DNV·GL

MANAGEMENT SYSTEM CERTIFICATE

Сертификат №:
281312-2018-AIS-MCW-UKAS

Дата начальной сертификации:
27 июня 2019

Действителен:
27 июня 2019 - 27 июня 2022

Настоящим удостоверяется, что система менеджмента организации:

ООО "ВНЕДРЕНЧЕСКИЙ ЦЕНТР"

Дмитровское шоссе, 9Б, Москва, Российская Федерация, 127434

была признана соответствующей стандарту системы менеджмента информационной безопасности:

ISO/IEC 27001:2013

Настоящий сертификат действителен для следующей области:

**Предоставление программных продуктов по модели подписки;
Предоставление вычислительных мощностей по модели подписки;
Проектирование, разработка и инсталляция облачных инфраструктур;
Техническая поддержка при предоставлении облачных сервисов в соответствии с заявлением о применимости версии 20.05.2019.**

Место и дата:
London, 27 июня 2019

UKAS MANAGEMENT SYSTEMS
0013

От выпускающего офиса:
DNV GL - Business Assurance
4th Floor, Vivo Building, 30 Stamford Street, London, SE1 9LQ, United Kingdom

Erie Koek
Представитель руководства

Сведения приведены на дату: 20.05.2019 15:48

Интерпретация требований стандарта ISO 27001

1. Интерпретация требований стандарта ISO

Элемент стандарта	Ссылки	Назначение
A.10. Криптография		
A.10.1 Криптографические методы защиты		
A.10.1.1 Политика использования криптографических методов защиты	QMS-27.02.04-R Политика использования криптографических методов защиты	Политика использования криптографических методов необходима для достижения максимальных выгод и минимизации рисков использования криптографических методов, а также чтобы избежать ненадлежащего или неправильного использования.
A.10.1.2 Управление ключами	QMS-27.02.04-R Политика использования криптографических методов защиты	Управление криптографическими ключами является принципиально важным с точки зрения результативного использования криптографических методов.
A.11. Физическая безопасность и защита от природных угроз		
A.11.1 Охраняемая зона		
A.11.1.1 Физический периметр безопасности	QMS-27.03.06-Pr. Управление физической безопасностью и защита от природных	Физическая защита обеспечена введением одной или нескольких линий защиты вокруг помещений организации и устройств обработки информации. Применение множественных линий защиты дает дополнительную защиту, так как сбой на одной не ведет к тому, что безопасность будет немедленно нарушена.
A.11.1.2 Средства контроля прохода	QMS-27.03.06-Pr. Управление физической безопасностью и защита от природных	Описание защиты охраняемых зон соответствующими средствами контроля прохода с целью гарантировать, что только имеющему права персоналу разрешен проход.
A.11.1.3 Защита офисов, помещений и устройств	QMS-27.03.06-Pr. Управление физической безопасностью и защита от природных	Защита офисов, помещений и устройств от несанкционированный доступ.
A.11.1.4 Защита от внешних угроз и угроз природного характера	QMS-27.03.06-Pr. Управление физической безопасностью и защита от природных	Снижение рисков повреждений от пожара, наводнения, землетрясения, взрыва, общественных беспорядков и других форм угроз природного, техногенного или социального характера.
A.11.1.5 Работа в охраняемых зонах	QMS-27.03.06-Pr. Управление физической безопасностью и защита от природных	Включение мер для сотрудников, поставщиков услуг и внешних пользователей, работающих в охраняемой зоне , охватывающий все виды деятельности, выполняемые в охраняемой зоне для снижения рисков
A.11.1.6 Зоны доставки и отгрузки	QMS-27.03.06-Pr. Управление физической безопасностью и защита от природных	Места доступа, такие как зоны доставки и отгрузки и иные, где есть возможность пройти в помещение лицам без соответствующих прав, должны контролироваться и быть изолированными от средств обработки информации, чтобы избежать несанкционированного доступа.
A.11.2 Оборудование		
A.11.2.1 Размещение и защита оборудования	QMS-27.03.06-Pr. Управление физической безопасностью и защита от природных	Предотвращение потери, повреждения, кражи или компрометации активов и нарушения деятельности ДОС. Определение того, как оборудование должно быть размещено и защищено так, чтобы снизить риски, связанные с природными угрозами и опасностями, а также возможностью несанкционированного доступа.
