиденциально»	Не разрешается	

Обращение с документами на бумажных носителях

Код	Предполагаемое действие	Классификация	Требования к обращению	Причина
HPD10	Работа с информацией на бумажных носителях в помещении, принадлежащем стороннему лицу, или дома	Внутренняя	Покидая рабочее место, придерживайтесь политики «чистого стола»	Для предотвращения случайного раскрытия информации
		«Конфиденциально»	То же, что и для «внутренней информации», а также • Когда работа с документами не ведется, необходимо их спрятать и закрыть на ключ.	
		«Совершенно конфиденциально»	То же, что и для информации под грифом «Конфиденциально»	
HPD20	Отправка документа на печать	Внутренняя	• Проверьте, отправлен ли документ на нужный принтер • Запрещается оставлять документы в лотке принтера	Для предотвращения случайного раскрытия информации
		«Конфиденциально»	То же, что и для «внутренней информации», а также • Используйте принтер с контролируемым доступом, принтер, подключенный к персональному компьютеру (ПК), или принтер в помещении с контролируемым доступом	
		«Совершенно конфиденциально»	То же, что и для информации под грифом «Конфиденциально»	
HPD30	Использование принтера, который не находится ни в помещении поставщика, ни дома (например, в помещении, принадлежащем стороннему лицу, в отеле и т. п.)	Внутренняя	Обычно это не разрешается, поскольку принтеры имеют запоминающие устройства, откуда могут быть извлечены данные. Воспользуйтесь здравым смыслом – вы действительно хотите, чтобы другие лица увидели эту информацию?	Данные и информация могут быть извлечены из запоминающего устройства принтера
		«Конфиденциально»	Не разрешается	
		«Совершенно конфиденциально»	Не разрешается	
HPD40	Перемещение информации на	Внутренняя	Поместите документ в непрозрачную папку или пакет	Для защиты от случайного раскрытия

	бумажном носителе за пределы рабочего места	«Конфиденциально»	То же, что и для «внутренней информации», а также • Запрещается выносить данные клиентов и/или платежные данные из офиса поставщика	
		«Совершенно конфиденциально»	То же, что и для информации под грифом «Конфиденциально»	
HPD50	Передача или отправка информации на бумажном носителе сотрудникам компании	Внутренняя	• Поместите документ в конверт и воспользуйтесь услугами внутренней почты.	Меры защиты против случайного просмотра информации
		«Конфиденциально»	• Запрещается ставить пометку «Конфиденциально» на внешней стороне конверта. • Если информация защищена юридической привилегией, обратитесь за указаниями в юридический отдел.	Предотвращается ознакомление с содержимым, проходящим под грифом «Конфиденциально», со стороны случайных наблюдателей. Подпись об отправке обеспечивает доказательство регистрации, подпись за доставку и подтверждение в режиме реального времени доставки документа.
		«Совершенно конфиденциально»	• Используйте 2 конверта и при отправке воспользуйтесь услугами «отслеживаемой доставки» • Запрещается ставить пометку «Совершенно конфиденциально» на внешней стороне конверта • Получите разрешение владельца документа на то, чтобы поделиться печатной копией • Предпочтительной является передача из рук в руки уполномоченных поименованных лиц • Установите связь между копиями и лицами путем печати водяных знаков в виде названия или номера документа (если это возможно) • В случае утери необходимо заявить о нарушении безопасности	Предотвращается ознакомление с содержимым, проходящим под грифом «Совершенно конфиденциально», со стороны случайных наблюдателей. Подпись об отправке обеспечивает доказательство регистрации, подпись за доставку и подтверждение в режиме реального времени доставки документа.
HPD60	Передача или отправка печатной	Внутренняя «Конфиденциально»	Убедитесь в наличии договора с соответствующими третьими	См. HPD50

