Состав мер по обеспечению безопасности для значимого объекта соответствующей категории значимости					
Обозначение и номер меры	Меры обеспечения безопасности значимого объекта*	Категория значимости			
		3	2	1	DKP CSE 1.67
I. Идентификация и аутентификация (ИАФ)					
ИАФ.0	Регламентация правил и процедур идентификации и аутентификации	да	да	да	n/a
ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов	да	да	да	user-authn + внешний провайдер
ИАФ.2	Идентификация и аутентификация устройств	да	да	да	user-authn + внешний провайдер
ИАФ.3	Управление идентификаторами	да	да	да	user-authn + внешний провайдер
ИАФ.4	Управление средствами аутентификации	да	да	да	user-authn + внешний провайдер
ИАФ.5	Идентификация и аутентификация внешних пользователей	да	да	да	user-authn + внешний провайдер
ИАФ.6	Двусторонняя аутентификация				user-authn + внешний провайдер
ИАФ.7	Защита аутентификационной информации при передаче	да	да	да	user-authn + внешний провайдер
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	user-authz
УПД.2	Реализация модели управления доступом	да	да	да	user-authz
УПД.3	Доверенная загрузка	да	да	да	n/a
УПД.4	Разделение полномочий (ролей) пользователей	да	да	да	user-authz
УПД.5	Назначение минимально необходимых прав и привилегий	да	да	да	user-authz
УПД.6	Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему	да	да	да	user-authn + внешний провайдер
УПД.7	Предупреждение пользователя при его доступе к информационным ресурсам				
УПД.8	Оповещение пользователя при успешном входе о предыдущем доступе к информационной (автоматизированной) системе				
УПД.9	Ограничение числа параллельных сеансов доступа			да	n/a
УПД.10	Блокирование сеанса доступа пользователя при неактивности	да	да	да	user-authn + внешний провайдер
УПД.11	Управление действиями пользователей до идентификации и аутентификации	да	да	да	n/a
УПД.12	Управление атрибутами безопасности				user-authn + внешний провайдер
УПД.13	Реализация защищенного удаленного доступа	да	да	да	user-authz
УПД.14	Контроль доступа из внешних информационных (автоматизированных) систем	да	да	да	user-authn + внешний провайдер
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	admission-policy-engine + runtine
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения		да	да	admission-policy-engine + runtine
ОПС.3	Управление временными файлами				

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 контролируемой зоны				
ЗНИ.4	Исключение возможности несанкционированного чтения информации на машинных носителях информации				
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на съемные машинные носители информации	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	console
АУД.2	Анализ уязвимостей и их устранение	да	да	да	trivy
АУД.3	Генерирование временных меток и (или) синхронизация системного времени	да	да	да	chrony
АУД.4	Регистрация событий безопасности	да	да	да	runtime-audit-engine + log-shipper + loki + prometheus
АУД.5	Контроль и анализ сетевого трафика			да	hubble cillium
АУД.6	Защита информации о событиях безопасности	да	да	да	user-authn + user-authz + внешние провайдеры
АУД.7	Мониторинг безопасности	да	да	да	runtime-audit-engine + log-shipper + loki + extended-monitoring
АУД.8	Реагирование на сбои при регистрации событий безопасности	да	да	да	runtime-audit-engine + log-shipper + loki + prometheus
АУД.9	Анализ действий отдельных пользователей			да	runtime-audit-engine + log-shipper + loki
АУД.10	Проведение внутренних аудитов	да	да	да	runtime-audit-engine + log-shipper + loki
АУД.11	Проведение внешних аудитов				
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	gost-integrity-controller
ОЦЛ.2	Контроль целостности информации				admission-policy-engine
ОЦЛ.3	Ограничения по вводу информации в информационную (автоматизированную) систему			да	n/a
ОЦЛ.4	Контроль данных, вводимых в информационную (автоматизированную) систему		да	да	dkp (validationwebhook)
ОЦЛ.5	Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях		да	да	dkp (validationwebhook)
ОЦЛ.6	Обезличивание и (или) деидентификация информации				
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	dkp high availability
ОДТ.2	Резервирование средств и систем		да	да	dkp (replicasets (deployments))
ОДТ.3	Контроль безотказного функционирования средств и систем		да	да	log-shipper + loki + prometheus
ОДТ.4	Резервное копирование информации	да	да	да	dkp (backup-etcd job) + dkp (volumesnapshot)
ОДТ.5	Обеспечение возможности восстановления информации	да	да	да	dkp (restore etcd)
ОДТ.6	Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях	да	да	да	dkp (probes + replicasets)
ОДТ.7	Кластеризация информационной (автоматизированной) системы				dkp high availability
ОДТ.8	Контроль предоставляемых вычислительных ресурсов и каналов связи	да	да	да	dkp (resources + networkpolicy)
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				
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 несанкционированный просмотр	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 обработке информации				
XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)					