A.11.2.2 Службы обеспечения	QMS-27.03.06-Pr. Управление физической безопасностью и защита от природных	Для снижения рисков оборудование должно быть защищено от перебоев в электроснабжении и других нарушений, вызванных перебоями в работе служб обеспечения.
A.11.2.3 Защита кабельных сетей	QMS-27.03.06-Pr. Управление физической безопасностью и защита от природных	Для снижения рисков питающие кабели и кабели, передающие данные или обеспечивающие работу сервисов, должны быть защищены от перехвата, помех или повреждения.
A.11.2.4 Обслуживание оборудования	QMS-27.03.06-Pr. Управление физической безопасностью и защита от природных	Для снижения рисков оборудование должно надлежащим образом обслуживаться, чтобы гарантировать его постоянную готовность и исправность.
A.11.2.5 Вынос активов	QMS-27.03.06-Pr. Управление физической безопасностью и защита от природных	Выявление случаев несанкционированного выноса активов, выявления неразрешенных записывающих устройств, оружия, а также для предупреждения их проноса на территорию и выноса с территории для снижения рисков.
A.11.2.6 Защита оборудования и активов вне территории	QMS-27.03.06-Pr. Управление физической безопасностью и защита от природных	Применение мер обеспечения безопасности к активам вне контролируемой зоны, принимая во внимание различные риски работы вне помещений ДОС.
A.11.2.7 Безопасная утилизация или повторное использование оборудования	QMS-27.02.11-R. Политика уничтожения и утилизации QMS-27.03.06-Pr. Управление физической безопасностью и защита от природных	Все элементы оборудования, содержащие накопители, должны быть проверены, чтобы гарантировать, что любые ценные данные и лицензионное программное обеспечение удалены или надежным образом затерты новой информацией до утилизации или повторного использования.
A.11.2.8 Оборудование пользователя, оставленное без присмотра	QMS-27.03.06-Pr. Управление физической безопасностью и защита от природных	Все пользователи должны быть осведомлены о требованиях безопасности и процедурах для защиты оборудования, остающегося без присмотра, равно как и об их ответственности за обеспечение такой защиты.
A.11.2.9 Политика чистого стола и чистого экрана	QMS-27.02.08-R. Политика чистого стола и чистого экрана QMS-27.03.06-Pr. Управление физической безопасностью и защита от природных	Снижение риска несанкционированного доступа, потери или повреждения информации в рабочее и внерабочее время.
A.12. Безопасность производственной деятельности		
A.12.1 Рабочие процедуры и обязанности		
A.12.1.1 Документированные рабочие процедуры	QMS-27.03.07-I Инструкция сотруднику ДРИП ДОС QMS-01.04.01-R Требования к процессу управления документацией СМК ГК 1С-Рарус QMS-01.04.02-Pr Управление документацией СМК QMS-01.04.04-Pis Согласование нормативного документа	Рабочие процедуры для повседневной деятельности, связанной с оборудованием обработки информации и средствами связи, такие, как процедуры включения и выключения компьютеров, резервного копирования, обслуживания оборудования, работы с носителями, управления и обеспечения безопасности в компьютерном зале и при обработке почты, с целью общего повышения уровня осведомленности и защищенности ИОС.
A.12.1.2 Управление изменениями	QMS-27.02.13-Pr. Политика управления изменениями QMS-01.04.01-R Требования к процессу управления документацией СМК ГК 1С-Р QMS-01.04.02-Pr Управление документацией СМК QMS-01.04.04-Pis Согласование нормативного документа	Управление изменениями в организации, бизнес-процессах, средствах обработки информации и системах, которые влияют на информационную безопасность. Несоответствующий контроль изменений в средствах обработки информации и системах является типичной причиной системных сбоев или нарушений безопасности.
A.12.1.3 Управление производительностью	QMS-27.02.15-Pr Политика ведения журналов и мониторинга	Отслеживание, регулирование и прогнозирование требований к производительности в будущем с тем, чтобы гарантировать необходимую работоспособность систем для снижения рисков.
A.12.1.4 Разделение среды разработки, тестирования и эксплуатации	QMS-27.02.14-R Политика безопасности при разработке	Разделение среды разработки, тестирования и рабочей среды необходимо для снижения риска случайного изменения или неавторизованного доступа к рабочему программному обеспечению или рабочим данным.
