Общество с ограниченной ответственностью
«РТ Медицинские
Информационные Системы»
(ООО «РТ МИС»)

УТВЕРЖДАЮ:
Генеральный директор

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат 42d0911f6880f58a4bd411be7c67424505123095
Владелец **Зима Дмитрий Петрович**
Действителен с 12.04.2024 по 12.07.2025

12.11.2024 № ЛНА.2024-18

г. Пермь

Д.П. Зима

Регламент работы подрядчиков на тестовых стендах ООО «РТ МИС»

РЕДАКЦИЯ:	1
РАЗРАБОТАН:	Отдел информационной безопасности
ВВЕДЕНО В ДЕЙСТВИЕ:	С даты подписания приказа ООО «РТ МИС» от 12.11.2024 № 11-2024-002/ОД
ВЗАМЕН:	Утверждается впервые
В КАКИЕ ЧАСТИ ВНЕСЕНЫ ИЗМЕНЕНИЯ (по сравнению с предыдущей версией):	

Содержание

1. Назначение

Настоящий регламент работы подрядчиков на тестовых стендах ООО «РТ МИС» (далее – регламент) устанавливает требования, предъявляемые ООО «РТ МИС» (далее - Общество) к третьим лицам/подрядчикам (далее - подрядчик) и необходимые для обеспечения информационной безопасности и защиты интересов Общества при использовании подрядчиками информационных активов Общества. Регламент применим ко всем подрядчикам и их субподрядчикам, которые хранят, обрабатывают информацию на информационных ресурсах Общества или имеют доступ к инфраструктуре Общества. Любые дополнительные обязательства подрядчика в отношении информационной безопасности по любому соглашению с Обществом являются дополнением к требованиям, изложенным в настоящем регламенте.

Настоящий регламент вводится в действие впервые с даты его утверждения.

2. Общие положения

2.1 Область применения

Требования настоящего регламента распространяются на подрядчиков, субподрядчиков и отдел информационной безопасности (далее – ОИБ) Общества.

2.2 Нормативные ссылки

В регламент разработан на основании требований, следующих нормативных документов:

– Федеральный закон от 27.07.2006 №149-ФЗ Об информации, информационных технологиях и о защите информации;

– Федеральный закон от 27.07.2006 №152-ФЗ О персональных данных;

– Федеральный закон от 26.07.2017 №187-ФЗ О безопасности критической информационной инфраструктуры Российской Федерации;

– Информационное сообщение ФСТЭК России №240-24-3057 от 23.06.2021 Об утверждении Требований по безопасности информации к средствам обеспечения безопасной дистанционной работы в информационных (автоматизированных) системах;

– Концепция информационной безопасности в сфере здравоохранения (утв. протоколом президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 10.03.2022 №7);

– ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования».

В регламенте использованы ссылки на следующие нормативные документы:

– ЛНА №ЛНА.2024-01 Политика информационной безопасности;

– ЛНА №ЛНА.2024-05 Положение о правилах доступа к значимым объектам критической информационной инфраструктуры;

– ЛНА №ЛНА.2023-12 Регламент предоставления прав доступа подрядчикам;

– ЛНА №ЛНА.2024-04 Регламент парольной защиты ООО РТ МИС;

– ЛНА №ЛНА.2023-08 Регламент резервного копирования и восстановления;

– ВНД №Р.УП4.1-7-2024 Регламент процесса управления уязвимостями;

– ВНД №Р.УП4.1-1-2023 Руководство по безопасной разработке;
– ВНД №П.УП4.1-3-2024 Положение об управлении антивирусной защитой.

