Перечень процессов обеспечения информационной безопасности и их содержание

№ п/п	Наименование процессов	Требование к содержанию процессов обеспечения ИБ	Пояснительная информация
1	**2**	**3**	**4**
1	Управление активами, связанными с информационно-коммуникационными технологиями	1. Идентификация активов в соответствии с порядком идентификации активов, определенном в Правилах идентификации, классификации и маркировки активов, связанных со средствами обработки информации; 2. Классификация информации в соответствии с системой классификации, определенной в Правилах идентификации, классификации и маркировки активов, связанных со средствами обработки информации. 3. Проверка класса, определенного для объекта испытаний на соответствие требованиям правил классификации объектов информатизации; 4. Маркировка активов в соответствии с принципами маркировки, определенными в Правилах идентификации, классификации и маркировки активов, связанных со средствами обработки информации; 5. Закрепление ответственных лиц за идентифицированными активами; 6. Ведение и актуализация реестра активов в соответствии с принятой формой реестра; 7. Определение, документирование и реализация процедур обращения с активами (выдача, использование, хранение, внос/вынос и возврат) в соответствии с системой классификации, определенной в Правилах идентификации, классификации и маркировки активов, связанных со средствами обработки информации; 8. Паспортизация средств вычислительной техники, телекоммуникационного оборудования и программного	*1. В организации должна быть выстроена процедура идентификации активов (установление активов) (по итогам работ идентификации активов, для каждого актива дается оценка его ценности, важности, критичности, конфиденциальности и определяется его ценность, используются следующие 3 уровня «высокий», «средний», «низкий» (в случае потери активом его свойств безопасности с нарушением конфиденциальности, целостности и доступности).* *Выполнение процедуры идентификации активов должно подтверждаться составлением и утверждением Реестра активов, а также посредством проведения инвентаризации в соответствии с Правилами инвентаризации и паспортизации средств вычислительной техники, телекоммуникационного оборудования и программного обеспечения).* *2. Необходимо проводить классификацию информации, циркулирующей в ИС и интернет-ресурсах в соответствии с системой классификации, которая должна быть определена в Правилах идентификации, классификации и маркировки активов, связанных со средствами обработки информации (Например, конфиденциальные данные, персональные данные и т.п.).* *Необходимо отразить (оформить) результаты классификации информации документально и утвердить данный документ.* *3. Необходимо определить класс ОИ, например, в (ТЭО, ТЗ согласно Правилам классификации объектов информатизации, и классификатор объектов*

		обеспечения; 9. Безопасная организация работ при приеме/отгрузке активов, связанных с информационно-коммуникационными технологиями; 10. Безопасная утилизация (повторное использование) серверного и телекоммуникационного оборудования, систем хранения данных, рабочих станций, носителей информации.	*информатизации», утвержденные Приказом и.о. Министра по инвестициям и развитию Республики Казахстан от 28 января 2016 года № 135 или информация с архитектурного портала "электронного правительства). Документ должен утверждаться владельцем ОИ (Например, первым Руководителем, Заместителем Руководителя и т.д.).* *4. В организации должен быть реализован набор процедур маркировки активов, в том числе, и информации, соответствующий принципам маркировки, определенным в Правилах идентификации, классификации и маркировки активов, связанных со средствами обработки информации. Процедуры для маркировки активов должны охватывать физические и информационные активы. Объекты, которые должны быть приняты во внимание, должны включать: серверную инфраструктуру, телекоммуникационную инфраструктуру, сетевую инфраструктуру, электро-фурнитуру и т.д. Для виртуальных активов, виртуальные сервера, виртуальные свитчи, сети, подсети, виртуальные диски, которые не могут быть помечены физически, должны быть использованы электронные средства маркировки.* *5. Должно быть осуществлено закрепление ответственных лиц за идентифицированными активами.* *Документально должна быть закреплена обязанность владельцев активов по обеспечению их ИБ.* *6. В организации должен вестись реестр активов.* *Форма реестра активов должна соответствовать той, что будет определена в Правилах идентификации, классификации и маркировки активов, связанных со средствами обработки информации.* *7. В документе(-ах) необходимо определить процедуры безопасного обращения с активами, учитывающие схему классификации активов.* *Содержание процедур безопасного обращения с мобильными устройствами должно соответствовать*