	копии сторонним лицам	«Совершенно конфиденциально»	сторонами в соответствии с кодом HSM40. Все остальные меры контроля аналогичны мерам, предпринимаемым при передаче информации сотрудникам	
HPD70	Отправка информации по факсу	Внутренняя	Убедитесь в наличии титульного листа факса перед страницей (страницами) с содержанием	Для предотвращения случайного раскрытия информации
		«Конфиденциально»	• Перед отправкой содержимого по факсу необходимо отправить титульный лист с пробной страницей, а затем связаться с получателем для подтверждения получения • Если информация защищена юридической привилегией, обратитесь за указаниями в юридический отдел	Для предотвращения получения информации неуполномоченными лицами
		«Совершенно конфиденциально»	Не разрешается	
HPD80	Уничтожение информации на бумажном носителе	Внутренняя	Необходимо • измельчить документ на мелкие куски или • положить документ в корзину для бумаг, откуда его нельзя просто достать	По критериям безопасности обычные мусорные корзины и/или мусорные ведра не подходят для уничтожения документов.
		«Конфиденциально»	Документ должен быть измельчен на мелкие куски с минимальным размером частиц $\leq$ 160 мм² и с одинаковой шириной полосок $\leq$ 2 мм, например, на полоски размером 2X15 мм.	Для защиты от раскрытия информации под грифом «Конфиденциально».
		«Совершенно конфиденциально»	Документ должен быть измельчен на мелкие куски с минимальным размером частиц $\leq$ 160 мм² и с одинаковой шириной полосок $\leq$ 2 мм, например, на полоски размером 2X15 мм с помощью измельчителя бумаг с поперечной резкой	Для защиты от раскрытия информации под грифом «Совершенно конфиденциально».

Обращение с электронными документами

Код	Предполагаемое действие	Классификация	Требования к обращению	Причина
HED10	Сохранение электронной информации на рабочий ноутбук/ПК	Внутренняя	Должно использоваться полное шифрование дисков в соответствии со Стандартом шифрования, указанным ниже.	Информация преобразуется в нечитаемый код, который не может быть легко разобран

				неуполномоченными лицами.
		«Конфиденциально»	Должно использоваться полное шифрование дисков в соответствии со Стандартом шифрования, указанным ниже.	
		«Совершенно конфиденциально»	Должно использоваться полное шифрование дисков в соответствии со Стандартом шифрования, указанным ниже.	
HED20	Сохранение документов в программе SharePoint или другой системе управления документами, которая НЕ находится в облачном хранилище или НЕ связана с интернет-услугами	Внутренняя	• Используйте уровни полномочий и группы для задания ролевого управления доступом. Они должны быть назначены минимально необходимому количеству лиц для выполнения работы • Пересматривайте уровни управления доступом каждый год	Ограничение доступа и/или редактирования кругом лиц, имеющих право на доступ.
		«Конфиденциально»	То же, что и для «внутренней информации», а также • Задокументируйте процесс назначения ролей лицам. • Роли и лица, назначенные им, подлежат пересмотру каждые 90 дней • Документы должны быть зашифрованы в соответствии со Стандартом шифрования, указанным ниже	
		«Совершенно конфиденциально»	То же, что и для «внутренней информации», а также • Задокументируйте процесс назначения ролей лицам. • Роли и лица, назначенные им, подлежат пересмотру каждые 90 дней • Документы должны быть зашифрованы в соответствии со Стандартом шифрования, указанным ниже	
HED30	Сохранение электронной информации в облачном хранилище или с помощью интернет-услуг, например, Google	Внутренняя	Не разрешается.	Пользование интернет-услугами повышает риск несанкционированного доступа к информации.
		«Конфиденциально»	Не разрешается.	