2.3 Термины и сокращения

Для целей регламента в нем используются термины, определенные в Глоссарии терминов и определений ООО «РТ МИС», а также следующие термины:

Термин	Определение
База данных	упорядоченный набор структурированной информации или данных, которые обычно хранятся в электронном виде в компьютерной системе
Демилитаризованная зона	экранированный сегмент информационной системы, размещенный на ее внешней границе и выполняющий функции «нейтральной зоны» (буферной зоны безопасности) между защищаемой информационной системой оператора и внешней информационной системой или информационно - телекоммуникационной сетью
Информационный обмен	порядок информационного обмена в рамках эксплуатации информационных систем между Обществом и Подрядчиком и требования к нему
Непрерывность бизнеса	обеспечение непрерывности деятельности и восстановления работоспособности инфраструктуры Общества
Облачная среда	технологии распределенной обработки цифровых данных, с помощью которых компьютерные ресурсы предоставляются интернет-пользователю как онлайн-сервис
Обезличенные данные	данные, хранимые в информационных системах в электронном виде, принадлежность которых конкретному субъекту персональных данных невозможно определить без дополнительной информации;
Персональные данные	любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных)
Подрядчик	исполнитель по договору
Регрессионное тестирование	набор тестов, направленных на обнаружение дефектов в уже протестированных участках приложения
Государственный регулятор	ФСТЭК, ФСБ, Роскомнадзор, Министерство цифрового развития, связи и массовых коммуникаций РФ
Тестовый стенд	среда для непромышленной эксплуатации, проверки, отладки программного комплекса
Коммерческая тайна	режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду

Для целей регламента в нем используются сокращения, определенные в Глоссарии терминов и определений ООО «РТ МИС», а также следующие сокращения:

Сокращение	Расшифровка
2FA	многофакторная аутентификация
ИБ	Информационная безопасность
ЦОД (центр обработки данных)	физическое местоположение, в котором хранятся вычислительные машины и связанное с ними аппаратное оборудование

3. Основные положения

3.1 Общие положения

В контексте настоящего регламента термин «информация» включает как конфиденциальную информацию, так и персональные данные, используемые в процессе осуществления коммерческой деятельности (далее по отдельности и (или) совместно именуемая - информация). Персональные данные означают любую информацию, относящуюся прямо или косвенно к определенному или определяемому лицу (п. 1 ст. 3 Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных»). Требования к уровням конфиденциальности информации определяются в договоре между Подрядчиком и Обществом.

Требования настоящего регламента применимы ко всей информации, обрабатываемой подрядчиком, в том числе, обрабатываемой при:

- создании;
- редактировании;
- управлении;
- получении доступа;
- получении;
- передаче;
- уничтожении;
- хранении или размещении на серверах в любом формате, в том числе, среди прочего:
  - в информационных системах;
  - в базах данных;
  - в облачной среде;
  - в тестовой и продуктивной среде;
  - в ресурсах, находящихся в памяти ЭВМ и на электронных устройствах (включая предоставленные Обществом устройства и устройства, используемые в соответствии с Политикой информационной безопасности Общества);
- версий такой информации на неэлектронных носителях.

Общество оставляет за собой право проводить проверку подрядчиков и их субподрядчиков, если они не предоставляют гарантий соответствия требованиям Общества на ежегодной основе. В случае, когда Общество имеет разумные основания для подозрений подрядчика в осуществлении мошенничества или серьезного нарушения требований обработки информации, то проверка проводится в любое время с предварительным письменным уведомлением подрядчика не менее чем за 10 (десять) рабочих дней.

Общество вправе приостановить доступ к информации Общества работнику Подрядчика в случае нарушения им требований настоящего регламента.

Подрядчик по запросу Обществу, в сроки, указанные в таком запросе, обязан предоставлять информацию и данные касающиеся, включая (но не ограничиваясь):

- обзора политик, процессов и процедур;
- оценки механизмов обеспечения информационной безопасности (физической безопасности и конфиденциальности информации).

Критерии проведения проверки включают соблюдение подрядчиком требований информационной безопасности, определенных настоящим регламентом.

3.2 Правила и процедуры обеспечения информационной безопасности

Подрядчик должен принять и соблюдать задокументированные политики, регламенты и процедуры в отношении информационной безопасности в целях создания контролируемой среды (далее - среда), связанной с защитой конфиденциальности, целостности и доступности информации. Политики и процедуры подлежат ежегодному пересмотру, обновлению и утверждению высшим руководством подрядчика.