			рекомендациям пункта 6.2.1 СТ РК 27002-2015. *В организации необходимо придерживаться реализации политики чистого стола и чистого экрана. Необходимо рассмотреть следующие рекомендации:* *a) чувствительная или критическая бизнес-информация, например, на бумаге или на электронных носителях данных, должна быть заперта (идеально в сейфе или в кабинете или других формах мебели безопасности) особенно когда офис освобожден.* *b) следует выполнить выход из компьютера или терминалов или защитить экраном и клавишным механизмом захвата, которым управляет пароль, знаком или аналогичным пользовательским механизмом идентификации, когда не проводится работа и должен быть защищен замками, паролями или другими средствами управления если не используется;* *c) несанкционированное использование фотокопировальных устройств и другой технологий воспроизводства (например, сканеры, цифровые фотоаппараты) должно быть предотвращено;* *d) информация, содержащая чувствительные или секретные данные, должна быть немедленно удалена из принтеров.* *8. В организации необходимо осуществлять инвентаризацию активов, связанных с ИКТ.* *Необходимо осуществлять паспортизацию СВТ и ПО, согласно Правил инвентаризации и паспортизации средств вычислительной техники, телекоммуникационного оборудования и программного обеспечения.* *Необходимо закрепление ответственных лиц за паспортизацию средств вычислительной техники и ПО документально.* *9. В организации должны быть документально определены процедуры безопасной организации работ при приеме/отгрузке активов. Определена ответственность за*

			несоблюдение этих процедур. (Например, Правилами инвентаризации и паспортизации средств вычислительной техники). *Процедуры безопасной организации работ должны соответствовать рекомендациям пункта 11.1.6 СТ РК 27002-2015.* *10. В организации необходимо документально определить процедуры безопасной утилизации и(или) повторного использования серверного и телекоммуникационного оборудования, систем хранения данных, рабочих станций, носителей информации и определена ответственность за несоблюдение этих процедур. Процедуры утилизации и(или) подготовки к повторному использованию серверного и телекоммуникационного оборудования, систем хранения данных, рабочих станций, носителей информации, должны соответствовать требованиям, определенным в ТД по ИБ.*
2	Организация информационной безопасности	1. Наличие подразделения информационной безопасности или сотрудника, ответственного за информационную безопасность, обособленного от подразделения информационных технологий, подчиняющегося непосредственно высшему руководству; 2. Функционирование рабочих групп и проведение совещаний по вопросам координации работ и обеспечения информационной безопасности; 3. Разработка (актуализация), утверждение, одобрение руководством технической документации по информационной безопасности, доведение их содержимого до сотрудников и привлекаемых со стороны исполнителей; 4. Поддержание контактов с полномочными органами, профессиональными сообществами, профессиональными ассоциациями или форумами специалистов по информационной безопасности;	*1. В целях разграничения ответственности и функций в сфере обеспечения ИБ создается подразделение ИБ, являющееся структурным подразделением, обособленным от других структурных подразделений, занимающихся вопросами создания, сопровождения и развития объектов информатизации, или определяется должностное лицо, ответственное за обеспечение ИБ. Сотрудники, ответственные за обеспечение ИБ, проходят специализированные курсы в сфере обеспечения ИБ не реже одного раза в три года с выдачей сертификата (требование п.30 ППРК ЕТ).* *2. Руководство должно демонстрировать поддержку политики информационной безопасности, ее процедур и мер управления (проводить совещания и координацию по вопросам ИБ). Неэффективный менеджмент может являться причиной того, что персонал будет чувствовать себя недооцененным, что в дальнейшем может иметь негативные последствия для организации. Например,*