	docs, GitHub, btcloud.bt.com, Drobox, Pastebin, Facebook и т. п.	«Совершенно конфиденциально»	Не разрешается.	
HED40	Сохранение электронной информации на съемном носителе, например, флеш-накопителе.	Внутренняя	• USB-устройства должны быть зашифрованы в соответствии со Стандартом шифрования, указанным ниже Ни при каких обстоятельствах не разрешается хранить персональные данные на этих устройствах, если они не зашифрованы в соответствии со Стандартом шифрования, указанным ниже.	Съемный носитель может быть утерян или украден с большей вероятностью, чем целый компьютер, поэтому и риск получения доступа к данным неуполномоченными лицами выше. Для защиты информации она должна быть преобразована в нечитаемый код, который не может быть легко разобран неуполномоченными лицами.
		«Конфиденциально»	То же, что и для «внутренней информации»	
		«Совершенно конфиденциально»	То же, что и для «внутренней информации»	
HED50	Сохранение электронных документов или информации ВТ на личный ноутбук или устройство	Внутренняя	Не разрешается	Неуполномоченные лица могут получить доступ к данным ВТ, особенно в случае, если устройство утеряно, украдено, или в случае отказа от него в пользу более новой модели.
		«Конфиденциально»	Не разрешается	
		«Совершенно конфиденциально»	Не разрешается	
HED60	Отправка электронных документов или информации на личный электронный адрес	Внутренняя	Не разрешается	Для предотвращения раскрытия неуполномоченным лицам.
		«Конфиденциально»	Не разрешается	
		«Совершенно конфиденциально»	Не разрешается	
HED70	Автоматическая переадресация на электронный адрес	Внутренняя	Не разрешается	К данным могут получить доступ неуполномоченные лица в случае взлома учетной записи электронной почты, ISP или интернет-соединения.
		«Конфиденциально»	Не разрешается	
		«Совершенно конфиденциально»	Не разрешается	
HED80	Передача или отправка электронной информации по электронной почте *в пределах компании*	Внутренняя	Особые требования отсутствуют	
		«Конфиденциально»	• Убедитесь, что электронное сообщение отмечено как «Конфиденциально» • Используйте настройки секретности, чтобы пометить электронное письмо как «Конфиденциально»	Для сохранения контроля над конфиденциальной информацией.

			• В идеальном варианте настройте разрешения на состояние «Переадресация запрещена» • Если информация защищена юридической привилегией, обратитесь за указаниями в юридический отдел •	
		«Совершенно конфиденциально»	То же, что и для информации под грифом «Конфиденциально», а также • Для отправки используйте защищенную электронную почту • Если нельзя воспользоваться защищенной электронной почтой, перед отправкой необходимо зашифровать документ в соответствии со Стандартом шифрования, указанным ниже • Настройте разрешения на состояние «Переадресация запрещена»	Для защиты информации во время передачи по сети.
HED90	Передача или отправка электронной информации по электронной почте *за пределы компании*	Внутренняя	Отправку информации стороннему лицу можно осуществлять только в случае наличия договора в соответствии с кодом HSM40	Для сохранения контроля над конфиденциальной информацией.
		«Конфиденциально»	То же, что и для «внутренней информации», а также • Шифрование в соответствии со Стандартом шифрования, указанным ниже • Перед отправкой убедитесь в правильности электронного адреса • Если информация защищена юридической привилегией, обратитесь за указаниями в юридический отдел	
		«Совершенно конфиденциально»	То же, что и для информации под грифом «Конфиденциально»	
HED120	Создание резервной копии	Внутренняя	• Документы должны храниться на сетевых	Резервные копии должны иметь тот же

	электронных документов ВТ		дисках поставщика или в системе управления документами поставщика, в соответствии с кодом HED030. • Резервные копии документов должны быть обеспечены тем же уровнем защиты, что и сетевой диск, SharePoint. • В случае использования съемного носителя, это устройство должно быть зашифровано в соответствии со Стандартом шифрования, указанным ниже.	уровень классификации и защиты, что и исходные данные.
		«Конфиденциально»	То же, что и для «Внутренней информации» а также • Зашифруйте документ в соответствии со Стандартом шифрования, указанным ниже, перед созданием резервной копии	
		«Совершенно конфиденциально»	То же, что и для информации под грифом «Конфиденциально»	

