Перечень функций информационной безопасности

№ п/п	Наименование функций	Содержание функций	Комментарий
1	2	3	4
Аудит безопасности			
1	Автоматическая реакция аудита безопасности	Осуществление генерации записи в регистрационном журнале, локальная или удаленная сигнализация администратору об обнаружении нарушения безопасности	*Функция отвечает за оперативное оповещение ответственных лиц о событиях и инцидентах ИБ, имеющих высокий или критический уровень риска (п. 52 ППРК ЕТ).* *Заявитель должен определить список событий с критическими и высокими уровнями риска. По этому списку будет проверяться оперативное оповещение ответственных лиц о событиях и инцидентах ИБ. (п. 37 ППРК ЕТ)* *- Оперативное оповещение должно достигаться средствами связи, например, через SMS, e-mail приходящие непосредственно на мобильное устройство ответственного лица. В качестве варианта, может поступать сообщением дежурной службе с дублированием сообщения ответственному лицу за ИБ.* *- Реализация достигается средствами мониторинга и управления инцидентами и событиями ИБ.*
2	Генерация данных аудита безопасности	Наличие протоколирования, по крайней мере, запуска и завершения регистрационных функций, а также всех событий базового уровня аудита, т.е. в каждой регистрационной записи присутствие даты и времени события, типа события, идентификатора субъекта и результата (успех или неудача) события	*Функция отвечает за обеспечение журналирования событий в прямой или обратной временной последовательности, на всех уровнях ПО (ОС, СУБД, Веб-сервер, сервер приложений, прикладное ПО, средства антивирусной защиты, системы управления контентом, среда виртуализации и другие программные компоненты объекта), создание записи в средствах мониторинга и управления инцидентами и событиями ИБ (п. 38 ППРК ЕТ, п. 102 ППРК ЕТ).* *Записи в журнале событий должны отвечать требованиям, указанным в Правилах мониторинга и содержать дату и время события (до миллисекунд), адреса инициатора и получателя, тип события и описание события.* *В правилах мониторинга указан перечень типов событий, которые должны журналироваться.*
3	Анализ аудита безопасности	Осуществление (с целью выявления вероятных нарушений), по крайней мере, путем накопления и/или объединения	*Анализ журналов событий проводится с целью выявления (фильтрации, выделения, чтения) записей, содержащих события или инциденты с высоким или критическим уровнем риска.*

		неуспешных результатов использования механизмов аутентификации, а также неуспешных результатов выполнения криптографических операций	*Анализ может выполняться средствами мониторинга и управления инцидентами и событиями ИБ (п. 38 и п. 54 ППРК ЕТ).*
4	Просмотр аудита безопасности	Обеспечение и предоставление администратору возможности просмотра (чтения) всей регистрационной информации. Прочим пользователям доступ к регистрационной информации должен быть закрыт, за исключением явно специфицированных случаев.	*Должны быть предусмотрены средства просмотра событий, позволяющие осуществлять поиск, сортировку и/или упорядочение. Необходимо чтобы инструментальные средства имели возможность просмотра, основанных на нескольких критериях (например, операциями «и», «или») и имели возможность обработки данных аудита (например, сортировки, фильтрации). (п. 7.4 СТ РК ISO/IEC 15408-2-2017).* *Управление доступом к журналу событий должно ограничивать привилегии администраторов на чтение, запрет на модификацию или отключение (удаление) журнала событий (п. 38 ППРК ЕТ)*
5	Выбор событий аудита безопасности	Наличие избирательности регистрации событий, основывающейся, по крайней мере, на следующих атрибутах: идентификатор объекта; идентификатор субъекта; адрес узла сети; тип события; дата и время события	*Должны быть предусмотрены средства для осуществления выбора событий из журнала событий по указанным параметрам для просмотра или печати.* *Параметры:* - *-идентификатор объекта;* - *-идентификатор субъекта;* - *-адрес узла сети;* - *-тип события;* - *-дата и время события* *(п. 7.5 СТ РК ISO/IEC 15408-2-2017).*
6	Хранение данных аудита безопасности	Наличие регистрационной информации о надежности защиты от несанкционированной модификации	*Журналы событий должны храниться не менее 2х месяцев в оперативном доступе (в месте генерации или на сервере логов) и не менее 3х лет в постоянном доступе (на лентах, CD или другое).* *К управлению журналами должен быть доступ только у ответственного лица за ИБ. Администраторы ОС, СУБД и ППО должны иметь доступ только для чтения (п. 38 ППРК ЕТ).* *Для конфиденциальных ИС требуются создание и ведение резервного хранилища журналов (пп. 6 п. 38 ППРК ЕТ).*
Организация связи			
7	Неотказуемость отправления	Предоставление пользователям/субъектам свидетельства идентичности отправителя некоторой информации, чтобы отправитель не смог	*В случае отправки внешнему объекту сообщения или файла в журналах событий должен регистрироваться факт отправки.* *Факт отправки регистрируется на сервере, являющемся конечной точкой отправки.*