Если подрядчик разрешает использование личных устройств для доступа к информации или системам Общества, то ему необходимо внедрить «Политику использования сотрудниками личных устройств».

3.3 Руководство и обучение

Работники подрядчика должны пройти соответствующее обучение по утвержденной им программе в области обеспечения информационной безопасности, включая требования к защите и безопасной работе с информацией. Материалы программы обучения должны периодически пересматриваться и обновляться. По запросу Общества необходимо предоставлять краткий обзор завершенного обучения.

При заключении договора подрядчик обязуется определить своего представителя в качестве единственного контактного лица по всем вопросам, связанным с информационной безопасностью. В дополнение подрядчик должен определить представителя, ответственного за контроль соблюдения настоящего регламента.

3.4 Правила обеспечения ИБ со стороны кадровых ресурсов

Подрядчик должен обеспечить подписание своими работниками до начала работ по договору «Обязательство о неразглашении сведений конфиденциального характера». Форма такого обязательства устанавливается подрядчиком, но должна содержать как минимум положения установленные, на официальном сайте Роскомнадзора по адресу: https://54.rkn.gov.ru/protection/docsamples/p3235/.

При получении от Общества информации о внесении изменений в настоящий регламент и размещении таких изменений (или новых версий регламента) на сайте Общества, подрядчик должен довести такие изменения до своих работников и субподрядчиков под подпись в течении 10 р.д.

3.5 Доступ к информации

Идентификаторы (учетные записи) предоставляются подрядчику, в порядке, предписанном в «Регламенте предоставления прав доступа подрядчикам Общества».

Подрядчик должен обеспечивать, как минимум, следующие меры контроля доступа к ресурсам Общества: когда подрядчик обладает информацией, принадлежащей или доверенной Обществом и находящейся за пределами среды Общества, и (или) когда подрядчик устанавливает удаленное подключение к среде Общества:

– процесс официального утверждения, с тем чтобы предоставление доступа осуществлялось, исходя из рабочей потребности по выполнению должностных обязанностей (т.е. наделение минимальным объемом полномочий, исключительно исходя из необходимого уровня доступа, но не больше);

– учетные записи для доступа к среде Общества должны закрепляться за каждым отдельным пользователем и быть уникальными;

– привилегированные и административные учетные записи должны отличаться от регламентной учетной записи пользователя и иметь уникальные идентификационные данные для входа. Привилегированные учетные записи (с повышенным уровнем доступа, который дает полномочия внутри компьютерной системы, значительно более обширные, чем те, что доступны обычному пользователю) должны предоставляться только ограниченному кругу уполномоченных пользователей.

– контроль паролей должен быть надлежащим образом реализован Подрядчиком, включая следующие требования:

- пароли с периодически истекающим сроком действия;
- защищенная передача временных паролей и напоминание о необходимости их замены после первого использования;
- замена пароля незамедлительно при возникновении оснований полагать, что учетная запись была скомпрометирована;
- пароли общей системы, сервиса и приложения должны меняться каждый раз, когда кто-то, кто знает пароль, либо уходит из организации Подрядчика, либо переходит на другую должность, в рамках которой доступ к системе больше не требуется;
- перед сбросом пароля необходимо проверять личность пользователя;
- необходимо заменять все пароли, установленные по умолчанию;
- требования по надежности пароля должны отвечать «Регламенту парольной защиты» Общества в отношении их длины и сложности.

Подрядчик должен применять следующие меры контроля деактивации:

– формальный процесс своевременной деактивации учетных записей пользователей, уходящих из организации подрядчика и (или) больше не испытывающих рабочей потребности входить в систему (например, в течение 24 часов с момента такого события);

– процесс, обеспечивающий направление уведомления Общества относительно изменений в составе работников подрядчика в течение 24 часов с момента такого события, если такие работники имеют учетные записи или им предоставлен доступ к информационным системам Общества.