A.12.2 Защита от вредоносного кода		
A.12.2.1 Меры защиты от вредоносного кода	QMS-27.03.05-R. Защита от вредоносного кода	В отношении вредоносного кода должны применяться меры по обнаружению, предупреждению и восстановлению с соответствующим информированием пользователей, с целью защиты информации и средств вычислительной техники.
A.12.3 Резервное копирование		
A.12.3.1 Резервное копирование информации	QMS-27.02.05-R. Политика резервного копирования	Определение требований ДОС к резервному копированию информации, программному обеспечению и системам, требованиям по защите и срокам хранения, предоставлению соответствующий устройств для резервного копирования с гарантией того, что существенная информация и программное обеспечение могут быть восстановлены после аварийной ситуации, сбоя носителя или запроса клиента ДОС.
A.12.4 Ведение журналов и мониторинг		
A.12.4.1 Регистрация событий	QMS-27.02.15-Pr Политика ведения журналов и мониторинга	Регистрация событий служит источником данных для автоматизированных систем мониторинга, которые способны генерировать консолидированные отчеты и предупреждения системы безопасности для снижения рисков.
A.12.4.2 Защита информации в журналах	QMS-27.02.15-Pr Политика ведения журналов и мониторинга	Предотвращение неавторизованных изменений информации в: журналах и проблем функционирования устройств ведения журналов, включая изменение типов сообщений, которые были записаны, удаление или редактирование лог-файлов.
A.12.4.3 Журналы действий администратора и оператора	QMS-27.02.15-Pr Политика ведения журналов и мониторинга	Контроль вмешательств системных и сетевых администраторов и операторов, обеспечение защиты журналов и обеспечение регулярного просмотра для снижения рисков.
A.12.4.4 Синхронизация часов	QMS-27.03.01-P Управление активами и техническими уязвимостями	Документирование внутренних требований к представлению времени, синхронности и точности. Правильная установка компьютерных часов является важной для обеспечения точности и отсутствия конфликтов записей в базах данных для снижения
A.12.5 Контроль эксплуатируемого программного обеспечения		
A.12.5.1 Установка программ в эксплуатируемых системах	QMS-27.03.05-R Защита от вредоносного кода	Компьютерное программное обеспечение может зависеть от извне поставляемых программ и модулей, которые должны контролироваться во избежание неавторизованных изменений, способных породить уязвимости в защите.
A.12.6 Управление техническими уязвимостями		
A.12.6.1 Управление техническими уязвимостями	QMS-27.03.01-P Управление активами и техническими уязвимостями	Производители часто находятся под значительным давлением необходимости выпустить патчи как можно быстрее. Вследствие чего существует возможность того, что патч не устраняет проблему надлежащим образом и имеет негативные побочные эффекты. Также в некоторых случаях деинсталляция патча после его применения не может быть выполнена достаточно легко.
A.12.6.2 Ограничения на установку программного обеспечения	QMS-27.03.05-R Защита от вредоносного кода	Определение правил, регулирующих установку программного обеспечения пользователям и сотрудникам ДОС, с целью снижения рисков
A.12.7 Ограничения на аудит информационных систем		
A.12.7.1 Средства управления аудитом информационных систем	QMS-01.05.03.08-Pr Внутренние аудиты	Планирование и сгласование требований и действий по аудиту, с целью минимизации нарушений нормального выполнения бизнес-процессов.
A.13. Безопасность обмена информацией		
A.13.1 Управление сетевой безопасностью		
A.13.1.1 Средства управления сетями	QMS-27.02.10-R. Политика управления сетевой безопасностью	Обеспечение безопасности в сетях и защита подключенных сервисов от несанкционированного доступа с целью снижения
A.13.1.2 Безопасность сетевых сервисов	QMS-27.02.10-R. Политика управления сетевой безопасностью	С целью снижения рисков определены для всех сетевых услуг механизмы обеспечения безопасности, уровни сервиса и требования к управлению, осуществляются ли эти услуги внутренними подразделениями или сторонней организацией.