		отрицать факт передачи информации, поскольку свидетельство отправления (например, цифровая подпись) доказывает связь между отправителем и переданной информацией	
8	Неотказуемость получения	Обеспечение невозможности отрицания получателем информации факта ее получения	*В случае получения от внешнего объекта сообщения или файла в журналах событий должен регистрироваться факт получения.* *Факт получения регистрируется на сервере, являющемся конечной точкой получения.*
	Криптографическая поддержка		
9	Управление криптографическими ключами	Наличие поддержки: 1) генерации криптографических ключей; 2) распределения криптографических ключей; 3) управления доступом к криптографическим ключам; 4) уничтожения криптографических ключей	*В случае применения криптографических средств, необходимо проверить процедуры получения или генерации ключей шифрования, способы и средства хранения и передачи ключей шифрования, сроки действия и способы утилизации устаревших ключей (например, ЭЦП, SSH ключи и т.д.).* *На момент проверки используемые ключи должны иметь необходимый срок действия, достаточный для использования при вводе в промышленную эксплуатацию объекта (п. 9.1 СТ РК ISO/IEC 15408-2-2017).* *Длительный срок действия ключей (например, более 3х лет) может создать риск его компрометации.*
10	Криптографические операции	Наличие для всей информации, передаваемой по доверенному каналу, шифрования и контроля целостности в соответствии с требованиями технической документации, нормативных правовых актов Республики Казахстан и действующих на территории Республики Казахстан стандартов в сфере информационной безопасности.	*В случае, если в объекте хранится или обрабатывается конфиденциальная информация, то она должна защищаться с применением СКЗИ на этапах хранения, обработки и передачи.* *Для защиты веб-интерфейса прикладного ПО должны применяться SSL-сертификаты по протоколу https в случае, если требуется ввод или получение конфиденциальной информации, например, пароль пользователя.* *Для защиты данных хранящихся в БД, содержащие персональные данные ограниченного доступа, конфиденциальные данные, а также служебную информацию ограниченного доступа, необходимо обеспечить шифрование, с целью исключения утечки.* *(п. 48 ЕТ, п. 114 ППРК ЕТ)* *(СТ РК 1073-2007 Средства криптографической защиты информации)*
	Защита данных пользователя		
11	Политика управления доступом	Осуществление разграничения доступа для пользователей, прямо или косвенно выполняющих операции с сервисом безопасности	*1) Должен использоваться механизм дискреционного управления (основанный на матрице доступа), а именно применение ролевых и групповых политик (п. 10.1 СТ РК ISO/IEC 15408-2-2017);* *2) Учетные записи пользователей должны использовать уникальный*

			идентификатор, чтобы определить связь пользователей с действиями и ответственностью за них (п. 9.2 СТ РК ISO/IEC 27002-2015); *3) Учетные записи пользователей должны иметь достаточные права и привилегии для выполнения повседневных задач, без возможности внесения модификации в политике безопасности, прав и привилегий других администраторов, а также полезных данных;* *4) Необходимо исключить использование не персонифицированных встроенных административных учетных записей (admin, administrator, root, sa, oracle и т.д.) в повседневной работе, допускается только для выполнения высоко привилегированных операций. Атрибуты безопасности (логин, пароль, криптографические ключи и т.д.) от высоко привилегированных встроенных и системных учетных записей должны храниться в запечатанном виде в конверте и храниться в недоступном месте от третьих лиц;* *5) Контроль и управление правами доступа администраторов должны осуществляться ответственным лицом за ИБ. В соответствии п. 5.1 стандарта 50739-2006 требования к разграничению доступа. Право изменять правила разграничения доступа должно быть предоставлено выделенным субъектам (например, администрации, службе безопасности).* *6) В соответствии с п.9.2.3 стандарта СТ РК ISO/IEC 27002-2015 управление привилегированными правами доступа, распределение и использование привилегированных прав доступа должно быть ограничено и управляемо.* *7) Согласно пп. 12.1.4 п. 12 СТ РК ISO/IEC 27002-2015 Необходимо исключить доступ разработчика к боевой среде.*
12	Функции управления доступом	Применение функций разграничения доступа основывается, по крайней мере, на следующих атрибутах безопасности: идентификаторы субъектов доступа; идентификаторы объектов доступа; адреса субъектов доступа; адреса объектов доступа; права доступа субъектов	*Управление доступом основывается, по крайней мере на следующих атрибутах безопасности:* *1) Атрибут «идентификатор»: идентификаторы субъектов доступа, идентификаторы объектов доступа;* *2) Атрибут «время»: ограничение доступа по времени суток, дни недели или календарный год:* *3) Атрибут «местоположение»: адреса субъектов доступа, адреса объектов доступа;* *4) Атрибут «группирование»: групповые и ролевые политики.* *п. 10.2 СТ РК ISO/IEC 15408-2-2017.*
13	Аутентификация данных	Поддержка гарантии правильности специфического набора данных, который	*Прикладное ПО должно регистрировать и отражать в наборе данных сведения о создателе набора данных или того, кто осуществил их*

		впоследствии используется для верификации того, что содержание информации не было подделано или модифицировано мошенническим путем	*модификацию. Рекомендуется так же сохранять время создания или модификации. Согласно пп. 5 п. 38 ППРК ЕТ: необходимо вести журналы регистрации событий в соответствии с форматами и типами записей, определенными в правилах мониторинга.* *Для важных данных должны применяться средства защиты от несанкционированной модификации, например, сохранение хеш-кода контрольной суммы или ЭЦП контента записи с проверкой соответствия при каждом чтении записи.* *В данном пункте согласно п. 10.3 СТ РК ISO/IEC 15408-2-2017 описываются специальные функции, используемые для аутентификации «статических» данных. Компоненты этого семейства используют при наличии требования аутентификации* ***«статических»*** *данных,* ***то есть, если данные обозначаются, но не передаются.*** *Функция может быть реализована с помощью односторонних хэш-функций (криптографической контрольной суммы, отображения отпечатков пальцев, хэш-образа сообщения) для генерации хэш-значения определяемого документа, которое может использоваться при верификации правильности или подлинности содержащейся в нем информации.* *Заявитель должен специфицировать список объектов или типов информации, для которых ФБО должны быть в состоянии генерировать свидетельство аутентификации данных.* *Заявитель должен специфицировать список субъектов, которые будут в состоянии верифицировать свидетельства аутентификации данных для объектов, указанных в предыдущем элементе. Список может перечислить субъекты, если все они известны, или описание субъектов в списке может носить более общий характер и ссылаться на «тип» субъекта, например, на идентифицированную роль.*
14	Экспорт данных за пределы действия функций безопасности ОИ (далее - ФБО)	Обеспечение при экспорте данных пользователя из ОИ защиты и сохранности или игнорирования их атрибутов безопасности	*При экспорте или другой передаче данных пользователя за пределы объекта, должны удаляться данные о пользователе, создавшего или осуществившего его передачу, например, удалить логины, адреса или наименования ПО из состава экспортируемого документа.*
15	Политика	Обеспечение предотвращения	*В случае если в объекте или в компоненте объекта осуществляется*