Подрядчик должен реализовать следующие средства контроля доступа:

– периодические проверки доступа для всех пользователей, системных учетных записей, тестовых учетных записей и общих учетных записей должны производиться и документироваться по меньшей мере раз в год;

– учетные записи пользователя должны блокироваться после определенного количества неудачных попыток входа;

– учетные записи, по которым в последнее время не было зафиксировано никаких операций (например, за последние 90 дней, за исключением тех, что используются для ежеквартальной, полугодовой и годовой обработки), должны быть отключены;

– должны применяться меры контроля сессий, включая блокировку учетной записи и истечение срока сессии;

– для любых привилегированных и (или) административных учетных записей должна быть предусмотрена 2FA;

– необходимо использовать 2FA в отношении любых онлайн-приложений;

– 2FA также применима для всех способов удаленного доступа (например, виртуальных частных сетей, протоколов удаленного рабочего стола).

3.6 Сетевая и системная безопасность

Подрядчик должен применять, как минимум, следующие меры сетевой и системной безопасности, когда подрядчик обладает информацией, принадлежащей или доверенной Обществом и находящейся за пределами среды Общества, и (или) когда подрядчик устанавливает удаленное подключение к среде Общества:

– регламенты защиты операционных систем, приложений и сетевых устройств;

– во все системы должны быть внесены соответствующие исправления с учетом обновлений операционной системы и ее основных компонентов и оценкой в соответствии с общепринятыми регламентами безопасности;

– исправление уязвимостей онлайн-приложений с высоким уровнем риска должно быть проведено как можно скорее, но не более, чем за 30 дней;

– техническое обслуживание систем должно осуществляться на уровне, позволяющем вносить последние обновления/внедрять сервисные пакеты;

Меры контроля сетевой безопасности:

– информация, принадлежащая или доверенная Обществом, не должна храниться в демилитаризованной зоне;

– на всех сетевых интерфейсах должны быть установлены межсетевые экраны, ограничивающие входящий и исходящий трафик, исходя из текущих потребностей;

– необходимо установить системы обнаружения или предупреждения несанкционированного доступа в целях выявления и реагирования на несанкционированное или вредоносное сетевое вторжение;

– доступ к среде Общества должен осуществляться только с информационных систем и/или оборудования, включая облачные сервисы, расположенных исключительно на территории Российской Федерации.

– трафик при передаче информации должен осуществляться только между информационными системами и/или оборудованием, включая облачные сервисы, расположенными исключительно на территории Российской Федерации.

Меры контроля системной безопасности:

– пользовательские устройства (ноутбуки) должны быть зашифрованы и защищены паролем;

– корпоративные мобильные устройства (смартфоны, планшеты) должны быть защищены с использованием системы управления мобильными устройствами;

– серверы и конечные точки должны быть защищены от воздействия вирусов/вредоносного программного обеспечения.

3.7 Вход и мониторинг

Операции по входу в информационные системы подрядчика должны протоколироваться и осуществляться в соответствии с общими регламентами безопасности. Мониторинг должен выявлять события информационной безопасности и проверять эффективность защитных мер.

3.8 Управление угрозами и уязвимостями

Подрядчик должен проводить непрерывную оценку уязвимостей и своевременно исправлять проблемы, связанные с приложениями, операционными системами и прочими компонентами инфраструктуры. В дополнение необходимо внедрить сервисы и процессы для выявления, оценки, смягчения и защиты от новых и существующих уязвимостей, и угроз безопасности, включая вирусы, боты и прочие вредоносные коды.

Подрядчик должен применять следующие меры контроля:

– ежегодные независимые проверки на проникновение в их сети и приложения, отвечающие за обработку Информации;

– ежеквартальный поиск уязвимостей в системе безопасности своих платформ и сетей, которые обрабатывают Информацию, в целях обеспечения соответствия общепринятым регламентам по конфигурированию настроек безопасности платформ и сетей;

– риск-ориентированную программу по устранению уязвимостей, направленную на реагирование на результаты проверок на проникновение, уязвимости и оценки нормативно-правового соответствия;

– при необходимости подрядчик должен обеспечить Обществу на условиях, указанных в запросе, возможность проведения теста защиты информационных систем от несанкционированного доступа.

