Состав мер по обеспечению безопасности для значимого объекта соответствующей категории значимости						
Обозначение и номер меры	**Меры обеспечения безопасности значимого объекта***	**категория значимости**			**Реализация мер в сертифицированной ФСТЭК России редакции Deckhouse Stronghold**	**Подтверждение реализации требований в ТУ и на официальных ресурсах разработчика**
		1	**2**	**3**		
I. Идентификация и аутентификация (ИАФ)						
ИАФ.0	Регламентация правил и процедур	да	да	да		n/a
ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов	да	да	да	+	п. 3.2.2.1
ИАФ.2	Идентификация и аутентификация устройств	да	да	да		n/a
ИАФ.3	Управление идентификаторами	да	да	да	+	п. 3.2.2.1
ИАФ.4	Управление средствами аутентификации	да	да	да	+	п. 3.2.2.1
ИАФ.5	Идентификация и аутентификация внешних пользователей	да	да	да	+	п. 3.2.2.1
ИАФ.6	Двусторонняя аутентификация					n/a
ИАФ.7	Защита аутентификационной информации при передаче	да	да	да		n/a
II. Управление доступом (УПД)						
УПД.0	Регламентация правил и процедур управления доступом	да	да	да		n/a
УПД.1	Управление учетными записями пользователей	да	да	да	+	п. 3.2.2.2
УПД.2	Реализация модели управления доступом	да	да	да	+	п. 3.2.2.2
УПД.3	Доверенная загрузка		да	да		n/a
УПД.4	Разделение полномочий (ролей) пользователей	да	да	да		n/a
УПД.5	Назначение минимально необходимых прав и привилегий	да	да	да		n/a
УПД.6	Ограничение неуспешных попыток доступа в информационную (автоматизированную)	да	да	да	+	п. 3.2.2.2
УПД.7	Предупреждение пользователя при его доступе к информационным ресурсам					n/a
УПД.8	Оповещение пользователя при успешном входе о предыдущем доступе к					n/a
УПД.9	Ограничение числа параллельных сеансов доступа			да		n/a
УПД.10	Блокирование сеанса доступа пользователя при неактивности	да	да	да	+	п. 3.2.2.2
УПД.11	Управление действиями пользователей до идентификации и аутентификации	да	да	да		n/a
УПД.12	Управление атрибутами безопасности					n/a
УПД.13	Реализация защищенного удаленного доступа	да	да	да		n/a
УПД.14	Контроль доступа из внешних информационных (автоматизированных) систем	да	да	да		n/a
III. Ограничение программной среды (ОПС)						
ОПС.0	Регламентация правил и процедур ограничения программной среды		да	да		n/a
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения			да		n/a
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения		да	да		n/a
ОПС.3	Управление временными файлами					n/a
IV. Защита машинных носителей информации (ЗНИ)						
ЗНИ.0	Регламентация правил и процедур защиты машинных носителей информации	да	да	да		n/a
ЗНИ.1	Учет машинных носителей информации	да	да	да		n/a
ЗНИ.2	Управление физическим доступом к машинным носителям информации	да	да	да		n/a
ЗНИ.3	Контроль перемещения машинных носителей информации за пределы					n/a
ЗНИ.4	Исключение возможности несанкционированного чтения информации на машинных					n/a
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на съемные	да	да	да		n/a
ЗНИ.6	Контроль ввода (вывода) информации на съемные машинные носители информации			да		n/a
ЗНИ.7	Контроль подключения съемных машинных носителей информации	да	да	да		n/a
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях информации	да	да	да		n/a
V. Аудит безопасности (АУД)						
АУД.0	Регламентация правил и процедур аудита безопасности	да	да	да		n/a
АУД.1	Инвентаризация информационных ресурсов	да	да	да		n/a
АУД.2	Анализ уязвимостей и их устранение	да	да	да		n/a
АУД.3	Генерирование временных меток и (или) синхронизация системного времени	да	да	да		n/a

АУД.4	Регистрация событий безопасности	да	да	да	+	п. 3.2.2.3
АУД.5	Контроль и анализ сетевого трафика			да		n/a
АУД.6	Защита информации о событиях безопасности	да	да	да	Выполняется частично	Не заявлена в ТУ
АУД.7	Мониторинг безопасности	да	да	да		n/a
АУД.8	Реагирование на сбои при регистрации событий безопасности	да	да	да	Выполняется частично	Не заявлена в ТУ
АУД.9	Анализ действий отдельных пользователей			да		n/a
АУД.10	Проведение внутренних аудитов	да	да	да		n/a
АУД.11	Проведение внешних аудитов					n/a
VI. Антивирусная защита (АВЗ)						
АВЗ.0	Регламентация правил и процедур антивирусной защиты	да	да	да		n/a
АВЗ.1	Реализация антивирусной защиты	да	да	да		n/a