	управления информационными потоками	раскрытия, модификации и/или недоступности данных пользователя при их передаче между физически разделенными частями сервиса безопасности	*передача потока данных (балансировщик нагрузки, веб-фильтр, прокси-сервер и другое) необходимо проверить соответствие политики управления потоком данных обеспечивающих безопасность, отсутствие потерь, надежной защиты от прочтения и достоверность передачи.* *Применяется для шлюзов, балансировщиков, прокси-серверов и других передаточных компонентов.* *Должно применяться защищенное подключение между пользователем и сервером, а также между серверами находящимися в разных ЦОДах (основной и резервный).* *Информационное взаимодействие государственных информационных систем с другими государственными информационными системами должно осуществляться через шлюз «электронного правительства» (статья 43 Закона РК «Об информатизации».* *Информационное взаимодействие негосударственных информационных систем с другими государственными информационными системами или объектами информатизации «электронного правительства» должно осуществляться через внешний шлюз «электронного правительства» (статья 44 Закона РК «Об информатизации»).* *Информационное взаимодействие информационной системы субъектов информатизации, размещённой в выделенном сегменте локальной сети внешнего контура и в сегменте локальной сети внутреннего контура, должно осуществляться через внешний шлюз электронного правительства (ВШЭП) (пп. 10 и 11 п. 139 ППРК ЕТ).*
16	Функции управления информационными потоками	Организация и обеспечение контроля доступа к хранилищам данных с целью исключения бесконтрольного распространения информации, содержащейся в них (управление информационными потоками для реализации надежной защиты от раскрытия или модификации в условиях недоверенного ПО)	*Функции, которые применяются при управлении потоками данных (п.15) должны обеспечивать гарантированность доставки, отсутствие искажения данных и обеспечение управления доступом к данным.* *Применяется для шлюзов, балансировщиков, прокси-серверов и других передаточных компонентов* *Информационное взаимодействие государственных информационных систем с другими государственными информационными системами должно осуществляться через шлюз «электронного правительства» (статья 43 Закона РК «Об информатизации»).* *Информационное взаимодействие негосударственных информационных систем с другими государственными информационными системами или объектами информатизации «электронного правительства» должно осуществляться через внешний шлюз «электронного правительства»*

			(статья 44 Закона РК «Об информатизации»).
17	Импорт данных из-за пределов действия ФБО	Наличие механизмов для передачи данных пользователя в ОИ таким образом, чтобы эти данные имели требуемые атрибуты безопасности и защиту	*В случае осуществления импорта данных извне объекта испытаний, необходимо обеспечить сохранение данных для идентификации данных пользователя, времени импорта и других сведений о событии импорта данных.* *Импортом данных признается потоковый или форматированный ввод данных, осуществляемый пользователем или ПО из файлов или из других видов наборов данных, внешних по отношению к объекту испытаний.*
18	Передача в пределах ОИ	Наличие защиты данных пользователя при их передаче между различными частями ОИ по внутреннему каналу	*При передаче данных по внутренним связям внутри объекта, должны обеспечиваться защита от прослушивания при передаче конфиденциальной информации или аутентификационных данных пользователей.* *Как правило, внутри сред виртуализации такое требование не должно предъявляться.*
19	Защита остаточной информации	Обеспечение полной защиты остаточной информации, то есть недоступности предыдущего состояния при освобождении ресурса	*Если в процессе обработки или выдачи информации формируются временные данные (временные файлы, cookies, временные записи или временные таблицы в БД, импортированные данные) должна обеспечиваться защита таких данных от возможности использования другими пользователями. Такие данные должны уничтожаться или перемещаться в места, недоступные для других пользователей.*
20	Откат текущего состояния	Наличие возможности отмены последней операции или ряда операций, ограниченных некоторым пределом (например, периодом времени), и возврат к предшествующему известному состоянию. Откат предоставляет возможность отменить результаты операции или ряда операций, чтобы сохранить целостность данных пользователя	*В случае, если в объекте применяются долговременные или составные операции, конечный результат которых зависит от результата каждой из составной части, необходимо предусмотреть возможность отката состояния до начала такой операции (rollback) в случае неудачи, или успешного завершения (commit). Например, возможность возврата осуществляется путем восстановления из резервных копий, а также при использовании системы виртуализации путем снятия снимка виртуальной машины непосредственно перед выполнением операций.* *(п. 10.10 СТ РК ISO/IEC 15408-2-2017)*
21	Целостность хранимых данных	Обеспечение защиты данных пользователя во время их хранения в пределах ФБО	*Для защиты важных данных, хранящихся в файлах и в записях БД должны применяться методы, позволяющие контролировать наличие изменений в данных, совершенных нелегитимным путем, например, администратором БД непосредственно в полях записи, минуя ППО. Применяются контрольные суммы, хеш-функции контрольных сумм, в случае достаточной ценности данных, должна применяться ЭЦП. Для обеспечения целостности хранимых данных необходимо исключить права и привилегии у*