Обращение с системными данными и данными приложений

Код	Предполагаемое действие	Классификация	Требования к обращению	Причина
HSADE	Сохранение и обработка электронных данных и информации, находящихся во центре данных или на системном сервере	Внутренняя	В случае соблюдения всех применимых требований, указанных выше в отношении сохранения данных для этой классификации, особые требования отсутствуют.	
		«Конфиденциально»	Необходимо соблюдать Требования к внешнему размещению данных сторонних лиц http://www.selling2bt.com/working/ThirdPartySecuritystandards/index.htm	
		«Совершенно конфиденциально»	То же, что и для информации под грифом «Конфиденциально», а также Для защиты данных о банковских счетах, поскольку это особо секретные данные, должны соблюдаться следующие меры контроля. Они обладают приоритетом перед любыми другими применимыми мерами контроля в этих положениях о безопасности. 1. Банковским счетам должны быть присвоены маркеры для лиц (персональные банковские счета клиентов и сотрудников BT), за исключением подробной информации о банковских счетах BT и подробной банковской информации различных юридических лиц BT). 2. Если в приложении хранятся только корпоративные банковские счета, то стороннее лицо может подвести базу под эту информацию (на основании времени, расходов, ресурсов, количества счетов и количества пользователей с доступом к приложению и т. п.) в отношении того, был ли изначально принят компанией BT алгоритм на основе шифрования. Если алгоритм на основе шифрования принят, то BT должно пересмотреть это решение, когда все банковские счета будут защищены, для определения того, можно ли продолжать. На это решение может повлиять уровень угрозы и готовность к принятию риска предприятия в целом. 3. При отображении действительной подробной информации о банковских счетах агенту в качестве части делового процесса (например, для удостоверения наличия правильного счета для оплаты, или при осуществлении связи с клиентом, например, по электронной почте, или при предъявлении счета) необходимо показывать только последние 4 цифры банковского счета (т. е. скрыть подробную информацию о банковском счете).	

			4. В случае возникновения необходимости в получении доступа ко всему банковскому счету (например, для создания запроса на кредитование или дебетование от банка) из подробной банковской информации должны быть удалены маркеры или она должна быть расшифрована, а затем передана в банк с использованием шифрованного механизма передачи, совместимого с политикой обеспечения безопасности ВТ. Немедленно после использования расшифрованной или лишенной маркеров подробной банковской информации, она должна быть удалена безопасным образом.	

Стандарты шифрования

Общие криптографические меры контроля.

Код	Меры контроля	Причина
C1.10	Должны использоваться текущие криптографические библиотеки	Криптографические библиотеки регулярно обновляются. В дополнение к обновлению пакетов программного обеспечения в соответствии с инструкциями разработчика, пакеты криптографического программного обеспечения должны регулярно пересматриваться и обновляться.
C1.20	Разрешается использовать только одобренные в отрасли наборы шифров для шифрования. Например, TLS SSLv2	Не одобренные шифры могут привести к появлению уязвимостей
C1.30	Для новых разработок должна использоваться самая последняя версия TLS. Запрещается использоваться SSL версии V1,2 и 3	Более ранние версии, вплоть до TLS1.0 включительно, больше не считаются безопасными
C1.40	Должна быть активирована функция совершенной прямой секретности	Алгоритмы совершенной прямой секретности предотвращают расшифровку перехваченных сообщений, даже в случае взлома секретного ключа аутентификации в будущем
C1.50	Запрещается использовать самозаверенные сертификаты	Самозаверенные сертификаты сводят на нет преимущества аутентификации оконечного устройства, а также существенно снижает возможность лица обнаружить атаку посредника (man-in-the-middle attack).
C1.60 **GTS2.370**	Принятый в отрасли центр сертификации должен использоваться для управления сертификатами. Например, verisign	Для хранения перечня выданных сертификатов, в целях проверки уязвимостей и определения срока истечения сертификата
C1.70	Пароли должны быть защищены с использованием необратимой математической функции (например, алгоритма хэширования) с помощью уникального фактора рандомизации («соли») для каждого пароля. Примечание: «СОЛЬ» — это случайные данные, которые используются в качестве дополнительной вводной для необратимой функции, которая «хэширует» пароль или кодовую фразу.	Сохраненные файлы паролей могут быть извлечены, и, таким образом, все записи должны быть защищены для предотвращения извлечения незашифрованных паролей
C1.80	Пароли, защищенные в соответствии с кодом C1.70, должны храниться отдельно от конфигурационных файлов системы. Также	Необходимо исключить возможность извлечения защищенных паролей посредством обхода каталога, команды SNMP walk, дампа файла

	должна быть реализована система управления доступом, чтобы только соответствующие привилегированные пользователи могли читать или копировать содержимое.	конфигурации, или другого механизма, который может позволить осуществлять попытки взлома в режиме «оффлайн».