АВЗ.2	Антивирусная защита электронной почты и иных сервисов	да	да	да		n/a
АВЗ.3	Контроль использования архивных, исполняемых и зашифрованных файлов			да		n/a
АВЗ.4	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	да	да	да		n/a
АВЗ.5	Использование средств антивирусной защиты различных производителей			да		n/a
VII. Предотвращение вторжений (компьютерных атак) (СОВ)						
СОВ.0	Регламентация правил и процедур предотвращения вторжений (компьютерных атак)		да	да		n/a
СОВ.1	Обнаружение и предотвращение компьютерных атак		да	да		n/a
СОВ.2	Обновление базы решающих правил		да	да		n/a
VIII. Обеспечение целостности (ОЦЛ)						
ОЦЛ.0	Регламентация правил и процедур обеспечения целостности	да	да	да		n/a
ОЦЛ.1	Контроль целостности программного обеспечения	да	да	да		n/a
ОЦЛ.2	Контроль целостности информации					n/a
ОЦЛ.3	Ограничения по вводу информации в информационную (автоматизированную) систему			да		n/a
ОЦЛ.4	Контроль данных, вводимых в информационную (автоматизированную) систему		да	да		n/a
ОЦЛ.5	Контроль ошибочных действий пользователей по вводу и (или) передаче информации		да	да		n/a
ОЦЛ.6	Обезличивание и (или) деидентификация информации					n/a
IX. Обеспечение доступности (ОДТ)						
ОДТ.0	Регламентация правил и процедур обеспечения доступности	да	да	да		n/a
ОДТ.1	Использование отказоустойчивых технических средств		да	да		n/a
ОДТ.2	Резервирование средств и систем		да	да		n/a
ОДТ.3	Контроль безотказного функционирования средств и систем		да	да		n/a
ОДТ.4	Резервное копирование информации	да	да	да	+	п. 3.2.2.4
ОДТ.5	Обеспечение возможности восстановления информации	да	да	да		n/a
ОДТ.6	Обеспечение возможности восстановления программного обеспечения при нештатных	да	да	да		n/a
ОДТ.7	Кластеризация информационной (автоматизированной) системы					n/a
ОДТ.8	Контроль предоставляемых вычислительных ресурсов и каналов связи	да	да	да		n/a
X. Защита технических средств и систем (ЗТС)						
ЗТС.0	Регламентация правил и процедур защиты технических средств и систем	да	да	да		n/a
ЗТС.1	Защита информации от утечки по техническим каналам					n/a
ЗТС.2	Организация контролируемой зоны	да	да	да		n/a
ЗТС.3	Управление физическим доступом	да	да	да		n/a
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее	да	да	да		n/a
ЗТС.5	Защита от внешних воздействий	да	да	да		n/a
ЗТС.6	Маркирование аппаратных компонентов системы относительно разрешенной к					n/a
XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)						

ЗИС.0	Регламентация правил и процедур защиты информационной (автоматизированной)	да	да	да		n/a
ЗИС.1	Разделение функций по управлению (администрированию) информационной	да	да	да		n/a
ЗИС.2	Защита периметра информационной (автоматизированной) системы	да	да	да		n/a
ЗИС.3	Эшелонированная защита информационной (автоматизированной) системы	да	да	да		n/a
ЗИС.4	Сегментирование информационной (автоматизированной) системы		да	да		n/a
ЗИС.5	Организация демилитаризованной зоны	да	да	да		n/a
ЗИС.6	Управление сетевыми потоками	да	да	да		n/a
ЗИС.7	Использование эмулятора среды функционирования программного обеспечения					n/a
ЗИС.8	Сокрытие архитектуры и конфигурации информационной (автоматизированной)	да	да	да		n/a
ЗИС.9	Создание гетерогенной среды					n/a
ЗИС.10	Использование программного обеспечения, функционирующего в средах различных					n/a
ЗИС.11	Предотвращение задержки или прерывания выполнения процессов с высоким					n/a
ЗИС.12	Изоляция процессов (выполнение программ) в выделенной области памяти					n/a
ЗИС.13	Защита неизменяемых данных		да	да		n/a
ЗИС.14	Использование неперезаписываемых машинных носителей информации					n/a
ЗИС.15	Реализация электронного почтового обмена с внешними сетями через ограниченное					n/a
ЗИС.16	Защита от спама		да	да		n/a
ЗИС.17	Защита информации от утечек					n/a
ЗИС.18	Блокировка доступа к сайтам или типам сайтов, запрещенных к использованию					n/a
ЗИС.19	Защита информации при ее передаче по каналам связи	да	да	да		n/a
ЗИС.20	Обеспечение доверенных канала, маршрута	да	да	да		n/a
ЗИС.21	Запрет несанкционированной удаленной активации периферийных устройств	да	да	да		n/a
ЗИС.22	Управление атрибутами безопасности при взаимодействии с иными					n/a
ЗИС.23	Контроль использования мобильного кода					n/a
ЗИС.24	Контроль передачи речевой информации					n/a