			администратора на модификацию данных. *(п. 10.11 СТ РК ISO/IEC 15408-2-2017)* *Согласно пп. 5 п. 38 ППРК ЕТ: необходимо вести журналы регистрации событий в соответствии с форматами и типами записей, определенными в правилах мониторинга.*
22	Защита конфиденциальности данных пользователя при передаче между ФБО	Обеспечение конфиденциальности данных пользователя при их передаче по внешнему каналу между ОИ и другим доверенным продуктом ИТ. Конфиденциальность осуществляется путем предотвращения несанкционированного раскрытия данных при их передаче между двумя оконечными точками. Оконечными точками могут быть ФБО или пользователь	*При передаче данных пользователя вне объекта (например, при интеграции), важные полезные данные должны защищаться шифрованием от возможности прослушивания.* *(п. 10.12 СТ РК ISO/IEC 15408-2-2017, п. 13.2 СТ РК ISO/IEC 27002-2015, п. 48 ППРК ЕТ)*
23	Защита целостности данных пользователя при передаче между ФБО	Обеспечивается целостность данных пользователя при их передаче между ФБО и другим доверенным продуктом ИТ, а также возможность их восстановления при обнаруживаемых ошибках	*При передаче данных пользователя вне объекта (например, при интеграции), важные полезные данные должны защищаться от модификации «налету» с применением методов, позволяющих выявить такие модификации, например циклические коды, контрольные суммы, для ценных данных должна применяться ЭЦП.* *(п. 13.2 СТ РК ISO/IEC 27002-2015)*
Идентификация и аутентификация			
24	Отказы аутентификации	Наличие возможности при достижении определенного администратором числа неуспешных попыток аутентификации отказать субъекту в доступе, сгенерировать запись регистрационного журнала и сигнализировать администратору о вероятном нарушении безопасности	*При превышении определенного количества попыток ввода неправильного пароля, учетная запись пользователя должна блокироваться на определенное время. Количество попыток и время блокировки определяется в Политике парольной защиты. Данная функция является основной защитой от атаки типа "brute force".* *(п. 11.1 СТ РК ISO/IEC 15408-2-2017)*
25	Определение атрибутов пользователя	Для каждого пользователя необходимо поддерживать, по крайней мере, следующие атрибуты безопасности: идентификатор; аутентификационная информация	*Проверяется наличие необходимых атрибутов для учетных записей пользователей, в том числе обязательные атрибуты ролевых и (при необходимости) групповых политик разграничения доступа.* *(п. 11.2 СТ РК ISO/IEC 15408-2-2017)*

		(например, пароль); права доступа (роль)	
26	Спецификация секретов	Если аутентификационная информация обеспечивается криптографическими операциями, поддерживаются также открытые и секретные ключи	*Проверяется наличие защиты процедур аутентификации, в том числе, визуальное закрытие пароля при вводе в интерфейсе пользователя, применение (при необходимости) ЭЦП, шифрование процедур обмена сессионными ключами (и других данных сессии пользователя), применение других средств обеспечения безопасности сессии пользователя.* *Необходимо проверить условия хранения и передачи секретов, в том числе, применение средств для шифрования паролей пользователей и интеграционных соединений от возможности прочтения или прослушивания.* *Проверяется:* - *наличие автоматической блокировки учетной записи при превышении срока действия пароля.* - *наличие процедуры смены пароля пользователя.* - *при смене пароля ставятся ограничения на минимальную длину и сложность пароля.* *(п. 11.3 СТ РК ISO/IEC 15408-2-2017)*
27	Аутентификация пользователя	Наличие механизмов аутентификации пользователя, предоставляемых ФБО	*Проверка наличия процедур аутентификации перед предоставлением доступа к данным и функциям, а так же (при необходимости) повторной аутентификации после определенных событий, например, перед получением доступа к важным данным.* *(п. 11.4 СТ РК ISO/IEC 15408-2-2017)*
28	Идентификация пользователя	Обеспечение: 1) успешности идентификации и аутентификации каждого пользователя до разрешения любого действия, выполняемого сервисом безопасности от имени этого пользователя; 2) возможностей по предотвращению применения аутентификационных данных, которые были подделаны или скопированы у другого пользователя; 3) аутентификации любого представленного идентификатора	*Перед предоставлением доступа, пользователь и/или его данные должны пройти аутентификацию, при этом должна обеспечиваться (при необходимости) его повторная идентификация. При этом данные, генерируемые в процессе аутентификации, должны быть скрыты от возможности доступа к ним.* *(п. 11.5 СТ РК ISO/IEC 15408-2-2017)*

		пользователя; 4) повторной аутентификации пользователя по истечении определенного администратором интервала времени; 5) предоставления пользователю функций безопасности только со скрытой обратной связью во время выполнения аутентификации.	
29	Связывание пользователь-субъект	Следует ассоциировать соответствующие атрибуты безопасности пользователя с субъектами, действующими от имени этого пользователя	*При необходимости, следует проверить обеспечение возможности идентификации конечного пользователя с его учетными данными.* *(п. 11.6 СТ РК ISO/IEC 15408-2-2017)*
	Управление безопасностью		
30	Управление отдельными функциями ФБО	Наличие единоличного права администратора на определение режима функционирования, отключения, подключения, модификации режимов идентификации и аутентификации, управления правами доступа, протоколирования и аудита	*Каждый администратор и пользователь должны использовать учетные записи (персонифицированный) с набором привилегий необходимым и достаточным для выполнения повседневных задач, без возможности модификации полезных данных, политики безопасности и изменения прав администраторов.* *Использование не персонифицированных встроенных административных учетных записей (admin, administrator, root, sa, oracle) допускается только для выполнения высокопривелигированных операций.* *Контроль и управление правами доступа администраторов должны осуществляться ответственным лицом за ИБ. В соответствии п. 5.1 стандарта 50739-2006 требования к разграничению доступа. Право изменять правила разграничения доступа должно быть предоставлено выделенным субъектам (например, администрации, службе безопасности).* *(п. 12.1 СТ РК ISO/IEC 15408-2-2017)*
31	Управление атрибутами безопасности	Наличие единоличного права администратора на изменения подразумеваемых значений, опрос, изменения, удаления, создания атрибутов безопасности, правил управления потоками информации. При этом	*Необходимо обеспечить управление атрибутами безопасности ответственным лицом за ИБ (например, учетными записями, паролями, ролями и т.д.).* *(п. 12.2 СТ РК ISO/IEC 15408-2-2017)*