		5. Определение и документирование процедур обеспечения информационной безопасности, в том числе, при привлечении сторонних организаций; 6. Разработка (пересмотр) соглашения о конфиденциальности или неразглашении, отражающие потребности в защите информации; 7. Определение и включение в соглашения со сторонними организациями требований по информационной безопасности и уровня обслуживания. Контроль за реализацией положений соглашения.	*неэффективный менеджмент может привести к игнорированию безопасности или возможному нецелевому использованию активов организации.* *3. ТД по ИБ создается в виде четырехуровневой системы документированных правил, процедур, практических приемов или руководящих принципов, которыми руководствуется ГО, МИО или организация в своей деятельности.* *4. ТД по ИБ разрабатывается на казахском и русском языках, утверждается правовым актом ГО, МИО или организации и доводится до сведения всех служащих ГО, МИО или работников организации.* *5. ТД по ИБ пересматривается с целью анализа и актуализации изложенной в них информации не реже одного раза в два года.* *6. Должны поддерживаться соответствующие контакты со специализированными профессиональными группами или участниками форумов по безопасности, а также с профессиональными ассоциациями.* *7. Сотрудники, подрядчики и представители третьей стороны, имеющие доступ к чувствительной информации, должны подписывать соглашение о конфиденциальности или* *8. неразглашении прежде, чем им будет предоставлен доступ к средствам обработки информации.*
3	Безопасность, связанная с персоналом	1. Предварительная проверка кандидатов при приеме на работу; 2. Определение, назначение и отражение в должностных инструкциях и (или) условиях трудового договора сотрудников и привлекаемых со стороны исполнителей ролей, обязанностей и ответственности, связанных с информационной безопасностью в период занятости, изменения или прекращения трудовых отношений и обязательств владельца объекта испытаний;	*1. В организации должна проводится предварительная проверка кандидатов при приеме на работу в случае, если работник принимается на должность, связанную с ИБ (проверка полноты и точности сведений резюме кандидата, возможно проверки уголовного прошлого или кредитной истории, соразмерные с предполагаемыми рисками при доступе к информации и (или) средствам обработки информации).* *2. Функциональные обязанности по обеспечению ИБ и обязательства по исполнению требований ТД по ИБ*

		3. Определение и документирование процедур увольнения сотрудников, имеющих обязательства в области обеспечения информационной безопасности; 4. Определение и регламентирование действий, которые будут предприняты к нарушителям правил информационной безопасности; 5. Извещение сотрудников об изменениях в политиках, правилах и процедурах обеспечения информационной безопасности, затрагивающих исполнение их служебных обязанностей; 6. Осведомленность и исполнение сотрудниками и привлекаемыми со стороны исполнителями об обязанностях и ответственности, связанными с обеспечением информационной безопасности в период занятости, изменения или прекращения трудовых отношений; 7. Обучение и подготовка сотрудников в сфере информационной безопасности; 8. Ответственность руководства за обеспечение возможности выполнения сотрудниками и привлекаемыми со стороны исполнителями обязательств в отношении информационной безопасности.	*служащих ГО, МИО или работников организации вносятся в должностные инструкции и (или) условия трудового договора (требования п.40 ППРК ЕТ).* *3. Необходимо в документах определить процедуры увольнения работников, имеющих обязательства в области обеспечения ИБ.* *Исполнение процедуры увольнения работников, имеющих обязательства в области обеспечения ИБ должны фактически подтверждаться.* *4. Необходимо в документах описать действия (процедуры), которые будут предприняты к нарушителям требований ИБ (служебные проверки, дисциплинарные наказания).* *Определить какими документами будут подтверждаться действия (процедуры), предпринимаемые к нарушителям требований ИБ (приказы и т.д.).* *5. В организации должны осуществляться извещения работников об изменениях в политиках, правилах и процедурах обеспечения информационной безопасности, затрагивающих исполнение их служебных обязанностей.* *Извещение работников об изменениях в политиках, правилах и процедурах обеспечения ИБ, затрагивающих исполнение их служебных обязанностей должны подтверждаться документально.* *6. Осведомленность работников об обязанностях и ответственности, связанная с обеспечением ИБ, должна подтверждаться подписанием листов ознакомления либо другим способом с ТД по ИБ, где отражаются все требования по вопросам ИБ.* *В организации контроль за исполнением работниками и привлекаемыми со стороны исполнителями обязанностей по соблюдению требований ИБ должен осуществляться ответственными за ИБ.* *7. В организации должны проводиться обучения (инструктажи) работников по вопросам ИБ.*