A.13.1.3 Разделение в сетях	QMS-27.02.10-R. Политика управления сетевой безопасностью	Сети часто выходят за границы организации, поскольку деловое сотрудничество требует взаимодействия и совместного использования сетевого оборудования и устройств обработки информации. Такое расширение может увеличивать риск неавторизованного доступа к информационным системам организации, использующим сеть, некоторые из которых требуют защиты от пользователей других сетей в силу их критической важности или уязвимости. С целью снижения риска определены требования по разделению в сетях.
A.13.2 Передача информации		
A.13.2.1 Политики и процедуры передачи информации	QMS-27.02.06-R. Политика передачи информации	Учет юридических последствия, влияния на бизнес и безопасность, связанные с обменом электронными данными и электронными коммуникациями, а также требованиями к средствам управления с целью снижения рисков.
A.13.2.2 Соглашения по передаче информации	QMS-27.02.06-R. Политика передачи информации	Регламентирование безопасной передачи бизнес-информации между ДОС и внешними сторонами, с целью снижения рисков.
A.13.2.3 Электронные сообщения	QMS-27.02.06-R. Политика передачи информации	Информация, передаваемая электронными сообщениями, должна быть соответствующим образом защищена, с целью снижения
A.13.2.4 Соглашения о конфиденциальности или неразглашении	QMS-27.01.10-R Требования к набору и компетентности персонала	Соглашения о конфиденциальности и неразглашении защищают информацию организации и доводят до сведения подписавших их обязанности по защите, использованию и разглашению информации в духе ответственности и полномочий.
A.14. Приобретение, разработка и обслуживание систем		
A.14.1 Требования по безопасности информационных систем		
A.14.1.1 Анализ и установление требований по информационной безопасности	QMS-27.02.13-Pr Политика управления изменениями	Требования по информационной безопасности должны быть определены, используя различные методы, такие как выделение требований по соответствию из политик и регламентов, моделирование угроз, анализ инцидентов или использование порогов уязвимости. Результаты определения должны быть документированы и рассмотрены всеми заинтересованными сторонами, с целью снижения рисков.
A.14.1.2 Безопасность прикладных услуг в сетях общего пользования	QMS-27.02.04-R Политика использования криптографических методов защиты	Информация, используемая прикладными услугами, передающаяся по общедоступным сетям, должна быть защищена от мошеннических действий, претензий, связанных с нарушениями контрактных обязательств, и несанкционированного раскрытия и изменения.
A.14.1.3 Защита операций прикладных услуг	QMS-27.02.03-R Политика классификации информации	Информация, участвующая в операциях, осуществляемых при пользовании прикладными услугами, должна быть защищена с целью предотвращения незавершенной передачи, неправильной маршрутизации, несанкционированного изменения сообщения, несанкционированного раскрытия, несанкционированного дублирования сообщения или воспроизведения.
A.14.2 Безопасность в процессах разработки и поддержки		
A.14.2.1 Политика безопасности при разработке	QMS-27.02.14-R. Политика безопасности при разработке	Безопасная разработка является требованием при построении защищенных сервисов, архитектуры, программного обеспечения и систем.
A.14.2.2 Процедуры управления системными изменениями	QMS-27.02.13-Pr Политика управления изменениями	С целью снижения рисков, изменения в системах в течение цикла разработки должны быть управляемыми посредством формализованных процедур управления изменениями.
A.14.2.3 Технический анализ приложений после изменений операционной платф	QMS-27.02.14-R. Политика безопасности при разработке	После изменения операционных платформ, критичные бизнес-приложения должны быть проанализированы и протестированы, чтобы гарантировать, что отсутствует негативное влияние на деятельность организации или безопасность.
A.14.2.4 Ограничения на изменения в пакетах программ	QMS-27.02.14-R. Политика безопасности при разработке	Насколько это возможно и практически осуществимо, приобретаемое у поставщика программное обеспечение должно использоваться без изменений. В тех случаях, когда программный пакет требует изменений, должны приниматься во внимание различные риски.