ЗИС.0	Регламентация правил и процедур защиты информационной (автоматизированной) системы и ее компонентов	да	да	да	n/a
ЗИС.1	Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями	да	да	да	user-authn + user-authz + внешние провайдеры
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	multitenancy-manager
ЗИС.5	Организация демилитаризованной зоны	да	да	да	multitenancy-manager + cilium
ЗИС.6	Управление сетевыми потоками	да	да	да	multitenancy-manager + cilium + istio
ЗИС.7	Использование эмулятора среды функционирования программного обеспечения ("песочница")				
ЗИС.8	Сокрытие архитектуры и конфигурации информационной (автоматизированной) системы	да	да	да	user-authn + user-authz + внешние провайдеры
ЗИС.9	Создание гетерогенной среды				
ЗИС.10	Использование программного обеспечения, функционирующего в средах различных операционных систем				РЕД ОС (7.3) + ALT Linux (8 СП (релиз 10)) + Astra Linux Special Edition (1.7)
ЗИС.11	Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом				priority-class
ЗИС.12	Изоляция процессов (выполнение программ) в выделенной области памяти				
ЗИС.13	Защита неизменяемых данных		да	да	admission-policy-engine
ЗИС.14	Использование неперезаписываемых машинных носителей информации				
ЗИС.15	Реализация электронного почтового обмена с внешними сетями через ограниченное количество контролируемых точек				
ЗИС.16	Защита от спама		да	да	n/a
ЗИС.17	Защита информации от утечек				
ЗИС.18	Блокировка доступа к сайтам или типам сайтов, запрещенных к использованию				
ЗИС.19	Защита информации при ее передаче по каналам связи	да	да	да	istio
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 информационными (автоматизированными) системами				
ЗИС.23	Контроль использования мобильного кода				
ЗИС.24	Контроль передачи речевой информации				
ЗИС.25	Контроль передачи видеоинформации				
ЗИС.26	Подтверждение происхождения источника информации				
ЗИС.27	Обеспечение подлинности сетевых соединений		да	да	istio
ЗИС.28	Исключение возможности отрицания отправки информации				

ЗИС.29	Исключение возможности отрицания получения информации				
ЗИС.30	Использование устройств терминального доступа				
ЗИС.31	Защита от скрытых каналов передачи информации				
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	ingress-nginx
ЗИС.35	Управление сетевыми соединениями	да	да	да	cilium + istio + metallb
ЗИС.36	Создание (эмуляция) ложных компонентов информационных (автоматизированных) систем				
ЗИС.37	Перевод информационной (автоматизированной) системы в безопасное состояние при возникновении отказов (сбоев)				
ЗИС.38	Защита информации при использовании мобильных устройств	да	да	да	ingress-nginx
ЗИС.39	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	да	да	да	node-manager
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	runtime-audit-engine + log-shipper + loki + prometheus
ИНЦ.2	Информирование о компьютерных инцидентах	да	да	да	runtime-audit-engine + log-shipper + loki + prometheus
ИНЦ.3	Анализ компьютерных инцидентов	да	да	да	runtime-audit-engine + log-shipper + loki + prometheus
ИНЦ.4	Устранение последствий компьютерных инцидентов	да	да	да	self-healing
ИНЦ.5	Принятие мер по предотвращению повторного возникновения компьютерных инцидентов	да	да	да	настройка политик
ИНЦ.6	Хранение и защита информации о компьютерных инцидентах	да	да	да	loki + prometheus
XIII. Управление конфигурацией (УКФ)					
УКФ.0	Регламентация правил и процедур управления конфигурацией информационной (автоматизированной) системы	да	да	да	n/a
УКФ.1	Идентификация объектов управления конфигурацией				
УКФ.2	Управление изменениями	да	да	да	n/a
УКФ.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения	да	да	да	admission-policy-engine
УКФ.4	Контроль действий по внесению изменений				
XIV. Управление обновлениями программного обеспечения (ОПО)					
ОПО.0	Регламентация правил и процедур управления обновлениями программного обеспечения	да	да	да	n/a
ОПО.1	Поиск, получение обновлений программного обеспечения от доверенного источника	да	да	да	operation policy
ОПО.2	Контроль целостности обновлений программного обеспечения	да	да	да	admission-policy-engine

ОПО.3	Тестирование обновлений программного обеспечения	да	да	да	istio
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 защиты информации	да	да	да	n/a
ПЛН.1	Разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации	да	да	да	n/a
ПЛН.2	Контроль выполнения мероприятий по обеспечению защиты информации	да	да	да	runtime-audit-engine + log-shipper + loki + prometheus
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 возникновения нештатных ситуаций		да	да	istio
ДНС.4	Резервирование программного обеспечения, технических средств, каналов связи на случай возникновения нештатных ситуаций		да	да	istio
ДНС.5	Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных ситуаций	да	да	да	есть возможность вручную восстановить etcd
ДНС.6	Анализ возникших нештатных ситуаций и принятие мер по недопущению их повторного возникновения	да	да	да	log-shipper + loki + prometheus
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				
* Состав мер рассматривается в разрезе применимости к ПО DKP без адаптации формулировок применимым к ПО и в случаях, где в мере, например, приводятся информационные (автоматизированные) системы и тд рассматриваем их в контексте реализации средствами DKP. В случае если мера выполняется отдельным подходом с использованием ПО, то это отдельно отмечено					