			Работниками организации ответственными за ИБ должны проводиться инструктажи с работниками сторонних организаций, имеющими доступ к средствам обработки информации по вопросам ИБ. *Проведение в организации обучения (инструктажи) по вопросам ИБ должно подтверждаться документально.* *8. Ответственность руководства за обеспечение возможности выполнения работниками организации и привлекаемыми со стороны исполнителями обязательств в отношении ИБ должна быть определена в ТД по ИБ.* *Ответственность руководства за обеспечение возможности выполнения работниками обязательств в отношении ИБ должна включать рекомендации пункта 7.2.1 СТ РК 27002-2015.*
4	Мониторинг событий ИБ и управление инцидентами ИБ	1. Регистрация действий пользователей, операторов, администраторов и событий операционных систем, систем управления базой данных, антивирусного ПО, прикладного ПО, телекоммуникационного оборудования, систем обнаружения и предотвращения атак, системы управления контентом; 2. Ведение, хранение и защита журналов регистрации событий; 3. Осуществление анализа журналов регистрации событий; 4. Мониторинг зарегистрированных событий и оповещение о событиях высокой и критичной степени важности для информационной безопасности; 5. Оценка и принятие решения по событию информационной безопасности; 6. Разработка, документирование, доведение до сведения сотрудников и привлекаемых со стороны исполнителей, выполнение процедур реагирования на инциденты информационной безопасности; 7. Проведение анализа инцидентов информационной безопасности.	*1. В организации ответственным подразделением/лицом за ИБ должна производиться регистрация действий пользователей, операторов, администраторов и событий операционных систем, систем управления базой данных, антивирусного ПО, прикладного ПО, телекоммуникационного оборудования, систем обнаружения и предотвращения атак, системы управления контентом.* *1) Необходимо вести журналы событий, регистрирующие действия:* - *администраторов,* - *операторов,* - *пользователей* *2) Необходимо вести журналы событий, регистрирующие события:* - *операционных систем,* - *систем управления базой данных,* - *антивирусного ПО,* - *прикладного ПО,* - *телекоммуникационного оборудования,*

			- *систем обнаружения и предотвращения атак,* - *системы управления контентом* *3) журналы событий должны соответствовать требованиям пунктов 12.4.1 и 12.4.3 СТ РК 27002-2015.* *2. Места хранения журналов событий должны соответствовать требованиям ИБ.* *Журналы регистрации событий должны быть обеспечены защитой от вмешательства и неавторизованного доступа. Применяемые способы защиты журналов событий должны соответствовать требованиям пункта 12.4.2 СТ РК 27002-2015.* *Фактический срок хранения журналов регистрации событий, должен соответствовать установленному в подпункте 4) пункта 38 ППРК ЕТ (журналы регистрации событий хранятся в течение срока, указанного в ТД ИБ, но не менее трех лет и находятся в оперативном доступе не менее двух месяцев).* *3. Регулярно, ответственным подразделением/лицом за ИБ должен осуществляться анализ журналов регистрации событий.* *4. Ответственным подразделением/лицом за ИБ регулярно должен осуществляться мониторинг зарегистрированных событий ИБ.* *В случае событий/инцидентов ИБ, должно осуществляться оповещение посредством уведомления ответственного за ИБ.* *Необходимо определить какими средствами будет происходить оповещение об инцидентах ИБ и уязвимостях.* *5. Все зарегистрированные события ИБ с целью принятия решения по поводу отнесения их к событиям ИБ должны оцениваться ответственным за ИБ.* *6. В организации должна быть утвержденная процедура по оповещению о событиях высокой и критичной*