A.14.2.5 Принципы разработки защищенных систем	QMS-27.02.14-R. Политика безопасности при разработке	Процедуры разработки изменений должны использовать методы безопасного проектирования в разработке приложений, имеющих интерфейсы ввода-вывода. Методы безопасного проектирования обеспечивают методическую основу для методов авторизации пользователей, управления защитой сессии и подтверждения правильности данных, удаления отладочных кодов.
A.14.2.6 Безопасная среда разработки	QMS-27.02.14-R. Политика безопасности при разработке	Обеспечение и соответсвующая защита сред разработки и интеграции систем, охватывающий весь цикл разработки.
A.14.2.7 Разработка, переданная на аутсорсинг	QMS-27.02.14-R. Политика безопасности при разработке	Определение требований к атусорсингу разработки, с целью снижения рисков.
A.14.2.8 Тестирование защищенности системы	QMS-27.02.14-R. Политика безопасности при разработке	Новые и обновляемые системы требуют тщательного тестирования и проверки в ходе процессов разработки, включая подготовку детального графика работ, исходных данных для тестирования и ожидаемых в некотором диапазоне условий результатов. При разработке собственными силами такие тесты должны первоначально выполняться Разработчиком. Затем должно выполняться независимое приемочное тестирование (как для разработки собственными силами, так и для переданной на сторону), чтобы гарантировать, что система работает как ожидалось и только как ожидалось. Объем тестирования должен соответствовать важности и характеру системы.
A.14.2.9 Приемочное тестирование системы	QMS-27.02.14-R. Политика безопасности при разработке	С целью снижения рисков, тестирование должно выполняться в реалистичной тестовой среде, чтобы гарантировать, что проверяемая система не внесет уязвимостей в инфраструктуру организации и что результаты тестирования надежны.
A.14.3 Данные для тестирования		
A.14.3.1 Защита данных для тестирования	Неприменимо	
A.15. Отношения с поставщиками		
A.15.1 Информационная безопасность в отношениях с поставщиками		
A.15.1.1 Политика информационной безопасности в отношениях с поставщиками	QMS-27.02.12-Pr. Политика безопасности в отношении поставщиков	Согласование требований с поставщиками и партнерами по информационной безопасности для снижения рисков, связанных с доступом поставщиков к активам организации.
A.15.1.2 Решение вопросов безопасности в соглашениях с поставщиками	QMS-27.02.12-Pr. Политика безопасности в отношении поставщиков	Гарантирование того, что нет разногласий между организацией и поставщиком в отношении взаимных обязательств по выполнению соответствующих требований информационной безопасности.
A.15.1.3 Цепочка поставок информационно-коммуникационных технологий	QMS-27.02.12-Pr. Политика безопасности в отношении поставщиков	Определение правил в отношении безопасности цепочек поставок в отношении получения уверенности в том, что критически важные компоненты и их происхождение могут быть прослежены по всей цепочке поставки.
A.15.2 Управление предоставлением услуги поставщиком		
A.15.2.1 Мониторинг и анализ услуг поставщика	QMS-27.02.12-Pr. Политика безопасности в отношении поставщиков	Поддержание согласованного уровня информационной безопасности и предоставления услуги в соответствии с соглашениями с поставщиком.
A.15.2.2 Управление изменениями в услугах поставщика	QMS-27.02.12-Pr. Политика безопасности в отношении поставщиков	Управление изменениями в предоставлении услуг поставщиками, включая поддержание и улучшение существующих политик информационной безопасности, процедур и средств управления, с учетом критичности бизнес-информации, используемых систем и процессов и повторной оценки рисков с целью их снижения.
A.16. Управление инцидентами информационной безопасности		
A.16.1 Управление инцидентами информационной безопасности и улучшени		
A.16.1.1 Обязанности и процедуры	QMS-27.03.07-I Инструкция сотруднику ДРИП ДОС	Гарантировать последовательный и результативный подход к управлению инцидентами информационной безопасности, включая информирование о событиях, связанных с безопасностью, и уязвимостях, с целью снижения рисков.
A.16.1.2 Оповещение о событиях, связанных с информационной безопасностью	QMS-27.03.07-I Инструкция сотруднику ДРИП ДОС	С целью снижения рисков, оповещение о событиях информационной безопасности должно доводиться по соответствующим каналам управления как можно быстрее.
A.16.1.3 Оповещение об уязвимостях в информационной безопасности	QMS-27.03.08-I Инструкция специалисту по информационной безопасности	Описание процесса, гарантирующего фиксацию и сообщение о любых обнаруженных или предполагаемых уязвимостях в информационной безопасности систем и сервисов.
A.16.1.4 Оценка и решение по событиям информационной безопасности	QMS-27.03.08-I Инструкция специалисту по информационной безопасности	Оценка и дальнейшее принятие решения, следует ли рассматриваемое событие классифицировать как инцидент информационной безопасности.
A.16.1.5 Ответные меры на инциденты информационной безопасности	QMS-27.03.02-Pr Управление инцидентами информационной безопасности	Первоочередной целью ответных мер на инцидент является возвращение «нормального уровня безопасности» и затем инициирование необходимого восстановления.
A.16.1.6 Излечение уроков из инцидентов информационной безопасности	QMS-27.03.02-Pr Управление инцидентами информационной безопасности QMS-27.03.04-R. План восстановления данных после аварии	Знания, полученные из анализа и разрешения инцидентов информационной безопасности, используются для уменьшения вероятности инцидентов в будущем или их воздействия.