3.9 Управление изменениями

Подрядчик должен задокументировать и принять политику контроля за внесением изменений, которая включает в себя:

– требования к утверждению, классификации, тестированию и испытанию плана восстановления предыдущего состояния;

– разделение обязанностей по направлениям: запрос, утверждение и реализация изменений;

– управление и обзор экстренных изменений в течение установленного периода (24 часа).

3.10 Управление активами

Подрядчик должен обеспечивать проведение инвентаризации активов, включая системы/устройства и программное обеспечение, когда подрядчик обладает информацией, принадлежащей или доверенной Обществом и находящейся за пределами среды Общества, и (или) когда у подрядчика есть удаленное подключение к среде Общества.

3.11 Обработка информации

Подрядчик обязан проводить анализ информации, содержащей персональные данные на предмет обезличенности субъектов персональных данных, перед внедрением ее в среду Общества. Обработка не обезличенной информации допускается только, если иное не определено договором, либо иными взаимными нормативными актами.

Подрядчик должен обеспечить отделение информации Общества от информации прочих контрагентов, если у подрядчика имеется информация, принадлежащая или доверенная Обществом, находящаяся за пределами среды Общества, и (или) если у подрядчика есть удаленный доступ к среде Общества. Кроме того, подрядчик должен составить документальное описание прохождения информации через его среду по запросу Общества.

Электронный обмен информацией между Обществом и подрядчиком (в том числе по электронной почте, путем передачи файлов, через удаленное подключение и т.д.) должен быть защищен с помощью взаимно согласованных сервисов.

Необходимо использовать процессы и инструменты для обнаружения и реагирования на утечку информации.

Информация не должна храниться или передаваться с использованием портативных устройств хранения без официального разрешения владельца - Общества (полученного посредством процесса направления запроса в Общество об использовании портативных устройств хранения данных). В случае использования таких устройств вся хранящаяся на них Информация должна быть зашифрована.

3.12 Физическая безопасность

Необходимо разработать и применять процедуры и физические средства контроля для защиты копий информации на бумажных носителях и в информационных системах (например, аппаратное обеспечение, программное обеспечение, документация и данные), если у подрядчика имеется информация, принадлежащая или доверенная Обществом, находящаяся за пределами среды Общества, и (или) если у подрядчика есть удаленный доступ к среде Общества.

ЦОД подрядчика должен находиться под физическим контролем, включая формальное управление доступом в зависимости от рабочих потребностей. В ЦОД должны применяться меры контроля среды (температуры, влажности, резервный источник энергии) в целях предупреждения перебоев или утраты данных.

Подрядчик, который передает, хранит или обрабатывает информацию, принадлежащую Обществу, должен проводить ежегодную независимую оценку физической безопасности своих объектов.

3.13 Непрерывность бизнеса

В дополнение к любым договорным требованиям относительно непрерывности бизнеса и послеаварийного восстановления в случае аварии или перебоев в работе, с учетом прочих требований соглашения и степени критичности информации, подрядчик должен гарантировать наличие следующих мер контроля:

– на объекте первичной обработки данных (входные каналы связи, серверы, терминалы) должно быть в наличии резервное питание и резервные технические возможности обработки;

– альтернативной площадки для обработки Информации в целях продолжения рабочих процессов и восстановления функциональности организации подрядчика в указанный временной период по соглашению, если применимо;

– ежегодной проверки отказоустойчивости в целях демонстрации эффективной способности к непрерывности ведения бизнеса и восстановлению;

– регулярное резервное копирование применяемых систем и данных в зависимости от уровня критичности. Необходимо периодически проверять данные после резервного копирования на устойчивость к текущим условиям применения;

– надлежащую защиту резервных копий и (или) передаваемой информации, а также их хранение отдельно от основного хранилища.

3.14 Хранение и уничтожение информации

Подрядчик должен хранить информацию только в течение срока, установленного в договоре, кроме случаев, когда по закону требуется более длительное хранение.