			степени важности для информационной безопасности и об обнаруженных уязвимостях. Работники и привлекаемые со стороны исполнители должны быть ознакомлены с этой процедурой. *Должны быть установлены обязанности руководства для обеспечения быстрого и результативного реагирования на инциденты ИБ.* *Выполнение процедуры реагирования на инциденты ИБ должны регистрироваться.* *7. В организации должен проводиться анализ причин возникновения инцидентов ИБ. Данные мероприятия должны проводиться ответственным подразделением либо лицом ответственным за ИБ. Результаты анализа причин возникновения инцидентов ИБ должны документироваться.* *Знания, полученные в результате анализа инцидентов ИБ, чтобы уменьшить вероятность или воздействие должны использоваться при риске возникновения будущих инцидентов.* *Причины возникшего инцидента по результатам его анализа должны быть доведены до персонала. Ответственным подразделением либо лицом ответственным за ИБ должно проводиться обучение персонала по возникшим инцидентам ИБ.*
5	Управление непрерывностью ИБ	1. Планирование непрерывности информационной безопасности; 2. Идентификация событий, которые являются возможной причиной нарушения непрерывности процесса обеспечения информационной безопасности или бизнес процессов; 3. Разработка (актуализация), внедрение процессов и процедур поддержания необходимого уровня непрерывности информационной безопасности во внештатных (кризисных) ситуациях; 4. Определение, документирование, доведение до сведения сотрудников и привлекаемых со стороны	*1. В организации должна быть стратегия или процесс, учитывающий требования ИБ для обеспечения непрерывности бизнес-процессов организации.* *В соответствии с Правилами по обеспечению непрерывной работы активов, связанных со средствами обработки информации, должна быть выстроена стратегия обеспечивающая непрерывность ИБ в ОИ и отражена в Плане обеспечения непрерывности работы активов, связанных со средствами обработки информации.* *2. Идентификация событий, которые являются возможной причиной нарушения непрерывности процессов обеспечения ИБ, должна быть определена в Правилах по*

		исполнителей, выполнение процедур во внештатных (кризисных ситуациях); 5. Проверка (тестирование), анализ и оценка процессов и процедур обеспечения непрерывности информационной безопасности; 6. Резервирование средств обработки информации, объекта информатизации с учетом требований законодательства.	*обеспечению непрерывной работы активов, связанных со средствами обработки информации и возложена на ответственных за ИБ.* *Должны быть отражены результаты идентификации событий, которые являются возможной причиной нарушения непрерывности процесса обеспечения ИБ и бизнес процессов.* *3. Необходимо документально определить процедуры, процессы и действия во внештатных (кризисных) ситуациях и ответственных за их выполнение. Определить кем будет составляться этот документ. Кем будет утверждаться этот документ.* *Необходимо определить ответственного в организации за актуализацию планов обеспечения непрерывности и восстановления.* *Необходимо определить периодичность осуществления актуализации процессов и процедур поддержания необходимого уровня непрерывности ИБ во внештатных (кризисных) ситуациях.* *По мере необходимости проводить обучение персонала, направленное на понимание процессов обеспечения непрерывности бизнеса и процессов обеспечения ИБ. Определить кто будет контролировать процесс и результат обучения персонала.* *4. Необходимо ознакомить работников организации и привлекаемых со стороны исполнителей с процедурами действий во внештатных (кризисных) ситуациях.* *Определить, кто и с какой периодичностью будет контролировать исполнение процедур и действий во внештатных (кризисных) ситуациях.* *В организации необходимо проводить (ответственным лицом и с регулярностью) анализ результативности и эффективности процессов, процедур и действий во внештатных (кризисных) ситуациях.* *5. Ответственным подразделением либо лицом за ИБ*