A.16.1.7 Сбор свидетельств	QMS-27.03.08-I Инструкция специалисту по информационной безопасности QMS-27.03.07-I Инструкция сотруднику ДРИП ДОС QMS-27.03.04-R. План восстановления данных после аварии	Когда инцидент информационной безопасности обнаружен впервые, неясно, приведет ли это событие к судебному разбирательству. Таким образом, существует опасность, что необходимое свидетельство будет намеренно или случайно уничтожено до того, как выяснится серьезность инцидента, соответственно, для снижения рисков, необходим сбор
A.17. Аспекты информационной безопасности в менеджменте непрерывнос		
A.17.1 Непрерывность информационной безопасности		
A.17.1.1 Планирование непрерывности информационной безопасности	QMS-27.03.04-R. План восстановления данных после аварии	Для снижения затрат времени и усилий на «дополнительный» анализ влияния информационной безопасности на бизнес определяются аспекты информационной безопасности в рамках общего менеджмента непрерывностью бизнеса или анализа влияния на бизнес в рамках управления восстановлением после чрезвычайной ситуации и четкое формулирование требований непрерывности информационной безопасности в рамках процессов управления непрерывностью бизнеса или управления восстановлением после чрезвычайной ситуации.
A.17.1.2 Обеспечение непрерывности информационной безопасности	QMS-27.03.04-R. План восстановления данных после аварии	Определение конкретных процессов и процедур, в рамках контекста обеспечения непрерывности бизнеса или восстановления после чрезвычайной ситуации, с целью снижения рисков.
A.17.1.3 Проверка, анализ и оценка непрерывности информационной безопаснос	QMS-27.03.08-I Инструкция специалисту по информационной безопасности	Проверка разработанных и внедренных средств управления непрерывностью информационной безопасности через определенные интервалы времени, с целью гарантирования, что эти средства пригодны и результативны во время неблагоприятных ситуаций.
A.17.2 Резервирование		
A.17.2.1 Возможность применения средств обработки информации	QMS-27.03.06-Pr Управление физической безопасностью и защита от природных угроз	Определение требований избыточности, достаточной для обеспечения заданного уровня надежности.
A.18. Соответствие		
A.18.1 Соответствие законодательным и контрактным требованиям		
A.18.1.1 Определение действующих законодательных и контрактных требований	QMS-27.02.12-Pr Политика безопасности в отношении поставщиков	Избегание нарушений законодательных, нормативных или контрактных обязательств, имеющих отношение к информационной безопасности, и любых требований безопасности, с целью снижения рисков.
A.18.1.2 Права интеллектуальной собственности	QMS-27.03.07-I Инструкция сотруднику ДРИП ДОС QMS-27.01.10-R Требования к набору и компетентности персонала	Доведение до персонала важности и необходимости осознания прав интеллектуальной собственности на программное обеспечение, разрабатываемое в организации.
A.18.1.3 Защита записей	QMS-27.02.15-Pr Политика ведения журналов и мониторинга	Защита записей с целью защиты от потери, повреждения, фальсификации, несанкционированного доступа и несанкционированной публикации в соответствии с законодательными, нормативными, контрактными требованиями и требованиями бизнеса.
A.18.1.4 Конфиденциальность и защита персональных данных	QMS-27.01.10-R Требования к набору и компетентности персонала	Определение необходимой меры обеспечения конфиденциальности и защиты персональных данных, согласно требованиям законодательства.
A.18.1.5 Регламентация применения криптографических методов	QMS-27.02.04-R Политика использования криптографических методов защиты	Регламентирование применения криптографических методов в соответствии с действующими соглашениями, законодательными и нормативными актами.
A.18.2 Анализ информационной безопасности		
A.18.2.1 Независимый анализ информационной безопасности	QMS-27.03.08-I Инструкция специалисту по информационной безопасности	Гарантирование того, что средства обеспечения информационной безопасности внедрены и используются в соответствии с организационной политикой и процедурами.
A.18.2.2 Соответствие политикам безопасности и стандартам	QMS-27.03.08-I Инструкция специалисту по информационной безопасности	Определение того, каким образом анализировать выполнение требований информационной безопасности, определенных в политиках, стандартах и других действующих нормах.
A.18.2.3 Анализ технического соответствия	QMS-27.03.08-I Инструкция специалисту по информационной безопасности	Регулярный анализ на соответствие политикам и стандартам информационной безопасности организации, с целью минимизации рисков.
A.5. Политики информационной безопасности		
A.5.1. Ориентация менеджмента на информационную безопасность		
A.5.1.1. Политики информационной безопасности	QMS-27.03.08-I Инструкция специалисту по информационной безопасности	Обеспечение ориентации менеджмента и поддержки информационной безопасности в соответствии с требованиями бизнеса и соответствующими законодательными и нормативными требованиями.
A.5.1.2 Пересмотр политик информационной безопасности	QMS-27.03.08-I Инструкция специалисту по информационной безопасности	Гарантирование постоянной пригодности , соответствия и результативности политик информационной безопасности для
A.6. Организация информационной безопасности		
A.6.1 Внутренняя организация		
A.6.1.1 Должностные функции и обязанности, связанные с информационной безо	QMS-27.03.08-I Инструкция специалисту по информационной безопасности	Формирование основных элементов управления для инициирования и контроля внедрения и эксплуатации средств защиты информации в ДОС для снижения рисков.