При истечении срока действия подрядчик должен вернуть и гарантированно удалить информацию.

По запросу Общества, подрядчик должен подтвердить, что информация была уничтожена, предъявив:

– акт об уничтожении информации;

– выгрузку из журналов информационных систем.

3.15 Управление инцидентами информационной безопасности

Подрядчик должен иметь процедуры управления и реагирования на инциденты в области информационной безопасности (например, раскрытие, нарушение требований конфиденциальности, хищение и т.д.), которые позволяют обоснованно выявлять, расследовать, реагировать, устранять и уведомлять о событиях, которые предполагают наличие определенной угрозы для конфиденциальности, целостности и (или) доступности информации, когда подрядчик обладает информацией, принадлежащей или доверенной Обществом и находящейся за пределами среды Общества, и (или) когда подрядчик устанавливает удаленное подключение к среде Общества. Процедуры реагирования и управления инцидентами должны документироваться и пересматриваться по меньшей мере 1 раз в год. Общество должно иметь возможность изучать такие процедуры по запросу.

Подрядчик должен уведомлять Общество в течение 24 часов о предположительных или известных инцидентах в области информационной безопасности, которые могут оказывать воздействие на информацию. В дополнение подрядчик должен использовать задокументированный процесс, включая определенных контактных лиц со стороны Общества и подрядчика, в целях обеспечения соблюдения данного требования о направлении уведомления.

Подрядчик должен в полной мере сотрудничать с Обществом для прояснения ситуации, понимания ключевых причин и определения необходимых действий для устранения таких причин в случае фактического или предполагаемого инцидента, связанного с информационной безопасностью.

3.16 Управление субподрядчиками

Настоящий регламент применяется ко всем субподрядчикам, используемым подрядчиком, которые работают с информацией, принадлежащей или доверенной Обществом и находящейся за пределами среды Общества, и (или) когда подрядчик устанавливает удаленное подключение к среде Общества. Подрядчик несет ответственность за то, чтобы обеспечивать уведомление каждого субподрядчика о содержании настоящего регламента и его соблюдение субподрядчиком. Во избежание сомнений, к субподрядчикам относятся, помимо прочего, подрядчики, оказывающие копировально-множительные услуги, услуги внешнего хранения (архивы), разработчики программного обеспечения, объекты облачного хранения и ЦОД.

Подрядчик и субподрядчики должны заключать официальные договоры, в которых описаны необходимые меры контроля, включая меры контроля за обеспечением конфиденциальности, доступности и целостности информации.

Подрядчику необходимо проводить первоначальные и текущие оценки в целях обеспечения соблюдения субподрядчиками настоящего регламента и надлежащего управления происшествиями и проблемами в области безопасности.

Подрядчик должен информировать Общество и получать письменное одобрение перед использованием услуг субподрядчиков, которые либо намереваются работать с информацией, либо будут иметь доступ к системам Подрядчика или Общества, в которых находится информация, а также уведомлять Общество о том, в какой стране(ах) будет осуществляться работа с информацией.

3.17 Право на проверку обеспечения мер ИБ

Подрядчик должен разрешать Обществу и государственным регуляторам проводить инспектирования, изучать и проверять объекты информатизации, системы, записи, реестры доступа, данные, практики и процедуры подрядчика (и любых субподрядчиков, услуги которых может использовать Подрядчик) в целях проверки целостности информации и мониторинга соблюдения настоящего регламента.

3.18 Жизненный цикл безопасной разработки системы

Требования к методологии проектирования и разработки безопасного программного обеспечения:

– определенная методология разработки систем должна быть официально закреплена в тексте политик, процедур и регламентов, подлежащих распространению и соблюдению, и соответствовать Руководству по безопасной разработке программного обеспечения Общества. Необходимо разработать и довести до сведения соответствующих работников регламенты программирования. Такие регламенты включают в себя спецификации в области архитектуры и дизайна, обзор бизнес-логики, внедрение защитных алгоритмов и библиотек, удаление тестового кода и исправления распространенных ошибок в системе безопасности;

– исходный код должен проходить проверки в целях подтверждения соблюдения вышеуказанных регламентов программирования;

– использование производственных данных в непроизводственной среде должно осуществляться только при необходимости. Необходимо применять те же меры контроля безопасности, которые действуют в производственной среде, или производственная информация, используемая в ходе испытаний, должна быть в достаточной степени замаскирована.