ЗИС.25	Контроль передачи видеоинформации					n/a
ЗИС.26	Подтверждение происхождения источника информации					n/a
ЗИС.27	Обеспечение подлинности сетевых соединений		да	да		n/a
ЗИС.28	Исключение возможности отрицания отправки информации					n/a
ЗИС.29	Исключение возможности отрицания получения информации					n/a
ЗИС.30	Использование устройств терминального доступа					n/a
ЗИС.31	Защита от скрытых каналов передачи информации					n/a
ЗИС.32	Защита беспроводных соединений	да	да	да		n/a
ЗИС.33	Исключение доступа через общие ресурсы			да		n/a
ЗИС.34	Защита от угроз отказа в обслуживании (DOS, DDOS-атак)	да	да	да		n/a
ЗИС.35	Управление сетевыми соединениями	да	да	да		n/a
ЗИС.36	Создание (эмуляция) ложных компонентов информационных (автоматизированных)					n/a
ЗИС.37	Перевод информационной (автоматизированной) системы в безопасное состояние при					n/a
ЗИС.38	Защита информации при использовании мобильных устройств	да	да	да		n/a
ЗИС.39	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на	да	да	да		n/a
XII. Реагирование на компьютерные инциденты (ИНЦ)						
ИНЦ.0	Регламентация правил и процедур реагирования на компьютерные инциденты	да	да	да		n/a
ИНЦ.1	Выявление компьютерных инцидентов	да	да	да		n/a
ИНЦ.2	Информирование о компьютерных инцидентах	да	да	да		n/a
ИНЦ.3	Анализ компьютерных инцидентов	да	да	да		n/a
ИНЦ.4	Устранение последствий компьютерных инцидентов	да	да	да		n/a
ИНЦ.5	Принятие мер по предотвращению повторного возникновения компьютерных	да	да	да		n/a
ИНЦ.6	Хранение и защита информации о компьютерных инцидентах	да	да	да		n/a
XIII. Управление конфигурацией (УКФ)						
УКФ.0	Регламентация правил и процедур управления конфигурацией информационной	да	да	да		n/a

УКФ.1	Идентификация объектов управления конфигурацией					n/a
УКФ.2	Управление изменениями	да	да	да		n/a
УКФ.3	Установка (инсталляция) только разрешенного к использованию программного	да	да	да		n/a
УКФ.4	Контроль действий по внесению изменений					n/a
XIV. Управление обновлениями программного обеспечения (ОПО)						
ОПО.0	Регламентация правил и процедур управления обновлениями программного	да	да	да		n/a
ОПО.1	Поиск, получение обновлений программного обеспечения от доверенного источника	да	да	да		n/a
ОПО.2	Контроль целостности обновлений программного обеспечения	да	да	да		n/a
ОПО.3	Тестирование обновлений программного обеспечения	да	да	да		n/a
ОПО.4	Установка обновлений программного обеспечения	да	да	да		n/a
XV. Планирование мероприятий по обеспечению безопасности (ПЛН)						
ПЛН.0	Регламентация правил и процедур планирования мероприятий по обеспечению	да	да	да		n/a
ПЛН.1	Разработка, утверждение и актуализация плана мероприятий по обеспечению защиты	да	да	да		n/a
ПЛН.2	Контроль выполнения мероприятий по обеспечению защиты информации	да	да	да		n/a
XVI. Обеспечение действий в нештатных ситуациях (ДНС)						
ДНС.0	Регламентация правил и процедур обеспечения действий в нештатных ситуациях	да	да	да		n/a
ДНС.1	Разработка плана действий в нештатных ситуациях	да	да	да		n/a
ДНС.2	Обучение и отработка действий персонала в нештатных ситуациях	да	да	да		n/a
ДНС.3	Создание альтернативных мест хранения и обработки информации на случай		да	да		n/a
ДНС.4	Резервирование программного обеспечения, технических средств, каналов связи на		да	да		n/a
ДНС.5	Обеспечение возможности восстановления информационной (автоматизированной)	да	да	да		n/a
ДНС.6	Анализ возникших нештатных ситуаций и принятие мер по недопущению их повторного	да	да	да		n/a
XVII. Информирование и обучение персонала (ИПО)						
ИПО.0	Регламентация правил и процедур информирования и обучения персонала	да	да	да	+	deckhouse-academy (https://deckhouse.ru/academy/)
ИПО.1	Информирование персонала об угрозах безопасности информации и о правилах безопасной работы	да	да	да	+	deckhouse-academy (https://deckhouse.ru/academy/)
ИПО.2	Обучение персонала правилам безопасной работы	да	да	да	+	deckhouse-academy (https://deckhouse.ru/academy/)
ИПО.3	Проведение практических занятий с персоналом по правилам безопасной работы		да	да	+	deckhouse-academy (https://deckhouse.ru/academy/)
ИПО.4	Контроль осведомленности персонала об угрозах безопасности информации и о правилах безопасной работы	да	да	да	+	n/a