A.6.1.2 Разделение обязанностей	QMS-27.02.02-Pr Политика контроля доступа	Разделение вступающих в противоречие друг с другом обязанностей и областей ответсвтенности, для снижения возможности несанкционированного или ненамеренного изменения или неправильного применения авктиво организации.
A.6.1.3 Контакты с полномочными органами	QMS-27.03.08-I Инструкция специалисту по информационной безопасности	Организации должны иметь процедуры, которые определяют, когда и через кого будет осуществляться контакт с полномочным органом (например, правоохранительными органами, контролирующими и надзорными органами) и каким образом выявленная информация по инцидентам информационной безопасности должна будет своевременно передаваться (например, если есть подозрение на возможное нарушение закона).
A.6.1.4 Контакты с профессиональными сообществами	QMS-27.03.08-I Инструкция специалисту по информационной безопасности	Расширение знаний о лучших практиках и получения самой последней информации в области информационной безопасности; Гарантирование того, что представление об аспектах информационной безопасности является актуальным и полным; Раннее получение предупреждений об опасности, информационных бюллетеней и патчей, касающихся атак и уязвимостей; Обеспечение возможности получения советов от специалистов по информационной безопасности; Опубликование и обмен информацией о новых технологиях, продуктах, угрозах или уязвимостях; Обеспечение соответствующих контактов при обработке инцидентов информационной безопасности.
A.6.1.5 Информационная безопасность в управлении проектами	QMS-27.02.13-Pr Политика управления изменениями	Меры по обеспечению информационной безопасности должны быть интегрированы в методы управления проектами в организации, чтобы гарантировать, что риски информационной безопасности выявлены и обработаны в рамках проекта.
A.6.2 Мобильные устройства и удаленная работа		
A.6.2.1 Политика в отношении мобильных устройств	QMS-27.02.09-R. Политика в отношении мобильных устройств и удаленной работ	Принятие во внимание рисков использования мобильных устройств в незащищенных средах для их снижения.
A.6.2.2 Удаленная работа	QMS-27.02.09-R. Политика в отношении мобильных устройств и удаленной работ	Определение условий и ограничений для дистанционной работы, там где это применимо и допустимо с точки зрения законодательных требований, для снижения рисков нарушения конфиденциальности, доступности и целостности.
A.7. Безопасность персонала		
A.7.1 До приема на работу		
A.7.1.1 Предварительная проверка	QMS-27.01.10-R Требования к набору и компетентности персонала	Гарантирование того, что проверка при приеме на работу, осуществляемая для всех кандидатов, должна проводиться в рамках соответствующих законодательных актов, регламентов и этических норм, а также должна быть соразмерна бизнес-требованиям, категории информации по классификации, к которой предполагается доступ, и предполагаемым рискам.
A.7.1.2 Условия трудового соглашения	QMS-27.01.10-R Требования к набору и компетентности персонала	Описание контрактных обязательств для сотрудников или работающих по контракту для снижения рисков.
A.7.2 В период занятости		
A.7.2.1 Ответственность руководства	QMS-27.03.07-I Инструкция сотруднику ДРИП ДОС QMS-27.03.08-I Инструкция специалисту по информационной безопасности	Гарантирование того, что сотрудники и работающие по контракту знают и выполняют свои обязанности, связанные с информационной безопасностью.
A.7.2.2 Осведомленность, образование и обучение в сфере информационной без	QMS-27.03.08-I Инструкция специалисту по информационной безопасности	Гарантирование того, что все сотрудники организации и, там, где это существенно, работающие по контракту соответствующим образом информированы и обучены, а также регулярно извещаются об изменениях в политиках и процедурах организации, в той мере, насколько это важно для исполнения их служебных обязанностей.
A.7.2.3 Дисциплинарные меры	QMS-27.01.10-R Требования к набору и компетентности персонала	Доведение до сведения персонала процесса для принятия мер к тем сотрудникам, которые допустили нарушение требований информационной безопасности.
A.7.3 Прекращение и изменение трудовых отношений		
A.7.3.1 Освобождение от обязанностей или их изменение	QMS-27.01.10-R Требования к набору и компетентности персонала	Обеспечение выполнения обязанностей в отношении информационной безопасности, остающихся в силе после прекращения или изменения трудовых отношений.
A.8. Управление активами		
A.8.1 Ответственность за активы		
A.8.1.1 Инвентаризация активов	QMS-27.03.01-P Управление активами и техническими уязвимостями	Реестры активов способствуют обеспечению результативной защиты и могут быть также востребованы для других целей, таких как охрана здоровья и труда, страхование или финансы (менеджмент активов).
A.8.1.2 Владение активами	QMS-27.03.01-P Управление активами и техническими уязвимостями	Определение утвержденной ответственности отдельных лиц, равно как и подразделений, за актив в течение его жизненного цикла для их защиты и контроля.
A.8.1.3 Надлежащее использование активов	QMS-27.03.01-P Управление активами и техническими уязвимостями	Сотрудники и внешние пользователи, использующие или имеющие доступ к активам организации, должны быть осведомлены о требованиях информационной безопасности, относящихся к информации и другим активам организации, которые связаны с информацией, устройствами и ресурсами для обработки информации. Они должны нести ответственность за применение ими любых ресурсов обработки информации и любое подобное использование, осуществляемое в зоне их ответственности.