– находящееся в открытом доступе программное обеспечение (например, программное обеспечение с открытым кодом, условно-бесплатное и бесплатное программное обеспечение), при использовании такового:

- должно проходить применимые проверки на предмет потенциального риска, включая потенциальный юридический риск (например, нарушение авторских прав);
- должно включать меры контроля, гарантирующие, что внедрение такого типа программного обеспечения не окажет отрицательного воздействия (например, вирус, «Троян», нарушения безопасности, такие как «программная закладка»).

– исходный код должен храниться в приемлемом для отрасли непубличном средстве управления версиями при наличии строгих средств контроля для проверки исходного кода. Подрядчик должен иметь системы постоянного мониторинга, которые осуществляют мониторинг изменений среды выполнения кода;

– должно производиться управление жизненным циклом безопасности всего программного обеспечения, как разработанного подрядчиком, так и приобретенного у третьих лиц.

Управление версиями кода:

– подрядчик должен стремиться к непрерывному усовершенствованию выбранной им модели разработки;

– подрядчик должен внедрить и применять официальную политику/процедуру управления изменениями/выпуском в отношении запланированных обновлений программного обеспечения, которая демонстрирует, что такие выпуски являются запланированными, управляемыми, были проверены, утверждены и надлежащим образом доведены до сведения указанных лиц, при этом Общество должно получать заблаговременные уведомления о запланированных изменениях;

– циклы управления изменениями/выпускам начинаются с определения требований.

Воздействие, обратная связь и потребность Общества должны быть надлежащим образом интегрированы в требования запланированных выпусков:

– регрессионное тестирование должно проводиться в течение каждого цикла выпуска. Тестирование должно проводиться на разных уровнях (например, на уровне единицы, интеграции и системы, пользователя). В основе пользовательского тестирования должны лежать официальные планы испытаний, проводимых лицами, которые никоим образом не зависят от тех, кто отвечает за проектирование и разработку системы;

– необходимо получать официальные одобрения на каждом этапе жизненного цикла разработки (определение требований, проектирование, тестирование, приемка пользователем, реализация производства и т.д.). При регистрации одобрений должно быть понятно, кто, когда и в отношении чего выдает одобрение;

– релизы и патчи должны предоставляться с достаточным объемом указаний по их развертыванию и (или) использованию. К ним относятся такие решения, когда Общество

само предоставляет релиз или патч для использования, а также решения, когда Общество уведомляют об изменении, которое подрядчик внес в среду Общества.

Промежуточные изменения/исправления ошибок:

– должна быть в наличии процедура внесения экстренных изменений/устранения ошибок, в том числе для устранения уязвимостей безопасности, для гарантии того, что такие изменения могут быть внесены своевременно, но при этом контролируемо;

– должен существовать официальный процесс по уведомлению Общества об известных ошибках и дефектах;

– изменения, вносимые в связи с исправлением ошибок, должны подлежать официальной проверке и демонстрировать надлежащее документирование и утверждение. Утверждение должно проводиться лицом, отличным от работника, вносящего изменение.

Вышеуказанные требования применимы только к создаваемым подрядчиком системам, программному обеспечению или приложениям, предназначенным для Общества.

4. Рассылка и актуализация

Периодическая проверка актуальности регламента проводится Начальником отдела информационной безопасности по мере необходимости, но не реже 1 раза в 24 месяца.

Решение о внесении изменений в регламент принимает ЗГД по безопасности на основании предложений других подразделений, результатов применения документа, анализа зарегистрированных и устраненных несоответствий, а также рекомендаций внутренних или внешних аудитов.

Актуальная версия утвержденного регламента размещена в СЭД и на корпоративном портале в разделе «Документы».