			должно проводиться тестирование планов (процедур и процессов) обеспечения непрерывности ИБ и бизнес-процессов и восстановления после внештатной (кризисной) ситуации с определенной периодичностью. *6. Необходимо осуществлять резервирование средств обработки информации, систем хранения данных, компонентов сетей хранения данных и каналов передачи данных. Применяемый способ резервирования средств обработки информации, систем хранения данных, компонентов сетей хранения данных и каналов передачи данных, должен соответствовать требованиям, установленным в подпункте 2) пункта 49 ППРК ЕТ.* *(подпункт 2) пункта 49 ППРК ЕТ резервирование аппаратно-программных средств обработки данных, систем хранения данных, компонентов сетей хранения данных и каналов передачи данных, в том числе для объектов информатизации ЭП).* *Процедуры резервирования информации должны соответствовать процедурам, определенным в Регламенте резервного копирования ОИ.* *Необходимо осуществлять работы по тестированию резервных копий.*
6	Управление сетевой безопасностью	1. Определение, документирование и доведение до сведения сотрудников и привлекаемых со стороны исполнителей, выполнение процедур управления сетевым оборудованием; 2. Определение и включение в соглашения по обслуживанию сетей и передаче информации механизмов обеспечения безопасности, уровней доступности для всех сетевых услуг и сервисов; 3. Определение, документирование, доведение до сведения сотрудников и привлекаемых со стороны исполнителей, выполнение политик и процедур использования сетей и сетевых услуг, передачи информации, подключения к Интернету, сетям	*1. Необходимо обеспечить регламентирование процедуры управления сетевым оборудованием и ознакомить работников и привлекаемых со стороны исполнителей с процедурами управления сетевым оборудованием.* *В организации должна осуществляться идентификация сетевого оборудования. Должен вестись утвержденный перечень портов управления. Ответственным за ИБ необходимо осуществлять контроль доступа к портам управления.* *2. Процедуры соглашения по обслуживанию сетей и передаче информации, гарантирующие безопасную передачу и реализующиеся должны соответствовать*

		телекоммуникаций и связи и использования беспроводного доступа к сетевым ресурсам; 4. Определение, документирование и выполнение процедур по применению средств защиты информации, передаваемой по сети и электронных сообщений; 5. Структуризация и сегментация сети; 6. Способы подключения и взаимодействия сетей, учитывающие требования законодательства.	*рекомендациям пункта 13.2.2 СТ РК 27002-2015 и включать в соглашение механизмы обеспечения безопасности по уровню доступности сетевых услуг и сервисов.* *3. Регламентирование политики и процедуры использования сетей и сетевых услуг, передачи информации, подключения к Интернету, сетям телекоммуникаций и связи и использования беспроводного доступа к сетевым ресурсам.* *Контроль со стороны ответственного за ИБ исполнения политик и процедур использования сетей и сетевых услуг, передачи информации, подключения к Интернету, сетям телекоммуникаций и связи и использования беспроводного доступа к сетевым ресурсам.* *Соответствие применяемых способов подключения и взаимодействия сетей требованиям:* – *подпунктов 1) - 4) пункта 128 ППРК ЕТ.* – *подпунктов 8) - 11) пункта 139 ППРК ЕТ.* *Соблюдение требований подпунктов 5) – 6) пункта 128. ППРК ЕТ.* *4. Применение и документирование средств обеспечения ИБ в ОИ.* *Реализация требований подпунктов 1) и 3) пункта 128 ППРК ЕТ. Реализация рекомендаций пункта 13.2.3 СТ РК 27002-2015.* *5. Разделение сетей на сегменты администрирования и сети пользователей.* *6. Соответствуют ли применяемые способы подключения и взаимодействия сетей требованиям:* – *подпунктов 123-124 ППРК ЕТ;* – *подпункт 2) пункта 128 ППРК ЕТ;* – *пунктов 129 -131 ППРК ЕТ;* – *подпунктов 5) – 7) пункта 139 ППРК ЕТ.* *Необходимо обеспечить соблюдение пункта 125 ППРК ЕТ.*