A.8.1.4 Возврат активов	QMS-27.03.01-P Управление активами и техническими уязвимостями	Процесс прекращения трудовых отношений установлен так, чтобы включать в себя возврат всех ранее выданных физических или электронных активов, принадлежащих или доверенных организации.
A.8.2 Классификация информации		
A.8.2.1 Классификация информации	QMS-27.02.03-R. Политика классификации информации	Классификация и связанные с нею методы защиты информации должны учитывать потребности бизнеса в обмене информацией или ограничения доступа к ней, равно как и законодательные требования.
A.8.2.2 Маркировка информации	QMS-27.02.03-R. Политика классификации информации	Руководящие указания, где и как размещается маркировка, с учетом того, каким образом осуществляется доступ к информации или способов использования активов, зависящих от типа носителя. Определение ситуаций, когда маркировка (во избежании лишних трат) не требуется для информации не являющейся конфиденциальной.
A.8.2.3 Обращение с активами	QMS-27.02.03-R. Политика классификации информации	Описание процедур для обращения, обработки, хранения и передачи информации в соответствии с классом информации.
A.8.3 Обращение с носителями информации		
A.8.3.1 Управление съемными носителями	Неприменимо	
A.8.3.2 Утилизация носителей информации	QMS-27.02.11-R. Политика уничтожения и утилизации	Установление формальных процедур для надежной утилизации носителей с целью минимизации риска утечки защищаемой
A.8.3.3 Физическое перемещение носителей информации	Неприменимо	
A.9. Контроль доступа		
A.9.1 Диктуемые бизнесом требования к контролю доступа		
A.9.1.1 Политика контроля доступа	QMS-27.02.02-Pr. Политика контроля доступа	Определение соответствующих правил для контроля доступа, права доступа и ограничения для определенных категорий пользователей по отношению к их активам с уровнем детализации и строгости контроля, отражающей риски, связанные с информационной безопасностью.
A.9.1.2 Доступ к сетям и сетевым службам	QMS-27.02.02-Pr. Политика контроля доступа	Пользователи должны получать доступ только к тем сетям и сетевым службам, для которых у них есть авторизация для снижения
A.9.2 Управление доступом пользователей		
A.9.2.1 Регистрация и отмена регистрации пользователя	QMS-27.02.02-Pr. Политика контроля доступа QMS-27.02.07-R. Парольная политика	Обеспечение формализованным процессом регистрации и отмены регистрации пользователей, обеспечивающий возможность назначения прав доступа для снижения рисков.
A.9.2.2 Предоставление доступа пользователю	QMS-27.02.02-Pr. Политика контроля доступа	Обеспечение формализованным процессом предоставления доступа пользователям для назначения или отмены прав всем
A.9.2.3 Управление привилегированными правами доступа	QMS-27.02.02-Pr. Политика контроля доступа	Обеспечение формализованным процессом авторизации в соответствии с действующей политикой контроля доступа для
A.9.2.4 Управление секретной информацией аутентификации пользователей	QMS-27.02.07-R. Парольная политика	Обеспечение формализованным процессом управления присваивания секретной информации аутентификации пользователей
A.9.2.5 Пересмотр прав доступа пользователей	QMS-27.02.02-Pr. Политика контроля доступа	Компенсация возможных слабых мест в выполнении методов реализации регистрации, отмены и предоставления доступа для
A.9.2.6 Отмена или изменение прав доступа	QMS-27.02.02-Pr. Политика контроля доступа	После завершения трудовых отношений права доступа пользователя к информации и активам, связанным с устройствами обработки информации и службами, должны быть отменены или приостановлены для снижения рисков.
A.9.3 Обязанности пользователей		
A.9.3.1 Использование секретной информации аутентификации	QMS-27.02.07-R. Парольная политика	Опередение обязательств пользователей при использовании секретной аутентификационной информации для снижения
A.9.4 Контроль доступа к системе и приложениям		
A.9.4.1 Ограничение доступа к информации	QMS-27.02.02-Pr. Политика контроля доступа	Ограничение доступа, основанное на требованиях конкретных бизнес-приложений и установление требований для снижения
A.9.4.2 Безопасные процедуры входа в систему	QMS-27.02.07-R. Парольная политика	Определение строгости процедуры авторизации пользователя должна соответствующей классу информации, к которой
A.9.4.3 Система управления паролями	QMS-27.02.07-R. Парольная политика	Обеспечение "диалога" и надлежащего качества генерации паролей для снижения рисков.
A.9.4.4 Использование утилит с привилегированными правами	QMS-27.02.02-Pr. Политика контроля доступа	Контроль назначения и использования утилит с привилигированными правами для снижения рисков.
A.9.4.5 Контроль доступа к исходным кодам	QMS-27.02.14-R Политика безопасности при разработке	Строгий контроль доступа к исходным кодам программ с целью предотвращения включения в него несанкционированной