		необходимо обеспечить присваивание атрибутам безопасности только безопасных значений	
32	Управление данными ФБО	Наличие единоличного права администратора на изменения подразумеваемых значений, опрос, изменения, удаления, очистки, определения типов регистрируемых событий, размеров регистрационных журналов, прав доступа субъектов, сроков действия учетных записей субъектов доступа, паролей, криптографических ключей	*Доступ для управления данными аудита должен иметь только ответственный за ИБ, у остальных администраторов доступ только для чтения.* *(п. 12.3 СТ РК ISO/IEC 15408-2-2017)*
33	Отмена атрибутов безопасности	Наличие осуществления отмены атрибутов безопасности в некоторый момент времени. Только у уполномоченных администраторов имеется возможность отмены атрибутов безопасности, ассоциированных с пользователями. Важные для безопасности полномочия отменяются немедленно	*Необходимость в отмене атрибутов безопасности для учетных записей пользователя или для ППО возникает при изменении условий использования объекта, например, во время отпуска, изменения должностных функций, при попытке доступа из мест, не определенных как штатное место доступа (из интернета или из-за пределов РК). При этом, ограничивать доступ могут только соответствующие администраторы и ответственные лица за ИБ.* *(п. 12.4 СТ РК ISO/IEC 15408-2-2017)*
34	Срок действия атрибута безопасности	Обеспечение возможности установления срока действия атрибутов безопасности	*Необходимо обеспечить ограничение срока действия атрибутов безопасности (например, пароль, криптографические ключи, учетная запись и т.д.).* *(п. 12.5 СТ РК ISO/IEC 15408-2-2017)*
35	Роли управления безопасностью	1) Обеспечение поддержки, по крайней мере, следующих ролей: уполномоченный пользователь, удаленный пользователь, администратор. 2) Обеспечение получения ролей удаленного пользователя и администратора только по запросу	*Для средних и крупных объектов должна быть предусмотрена иерархия администраторов:* *1) администратор безопасности – чаще всего, это ответственный за ИБ, имеющий право создавать других администраторов и не имеющего права доступа к полезным данным пользователей. У него хранятся пароли суперпользователей;* *2) администратор пользователей – создает и управляет учетными записями только простых пользователей и имеет права по доступу к данным пользователей только для чтения;* *3) администратор данных – имеет доступ к данным, хранящимся в БД*

			только для чтения. *(п. 12.7 СТ РК ISO/IEC 15408-2-2017)*
	Защита ФБО		
36	Безопасность при сбое	Сохранение сервисом безопасного состояния при аппаратных сбоях (вызванных, например, перебоями электропитания)	*Должна обеспечиваться резервным копированием данных пользователей, конфигурационных файлов и настроек, исполняемых файлов ППО, данных и файлов СУБД, среды виртуализации и ОС.* *Необходимо определить условия хранения и доступность для администраторов резервных копий. Места хранения резервных копий должны быть доступны только авторизованному для этого персоналу. При этом место хранения копий не должно быть повержено риску повреждения вместе с объектом.* *Должны быть предусмотрены как минимум два режима резервного копирования – полное копирование (не реже 1 раза в месяц) и инкрементное копирование (не реже 1 раза в день для слабо активных объектов. Для объектов, у которых обновление данных осуществляется активно, должны предусматриваться более частые периоды копирования).* *Резервные копии должны регулярно тестироваться на восстановление.* *Для защиты от сбоя сервера применяются отказоустойчивые кластеры.* *(п. 14.1 СТ РК ISO/IEC 15408-2-2017)* *Необходимо резервирование аппаратно-программных средств обработки данных, систем хранения данных, компонентов сетей хранения данных и каналов передачи данных, в том числе для объектов информатизации ЭП:* *первого класса в соответствии с классификатором – нагруженное (горячее) в резервном серверном помещении;* *второго класса в соответствии с классификатором – не нагруженное (холодное) в резервном серверном помещении;* *третьего класса в соответствии с классификатором – хранение на складе в непосредственной близости от основного серверного помещения.* *(п. 49 ППРК ЕТ).*
37	Доступность экспортируемых данных ФБО	Предоставление сервисом возможности верифицировать доступность всех данных при их передаче между ним и удаленным доверенным продуктом информационных технологий и выполнять повторную передачу информации, а также	*При осуществлении передачи учетных данных за пределы объекта, например, при интеграции необходимо удостовериться, что такие данные передаются получателю достоверно (квитирование с проверкой целостности) и регистрацию событий сбоя или искажения передачи с повторением передачи. (п. 14.2 СТ РК ISO/IEC 15408-2-2017)*