7	Криптографические методы защиты	1. Регламентация управления криптографическими ключами, включающая вопросы изготовления, учета, хранения, передачи, использования, возврата (уничтожения), защиты криптографических ключей, учитывающая требования законодательства; 2. Применение криптографических средств при хранении и передаче информации, включая аутентификационные данные.	*1. В организации должно осуществляться регламентирование управления криптографическими ключами, включающее вопросы изготовления, учета, хранения, передачи, использования, возврата (уничтожения), защиты криптографических ключей, учитывающая требования законодательства, в случае применения.* *Соответствие политики управления криптографическими ключами рекомендациям пункта 10.1.2 СТ РК 27002-2015.* *Обеспечить реализацию требования подпункта 2) пункта 114 ППРК ЕТ.* *2. Применение в ОИ криптографических методов защиты.* *Необходимо обеспечить соответствие используемых СКЗИ требованиям пункта 48 ППРК ЕТ.* *Необходимо обеспечить соответствие применяемых политик криптографических методов защиты рекомендациям пункта 10.1.1 СТ РК 27002-2015.*
8	Управление рисками информационной безопасности	1. Выбор методики оценки рисков; 2. Идентификация угроз (рисков) для идентифицированных и классифицированных активов и формирование (актуализация) каталога угроз (рисков) информационной безопасности. Отражение в каталоге угроз (рисков), рисков связанных с процессами обеспечения информационной безопасности; 3. Оценка (переоценка) идентифицированных рисков; 4. Обработка рисков, формирование и утверждение (актуализация) плана обработки рисков; 5. Мониторинг и пересмотр рисков.	*1. В организации должна быть определена методика оценки рисков ИБ.* *2. В организации должен вестись каталог угроз (рисков) активов, связанных со средствами обработки информации ОИ. В каталоге угроз (рисков) должны вестись риски, связанные с процессами обеспечения информационной безопасности.* *3. Ответственными работниками, определенными в методике оценки рисков должно осуществляться измерение рисков ИБ с измерениями рисков применяющие способы – количественный, качественный или их комбинация.* *4. Ответственными работниками должна производиться оценка последствий в случае реализации рисков.* *Ответственными работниками должна производиться обработка рисков ИБ и оценка остаточных рисков, в*