Техническая реализация криптографии

Протоколы SSL/TLS	
Разрешается использовать	**Запрещается использовать**
TLSv1.3 (tbc — доступен в пакете OpenSSL после 5 апреля).	SSLv3.0
TLSv1.2	SSLv2.0
TLSv1.1	
TLS v1.0*	

***** Срок работы протокола TLSv1.0 уже истекает и он может быть не рекомендован к применению в любой момент времени в связи с известными проблемами. В целях соблюдения совместимости (например, PCI-DSS) может потребоваться отключение таких протоколов, как TLSv1.0 и TLSv1.1. Все разработчики должны быть готовы к отключению этих протоколов в файле конфигурации.

Размеры ключей			
	Симметричный	**Асимметричный**	**На эллиптической кривой**
Действующие предприятия	≥ 112 битов	≥ 2048 битов	≥ 224 бита
Новые предприятия	≥ 128 битов	≥ 3072 бита	≥ 384 бита

Обмен ключами	
Разрешается использовать	**Запрещается использовать**
ECDHE (обмен эфемерными (временными) ключами по алгоритму Диффи-Хеллмана (ключи не основаны на сертификатах))	kRSA (обмен ключами по алгоритму RSA)
	kDHr (обмен ключами по алгоритму Диффи-Хеллмана с использованием RSA-ключа)
	kDHd (обмен ключами по алгоритму Диффи-Хеллмана с использованием DSA-ключа)
	kSRP (обмен ключами по протоколу безопасного распределения ключей (SRP)) kADH (анонимный обмен ключами по алгоритму Диффи-Хеллмана)
	kPSK (обмен предварительно выданными ключами)

Алгоритм совершенной прямой секретности должен быть основан на локально сконфигурированных или сгенерированных значений групп Диффи-Хеллмана, которые включают «безопасные» затравки.

Параметры Диффи-Хеллмана

Параметры Диффи-Хеллмана	
Разрешается использовать	**Запрещается использовать**
3072-битная группа Диффи-Хеллмана (наилучший вариант – сгенерированная на локальном устройстве).	Значения сервера по умолчанию (сгенерируйте свои собственные значения на локальном устройстве)

2048-битная группа Диффи-Хеллмана (в случае приближения конца срока использования – должна быть сгенерирована на локальном устройстве).	

Аутентификация	
Разрешается использовать	**Запрещается использовать**
aRSA (Аутентификация RSA)	aNULL (без аутентификации)
aECDSA (Аутентификация по алгоритму цифровой подписи на основе эллиптических кривых)	aDSS (Аутентификация DSS)
	aECDH (алгоритм Диффи-Хеллмана на эллиптических кривых)
	aDH (алгоритм Диффи-Хеллмана)
	aDSA (алгоритм цифровой подписи)
	aPSK (предварительно выданный ключ)
	aSRP (безопасное распределение ключей)

Шифр/шифрование	
Разрешается использовать	**Запрещается использовать**
AES 256 GCM (Rijndael (усовершенствованный стандарт шифрования) — режим счетчика с аутентификацией Галуа)	eNULL (без шифрования)
AES 128 GCM (Rijndael (усовершенствованный стандарт шифрования) — режим счетчика с аутентификацией Галуа)	DES (шифрование DES)
CHACHA20/POLY1305 (256)	3DES (шифрование 3DES)
AES 256 CCM (Rijndael (усовершенствованный стандарт шифрования) — (режим счетчика с CBC-Mac)	RC4 (шифрование RC4)
AES 128 CCM (Rijndael (усовершенствованный стандарт шифрования) — (режим счетчика с CBC-Mac)	RC2 (шифрование RC2)
AES 256 CBC (сцепление блоков шифротекста по стандарту Rijndael) — приближается конец использования.	IDEA (шифрование IDEA)
AES 128 CBC (сцепление блоков шифротекста по стандарту Rijndael) — приближается конец использования.	Seed (шифрование Seed)
	Camellia (шифрование Camellia)
	ARIA (шифрование ARIA)

Цифровой алгоритм MAC	
Разрешается использовать	**Запрещается использовать**
AEAD (аутентифицированное шифрование с присоединенными данными)	MD5 (хэш-функция MD5)
SHA512 (семейство SHA2 — хэш-функция SHA512)	SHA1 (хэш-функция SHA1)
SHA384 (семейство SHA2 — хэш-функция SHA384)	SHA (альтернативное название для SHA1)
SHA256 (семейство SHA2 — хэш-функция SHA256)	