		генерировать запись регистрационного журнала, если модификации обнаружены	
38	Конфиденциальность экспортируемых данных ФБО	Предоставление сервисом возможности верифицировать конфиденциальность всех данных при их передаче между ним и удаленным доверенным продуктом информационных технологий и выполнять повторную передачу информации, а также генерировать запись регистрационного журнала, если модификации обнаружены	*При осуществлении передачи учетных данных пользователей за пределы объекта, например при интеграции, необходимо удостовериться, что такие данные передаются получателю без возможности прослушивания, например, с применением шифрования. (п. 14.3 СТ РК ISO/IEC 15408-2-2017)*
39	Целостность экспортируемых данных ФБО	Предоставление сервисом возможности верифицировать целостность всех данных при их передаче между ним и удаленным доверенным продуктом информационных технологий и выполнять повторную передачу информации, а также генерировать запись регистрационного журнала, если модификации обнаружены	*При осуществлении передачи учетных данных за пределы объекта, например при интеграции, необходимо удостовериться, что такие данные передаются получателю без потери целостности, например, с применением шифрования, ЭЦП, контрольной суммы, циклических кодов.* *(п. 14.4 СТ РК ISO/IEC 15408-2-2017)*
40	Передача данных ФБО в пределах ОИ	Сервис предоставляет возможность верифицировать доступность. Предоставление сервисом возможности конфиденциальности и целостности всех данных при их передаче между ним и удаленным доверенным продуктом информационных технологий и выполнять повторную передачу информации, а также генерировать запись регистрационного журнала, если модификации обнаружены	*При осуществлении передачи учетных данных внутри объекта, например между серверами, необходимо удостовериться, что такие данные передаются получателю без потери конфиденциальности, например, с применением шифрования.*
41	Физическая защита ФБО	Осуществление физической защиты ФБО	*Чек-лист по ФБО*
42	Надежное восстановление	Когда автоматическое восстановление после сбоя или прерывания обслуживания невозможно,	*Необходимо удостовериться в наличии надежных процедур восстановления работоспособности объекта после сбоя с применением автоматизированных процедур из резервных копий.*

		сервис переходит в режим аварийной поддержки, позволяющей вернуться к безопасному состоянию. После аппаратных сбоев обеспечивается возврат к безопасному состоянию с использованием автоматических процедур	*Наличие скриптов или ПО для такой автоматизации обусловлено сложностями процедур восстановления, как правило, проходящих ночью или в стесненных условиях.* *(п. 14.7 СТ РК ISO/IEC 15408-2-2017)*
43	Обнаружение повторного использования	Обеспечение обнаружения сервисом повторного использования аутентификационных данных, отказа в доступе, генерирования записи регистрационного журнала и сигнализирования администратору о вероятном нарушении безопасности	*Необходимо проверить наличие журналирования событий доступа пользователей к временным данным (файлам, таблицам, данным аутентификации) и отслеживания или оповещения о таких событий.*
44	Посредничество при обращениях	Обеспечение вызова и успешного выполнения функций, осуществляющих политику безопасности сервиса, прежде чем разрешается выполнение любой другой функции сервиса	*Функция обеспечивающая удаление пользователя от источника данных, например, доступ к СУБД с БД должен осуществляться через сервер приложений. При этом должна быть гарантирована невозможность обхода домена безопасности*
45	Разделение домена	Поддержка отдельного домена для собственного выполнения функций безопасности, который защищает их от вмешательства и искажения недоверенными субъектами	*Важные компоненты объекта должны защищаться от пользователя другими последовательными компонентами – доменами безопасности.* *Например, для СУБД доменом является сервер приложений, для сервера приложений – веб-сервер, для веб-сервера – обратный прокси-сервер или WAF и т.д.*
46	Протокол синхронизации состояний	Обеспечение синхронизации состояний при выполнении идентичных функций на серверах	*В случае, если в объекте имеется несколько компонентов, идентичных по функционалу или по содержанию (несколько узлов кластера или резервный сервер БД) процедуры синхронизации должны обеспечивать идентичное состояние программной среды, настроек конфигурации, перечня учетных записей, содержания записей и настроек БД и т.д.* *(п. 14.9 СТ РК ISO/IEC 15408-2-2017)*
47	Метки времени	Предоставление для использования функциями безопасности надежных меток времени	*Все компоненты объекта должны осуществлять синхронизацию внутренних часов от одного источника времени.* *(п. 14.10 СТ РК ISO/IEC 15408-2-2017)* *Необходимо обеспечить синхронизацию времени в журналах событий, всех серверов с эталоном времени и частоты, воспроизводящим национальную шкалу всемирного координированного времени UTC (kz). (п. 139*

			ППРК ЕТ)
48	Согласованность данных между ФБО	Обеспечение согласованной интерпретации регистрационной информации, а также параметров используемых криптографических операций	*В случае, если в объекте имеется несколько точек авторизации, подключения пользователей или несколько доменов LDAP или AD, должны быть настроены процедуры синхронизации данных учетных записей и зарегистрированных криптографических ключей.* *(п. 14.11 СТ РК ISO/IEC 15408-2-2017)*
49	Согласованность данных ФБО при дублировании в пределах ОИ	Обеспечение согласованности данных функций безопасности при дублировании их в различных частях объекта испытаний. Когда части, содержащие дублируемые данные, разъединены, согласованность обеспечивается после восстановления соединения перед обработкой любых запросов к заданным функциям безопасности	*В случае, если в объекте имеется несколько площадок, например, основной и резервный ЦОД, отдельные ЦОДы в регионах, должны быть настроены процедуры синхронизации данных учетных записей и зарегистрированных криптографических ключей.* *(п. 14.13 СТ РК ISO/IEC 15408-2-2017)* *Для обеспечения доступности и отказоустойчивости владельцами объектов информатизации ЭП обеспечиваются:* *1) наличие резервного собственного или арендованного серверного помещения для объектов информатизации ЭП первого и второго классов в соответствии с классификатором;* *2) резервирование аппаратно-программных средств обработки данных, систем хранения данных, компонентов сетей хранения данных и каналов передачи данных, в том числе для объектов информатизации ЭП:* - *первого класса в соответствии с классификатором – нагруженное (горячее) в резервном серверном помещении;* - *второго класса в соответствии с классификатором – не нагруженное (холодное) в резервном серверном помещении;* - *третьего класса в соответствии с классификатором – хранение на складе в непосредственной близости от основного серверного помещения.* *(п. 49 ППРК ЕТ).*
50	Самотестирование ФБО	Для демонстрации правильности работы функций безопасности при запуске, периодически в процессе нормального функционирования и/или по запросу администратора выполнение пакета программ самотестирования. У администратора наличие возможности верифицировать целостность данных и выполняемого кода функций	*Должны быть процедуры тестирования работоспособности процедур авторизации.*

