Веб-платформа "БЕГЕТ"

АКТ ОЦЕНКИ ЭФФЕКТИВНОСТИ РЕАЛИЗОВАННЫХ В РАМКАХ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Обществом с ограниченной ответственностью «Бегет» (в дальнейшем — Общество) осуществлен анализ результативности принятых в рамках системы защиты персональных данных мер, направленных на обеспечение безопасности персональных данных при их обработке в информационной системе Веб-платформа «БЕГЕТ». Указанный анализ проведен в соответствии с «Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденным приказом ФСТЭК России от 18 февраля 2013 г. № 21.

2. В состав Информационной системы Веб-платформа «БЕГЕТ» входят сервисы, предоставляемые на платной основе, если Лицензиаром не установлено иное:
    - Управление конфигурацией веб-сервера
    - Управление базовым хранилищем S3
    - Управление расширенным хранилищем S3
    - Управление хранилищем S3
    - Управление CDN
    - Управление конфигурацией облачного сервера
    - Управление конфигурацией Kubernetes
    - Управление публичными IP
    - Управление бэкапами

3. Технические средства Информационной системы Веб-платформа "БЕГЕТ" располагаются на следующих территориальных площадках:

Регион	Зона	Адрес
Санкт-Петербург	RU-1	Россия, г. Санкт-Петербург, Евпаторийский пер., д. 7, литера А
Санкт-Петербург	RU-1	Россия, г. Санкт-Петербург, ул. Жукова, д. 43
Москва	RU-2	Россия, г. Москва, ул. Подольских Курсантов, 15Б, стр. 1

4. Оценка эффективности проведена в форме, определенной оператором, в соответствии с информационным сообщением ФСТЭК России от 15 июля 2013 г. № 240/22/2637.

5. По итогам анализа результативности применяемых мер и оценки соответствия системы защиты установленным требованиям в области безопасности персональных данных выявлено, что система защиты Информационной системы Веб-платформа «БЕГЕТ» отвечает требованиям, предъявляемым к составу и содержанию мер по обеспечению безопасности персональных данных для 1-го уровня защищенности (УЗ-1) персональных данных, а также обеспечивает защиту от актуальных угроз безопасности информации в пределах зоны ответственности оператора.

6. Срок действия результатов оценки составляет 3 (три) года. Повторная оценка эффективности проводится в случае изменения структурно-функциональных характеристик Информационной системы Веб-платформа «БЕГЕТ», условий ее эксплуатации, требований, соответствие

которым проверялось в ходе оценки, а также при возникновении новых актуальных угроз безопасности информации.

7. Обеспечение безопасности информации, обрабатываемой посредством Информационной системы Веб-платформа «БЕГЕТ» и информационных систем, развернутых на ее основе, а также соблюдение требований законодательства возлагаются на Лицензиара (ООО «Бегет») и Лицензиатов в рамках совместной ответственности. Распределение зон ответственности установлено в Приложении 1.

8. Перечень мер, соответствие которым оценивалось в ходе проведения оценки, представлен в Приложении 2. Кроме того, в указанном приложении содержатся сведения о мерах, подлежащих реализации в информационных системах Лицензиата, функционирующих на базе Информационной системы Веб-платформа «БЕГЕТ», в целях обеспечения безопасности персональных данных вплоть до 1-го уровня защищенности (УЗ-1) включительно.

Генеральный директор ООО “Бегет” А.Е. Клюков

“26” февраля 2026

Приложение 1

Разграничение зон ответственности в части обеспечения безопасности Информационной системы Веб-платформа "БЕГЕТ"

Информационная система Веб-платформа «БЕГЕТ» представляет собой распределенную вычислительную инфраструктуру, включающую совокупность инфраструктурных сервисов и предназначенную для размещения на своей основе информационных систем Лицензиатов, в том числе информационных систем персональных данных с уровнем защищенности вплоть до 1-го (УЗ-1) включительно.

Обеспечение безопасности информации, обрабатываемой с применением Информационной системы Веб-платформа «БЕГЕТ» и информационных систем Лицензиатов, развернутых на ее базе, а также соблюдение требований законодательства являются совместной ответственностью Лицензиара (ООО «Бегет») и Лицензиатов.

На уровне общего подхода разграничение зон ответственности между Лицензиаром (ООО «Бегет») и Лицензиатами при использовании сервисов, перечисленных в настоящем документе, выглядит следующим образом:

1. Лицензиар (ООО «Бегет») обеспечивает физическую безопасность и отказоустойчивость оборудования, безопасность служебных сетей, а также защиту платформы виртуализации и служебных серверов Веб-платформы «БЕГЕТ».
2. Лицензиаты отвечают за информационную безопасность собственных информационных систем, развернутых на базе Веб-платформы «БЕГЕТ»: обеспечивают безопасность виртуальных машин (включая операционные системы, программное обеспечение, веб-сайты, базы данных и прочие ИТ-решения, размещенные Лицензиатом), безопасность виртуальных сетей и IP-адресов Лицензиата, а также организуют управление доступом.
3. В целях реализации мер защиты информации в своей зоне ответственности (полностью или частично — на усмотрение Лицензиата) Лицензиаты могут использовать дополнительные сервисы платформы: Firewall, маршрутизаторы, WAF, системы резервного копирования, защиту от DDoS-атак, а также услуги по сканированию и поиску уязвимостей на виртуальных серверах с публичными IP-адресами.

Детальное распределение зон ответственности между ООО «Бегет» и Лицензиатами, дополнительные сервисы платформы приведены в Приложении 2.