		безопасности	
	Использование ресурсов		
51	Отказоустойчивость	Обеспечение доступности функциональных возможностей объекта испытаний даже в случае сбоев. Примеры таких сбоев: отключение питания, отказ аппаратуры, сбой ПО	*Должны быть предусмотрены средства обеспечения работоспособности или восстановления объекта после серьезного сбоя или отказа системы, например, отказ сервера или пожар в ЦОДе.* *Достигается наличием резервного оборудования, резервного ЦОДа.* *Для ИС 1 класса – подключенных в активном нагруженном состоянии как два узла одного кластера, расположенных в удаленных друг от друга ЦОДах, для ИС 2 класса – холодное резервирование идентичного оборудования, расположенных в удаленных друг от друга ЦОДах, ИС 3 класса – резервное оборудование на складе.* *Для защиты от сбоя сервера применяются отказоустойчивые кластеры.* *(п. 15.1 СТ РК ISO/IEC 15408-2-2017)*
52	Приоритет обслуживания	Обеспечение управления использованием ресурсов пользователями и субъектами в пределах своей области действия так, что высокоприоритетные операции в пределах объекта испытаний всегда будут выполняться без препятствий или задержек со стороны операций с более низким приоритетом	*Устанавливаются процедуры или пользователи, запросы которых обслуживаются вне очереди или в первоочередном режиме.* *Такие операции требуются в тех случаях, когда от своевременности выполнения зависит какой-то технологический процесс с ограничением на реактивность или если пользователь должен иметь возможность получения результата вне зависимости от присутствия запросов от других пользователей.* *(п. 15.2 СТ РК ISO/IEC 15408-2-2017)*
53	Распределение ресурсов	Обеспечение управления использованием ресурсов пользователями и субъектами таким образом, чтобы не допустить несанкционированные отказы в обслуживании из-за монополизации ресурсов другими пользователями или субъектами	*Должны быть предусмотрены автоматические процедуры по мониторингу и разблокировке монополизированных ресурсов, роста очередей на обслуживание. Например, загрузка процессов чтения и записи в СУБД.* *Применяемые ресурсы системы должны иметь необходимый запас для работы, например, необходимый расчетный объем жесткого диска.* *(п. 15.3 СТ РК ISO/IEC 15408-2-2017).*
	Доступ к ОИ		
54	Ограничение области выбираемых атрибутов	Ограничение как атрибутов безопасности сеанса, которые может выбирать пользователь, так и атрибутов субъектов, с которыми пользователь может быть связан, на основе метода или	*При доступе к объекту должны ставиться ограничения по доступу в зависимости от:* - *времени суток - во внерабочее время, в выходные или праздничные дни,* - *способа подключения из локальной сети, из ЕТС ГО, из казахстанского Интернета, из зарубежного Интернета.*

		места доступа, порта, с которого осуществляется доступ, и/или времени (например, времени суток, дня недели)	*(п. 16.1 СТ РК ISO/IEC 15408-2-2017).*
55	Ограничение на параллельные сеансы	Ограничение максимального числа параллельных сеансов, предоставляемых одному пользователю. У этой величины подразумеваемое значение устанавливается администратором	*При попытке подключения пользователя с учетной записью, уже имеющей активный сеанс пользователя:* *1) уже открытый сеанс закрывается;* *2) новый сеанс блокируется.* *Проверяется с целью недопущения бесконтрольного использования одной учетной записи большим числом пользователей.* *(п. 16.2 СТ РК ISO/IEC 15408-2-2017).*
56	Блокирование сеанса	Принудительное завершение сеанса работы по истечении установленного администратором значения длительности бездействия пользователя	*Блокировка сеанса в целях недопущения использования объекта от имени пользователя, отошедшего на время.* *(п. 16.3 СТ РК ISO/IEC 15408-2-2017).*
57	Предупреждения перед предоставлением доступа к ОИ	Обеспечение возможности еще до идентификации и аутентификации отображения для потенциальных пользователей предупреждающего сообщения относительно характера использования объекта испытаний	*Перед авторизацией пользователя для конфиденциальных объектов должно появляться предупреждение о санкциях за нарушения при использовании объекта. Например, баннера с предупреждением и ссылкой на статьи КоАП или УК.* *(п. 16.4 СТ РК ISO/IEC 15408-2-2017).*
58	История доступа к ОИ	Обеспечение возможности отображения для пользователя, при успешном открытии сеанса, истории неуспешных попыток получить доступ от имени этого пользователя. Эта история может содержать дату, время, средства доступа и порт последнего успешного доступа к объекту испытаний, а также число неуспешных попыток доступа к объекту испытаний после последнего успешного доступа идентифицированного пользователя	*Пользователь после авторизации должен получать информацию о последнем удачном и неудачном входе, на случай, если были попытки подбора пароля или нелегитимного использования учетной записи.* *(п. 16.5 СТ РК ISO/IEC 15408-2-2017).*
59	Открытие сеанса с ОИ	Обеспечение сервисом способности отказать в открытии сеанса, основываясь на идентификаторе субъекта, пароле субъекта, правах доступа субъекта	*Объект должен иметь процедуры ограничения в доступе пользователя по различным причинам, например, заблокирован по причине увольнения, несоответствия уровня доступа к информации, времени суток, местоположения и т.д.*