Приложение 2

Выполнение мер по обеспечению безопасности информации Информационной системы

Веб-платформа "БЕГЕТ"

Реализация мер, необходимых для обеспечения безопасности персональных данных вплоть до 1-го уровня защищенности (УЗ-1) включительно, а также для нейтрализации актуальных угроз безопасности, обеспечивается посредством использования штатных возможностей системного и прикладного программного обеспечения, входящего в состав Информационной системы Веб-платформа «БЕГЕТ», применяемых средств защиты информации, а также за счет комплекса организационных мероприятий.

Перечень мер, реализуемых ООО «Бегет», сформированный в соответствии с требованиями приказа ФСТЭК России от 18.02.2013 № 21 и постановления Правительства Российской Федерации от 01.11.2012 № 1119, представлен в нижеприведенной таблице. Указанная таблица также содержит перечень мер, подлежащих реализации в информационных системах Лицензиатов, размещаемых на базе Информационной системы Веб-платформа «БЕГЕТ», в целях обеспечения безопасности персональных данных для уровня защищенности до 1-го (УЗ-1) включительно.

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Реализация Лицензиаром (ООО «Бегет»)	Реализация Лицензиатом	Дополнительные сервисы платформы, доступные Лицензиату
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	Реализуется на уровне сетевого оборудования, серверов и платформы виртуализации (далее - инфраструктура платформы)	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	Не применимо	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	

УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами объекта информатизации	Реализуется на уровне инфраструктуры платформы для служебных сетей	Необходимо реализовать, настроив услуги: Виртуальные сети, Интернет канал, Публичный IP	Возможность использования сервисов Firewall, Роутеры, WAF
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование объекта информатизации	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование объекта информатизации	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование объекта информатизации	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
УПД.6	Ограничение неуспешных попыток входа в объект информатизации (доступа к объекту информатизации)	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
УПД.10	Блокирование сеанса доступа в объект информатизации после установленного времени бездействия (неактивности) пользователя или по его запросу	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	Реализуется на уровне инфраструктуры платформы	На уровне удаленного доступа к виртуальным серверам Лицензиата	
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	Не применимо	Не применимо	
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств	Не применимо	Не применимо	
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	Реализуется на уровне служебной инфраструктуры	На уровне виртуальных машин Лицензиата	Возможность использования сервисов Firewall, Роутеры
УПД.17	Обеспечение доверенной загрузки средств вычислительной техники	Реализуется на уровне инфраструктуры платформы	Не применимо	

ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
ЗНИ.1	Учет машинных носителей персональных данных	Реализуется на уровне инфраструктуры платформы	Не применимо	
ЗНИ.2	Управление доступом к машинным носителям персональных данных	Реализуется на уровне инфраструктуры платформы	Не применимо	
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания	Реализуется на уровне инфраструктуры платформы	Не применимо	
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
РСБ.7	Защита информации о событиях безопасности	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
АВЗ.1	Реализация антивирусной защиты	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	

СОВ.1	Обнаружение вторжений	Реализуется на уровне служебной сети и служебных серверов	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
СОВ.2	Обновление базы решающих правил	Реализуется на уровне служебной сети и служебных серверов	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
АНЗ.1	Выявление, анализ уязвимостей объекта информатизации и оперативное устранение вновь выявленных уязвимостей	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	Возможность заказа услуги по сканированию и поиску уязвимостей на виртуальных серверах с белыми IP
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	Возможность заказа услуги по сканированию и поиску уязвимостей на виртуальных серверах с белыми IP
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
ОЦЛ.4	Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию Информационной системы (защита от спама)	Не применимо	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование	Реализуется на уровне инфраструктуры платформы	Не применимо	
ОДТ.4	Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных	Не применимо	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	

ОДТ.5	Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала	Не применимо	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	Возможность заказа услуги Бэкапы
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	Реализуется на уровне инфраструктуры платформы	Не применимо	
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
ЗСВ.8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре	Реализуется на уровне инфраструктуры платформы	Не применимо	
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	Возможность использования сервисов Firewall, Роутеры
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования	Реализуется на уровне центров обработки данных	Не применимо	

ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования объекта информатизации, в помещения и сооружения, в которых они установлены	Реализуется на уровне инфраструктуры платформы	Не применимо	
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	Не применимо	Не применимо	
ЗИС.1	Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты персональных данных, функций по обработке персональных данных и иных функций Информационной системы	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
ЗИС.3	Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
ЗИС.17	Разбиение Информационной системы на сегменты (сегментирование Информационной системы) и обеспечение защиты периметров сегментов Информационной системы	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе	Не применимо	Не применимо	
ЗИС.22	Защита от угроз безопасности информации, направленных на отказ в обслуживании.	Реализуется на уровне служебной сети для панели управления, служебных сетей и IP адресов Лицензиара	Необходимо реализовать Лицензиату на уровне сетей, IP адресов, сайтов, программ для ЭВМ, баз данных и иных размещенных Лицензиатом ИТ-решений	Возможность заказа дополнительных сервисов защиты от DDoS-атак, WAF

ИНЦ.1	Определение лиц, ответственных за выявление инцидентов и реагирование на них	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
ИНЦ.3	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
ИНЦ.4	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
ИНЦ.5	Принятие мер по устранению последствий инцидентов	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
ИНЦ.6	Планирование и принятие мер по предотвращению повторного возникновения инцидентов	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию объекта информатизации и системы защиты информации	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
УКФ.2	Управление изменениями конфигурации объекта информатизации и системы защиты информации	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации объекта информатизации и системы защиты информации на обеспечение защиты информации и согласование изменений в конфигурации объекта информатизации с должностным лицом (работником), ответственным за обеспечение безопасности информации	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	
УКФ.4	Документирование информации (данных) об изменениях в конфигурации объекта информатизации и системы защиты информации	Реализуется на уровне инфраструктуры платформы	На уровне виртуальных машин Лицензиата и применяемого на них системного и прикладного ПО, средств защиты информации	