			(п. 16.6 СТ РК ISO/IEC 15408-2-2017).
	Функции защиты от вредоносного кода		
60	Наличие средств антивирусной защиты	Применение для защиты от вредоносного кода средств мониторинга, обнаружения и блокирования или удаления вредоносного кода на серверах и при необходимости, на рабочих станциях объекта испытаний	*Наличие полно функциональной версии антивируса.* *(п. 54 ППРК ЕТ).*
61	Лицензии для средств антивирусной защиты	Наличие у средств антивирусной защиты лицензии (приобретенной, ограниченной, свободно распространяемой) на сервера и рабочие станции	*Наличие легитимной версии антивируса.* *(пп. 4 п. 79 ППРК ЕТ).*
62	Обновление баз сигнатур и программного обеспечения средств антивирусной защиты	Обеспечение регулярного обновления и поддержания в актуальном состоянии средств антивирусной защиты	*Наличие возможности регулярного обновления антивируса. Особенно важно для Windows-серверов в закрытых сетях, например ЕТС ГО - подключение к Интернету для обновления недопустимо и тщательно проверяется.*
63	Управление доступом к средствам антивирусной защиты	Осуществление централизованного управления и конфигурирования средств антивирусной защиты	*Проверяется наличие серверного центра сбора сведений о вирусной активности и работоспособности антивирусов на серверах объекта.*
64	Управление защитой от вредоносного кода на внешних электронных носителях информации средствами антивирусной	Обеспечение управлением защитой от вредоносного кода на внешних электронных носителях информации проверки и блокировки файлов и при необходимости носителей информации.	*Проверка автоматического контроля на наличие вирусов на подключаемых переносных носителях, например, блокировка файлов на флешках до завершения проверки на наличие вирусов*

	защиты		
	Безопасность при обновлении ПО		
65	Регулярное обновление ПО	Обеспечение регулярного обновления общесистемного и прикладного ПО серверов и рабочих станций	*Проверяется наличие процедур обновления ПО на серверах с предварительной проверкой корректности скачивания и тестирования обновлений.*
66	Обновление ПО в сетевых средах без доступа к серверам обновления в Интернете	Обеспечение обновления ПО в сетевых средах без доступа к серверам обновления в Интернете от специализированного сервера обновлений	*Для закрытых сетей проверяется наличие промежуточного сервера обновления, например, WSUS для операционных систем семейства Windows и сервера репозитория для систем семейства Linux.*
	Безопасность при внесении изменений в прикладное ПО		
67	Среда разработки и тестирования прикладного ПО	Обеспечение наличия среды для разработки и тестирования прикладного ПО, изолированной от среды промышленной эксплуатации прикладного ПО	*Из среды промышленной эксплуатации не должны быть доступны средства программирования и исходные коды. Среда разработки должна поддерживать учет версионности ППО. Не допускается использование реальной учетой записи пользователей систем, находящихся в промышленной эксплуатации; не подлежат копированию данные из ИС, находящихся в промышленной эксплуатации, в испытательную среду пп. 3 п. 98 ППРК ЕТ).*
68	Разграничение доступа в средам разработки и тестирования прикладного ПО	Обеспечение управления доступом к средам разработки и тестирования прикладного ПО для программистов и администраторов	*Разработчики не должны иметь доступ к среде промышленной эксплуатации.*
69	Система развертывания прикладного ПО	Наличие системы развертывания (распространения) прикладного ПО на серверах и рабочих станциях среды промышленной эксплуатации	*Система развертывания новых версий должна обеспечивать санкционированную процедуру развертывания новой версии ППО.*
70	Разграничение доступа к системе развертывания прикладного	Обеспечение управления доступом к системе развертывания (распространения) прикладного ПО на серверах и рабочих станциях среды промышленной эксплуатации	*Доступ к средам разработки, тестирования и промышленной эксплуатации должен быть строго разграничен между разработчиками и эксплуатационщиками.*

	ПО		

Перечень сокращений и аббревиатур:

ОИ – объект испытаний;
ОС – операционная система;
ЭЦП – электронная цифровая подпись;
БД – база данных;
СУБД – система управления базами данных;
ППО – прикладное программное обеспечение;
ПО – программное обеспечение;
ИС – информационная система;
ЭП – электронное правительство;
ИБ – информационная безопасность;
ЦОД – центр обработки данных;
ЕТС ГО – единая транспортная среда государственных органов Республики Казахстан;
Закон – Закон Республики Казахстан от 24 ноября 2015 года № 418-V ЗРК Об информатизации.
ППРК ЕТ – Единые требования в области информационно-коммуникационных технологий и обеспечения информационной безопасности, утвержденные постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832.
Правила мониторинга – Об утверждении Правил проведения мониторинга обеспечения информационной безопасности объектов информатизации "электронного правительства" и критически важных объектов информационно-коммуникационной инфраструктуры, приказ Министра оборонной и аэрокосмической промышленности Республики Казахстан от 28 марта 2018 года № 52/НҚ.