			соответствии с утвержденным планом обработки рисков, определенным в Методике обработки рисков. *5. Необходимо обеспечить выбор критериев пересмотра, используемых для измерения рисков, определить регулярность пересмотра угроз и уязвимостей ОИ и актуализации каталога угроз (рисков).*
9	Управление доступом	1. Разработка (актуализация), документирование, ознакомление пользователей с правилами разграничения прав доступа к информации, функциям прикладных систем, услугам, системному ПО, сетям и сетевым сервисам; 2. Применяемые методы и процедуры идентификации, аутентификации и авторизации пользователей; 3. Реализация правил разграничения прав доступа, установленных в Правилах разграничения прав доступа к электронным информационным ресурсам; 4. Процедуры регистрации и отмены регистрации (блокировки) пользователей; 5. Управление учетными записями с привилегированными правами доступа; 6. Использование и управление криптографическими методами в процедурах аутентификации пользователей; 7. Управление изменениями прав доступа; 8. Управление паролями; 9. Использование привилегированных утилит; 10. Управление доступом к исходному коду объекта испытаний.	*1. Необходимо обеспечить регламентирование применяемых методов и правил разграничения прав доступа к информации, функциям прикладных систем, услугам, системного ПО, сетям, сетевым сервисам, ресурсам и ознакомление системных администраторов и пользователей с необходимостью сохранения конфиденциальности личной секретной аутентификационной информации.* *2. Применение методов идентификации и аутентификации пользователей ОИ должно соответствовать соответствующему классу ОИ.* *3. Необходимо определить на основании каких документов предоставляются права доступа к информации, функциям прикладных систем, услугам, системному ПО, сетям, сетевым сервисам и ресурсам работников или привлеченных со стороны исполнителей.* *Определение в документе перечня ресурсов и перечня полномочий работника или привлеченного со стороны исполнителя по отношению к информации, функциям прикладных систем, услугам, системному ПО, сетям, сетевым сервисам и ресурсам, кем утверждается (подписывается, согласовывается) документ.* *Периодичность контроля соответствия предоставляемых полномочий работников или привлеченных со стороны исполнителей по отношению к информации, функциям прикладных систем, услугам, системному ПО, сетям и сетевым сервисам его должностным обязанностям, принятым политикам доступа и требованиям по разделению обязанностей.*

			Ознакомление работников или привлекаемых со стороны исполнителей с предоставляемыми им правами по отношению к информации, функциям прикладных систем, услугам, системному ПО, сетям, сетевым сервисам и ресурсам. *4. Определение процедуры регистрации и отмены регистрации пользователей ОИ.* *Реализация процедур назначения, активации, отмены и выдачи идентификаторов и факторов аутентификации пользователям ОИ.* *Осуществление проверки идентичности пользователя перед выдачей нового или заменой секретного идентификатора и факторов аутентификации.* *Исключить использование общих идентификаторов для нескольких пользователей и администраторов ОИ.* *Осуществление учета зарегистрированных пользователей в реестре пользователей ОИ.* *Осуществление учета выданных пользователям идентификаторов или факторов аутентификации.* *Ознакомление пользователей ОИ с требованием сохранения конфиденциальности их аутентификационных данных.* *Обеспечение конфиденциальности при вводе аутентификационной информации в пользовательском интерфейсе.* *5. Определение процедуры по управлению паролями и использование индивидуальных паролей в ОИ.* *Определить периодичность смены паролей.* *Необходимо реализовать ограничения по количеству попыток ввода паролей.* *Установить требования к выбору качественных (стойких) паролей и выполнение этих требований при смене пароля в ОИ.* *6. Регламентирование процедуры распределения и предоставления привилегированных прав доступа по*

			отношению к информации, функциям прикладных систем, услугам, системному ПО, сетям и сетевым сервисам. *Определение процедуры избежания неавторизованного использования администраторских идентификаторов.* *Регламентирование регулярности обновления привилегированных учетных записей в ТД ИБ.* *7. Использование в ОИ криптографических методов сокрытия передаваемой и хранимой аутентификационной информации.* *8. Регламентирование и реализация процедуры по отмене прав доступа к информации и средствам обработки информации работников или привлеченных со стороны исполнителей по окончании срока трудового соглашения.* *9. Использование в ОИ утилит с привилегированными правами (при необходимости). Документирование использования в ОИ утилиты с привилегированными правами.* *Учитываются ли рекомендации пункта 9.4.4 СТ РК 27002-2015 при использовании утилит с привилегированными правами.* *10. Способы и методы хранения исходного кода ОИ.* *Как контролируется и документируется доступ к исходным кодам ОИ, кто имеет право доступа.* *Документирование процесса по периодичности обслуживания и копирование исходных кодов ОИ.*
10	Физическая безопасность и защита от природных угроз	1. Размещение серверного, телекоммуникационного оборудования, систем хранения данных с учетом требования законодательства; 2. Физическая защита периметра безопасности помещений, в которых размещены активы, связанные с информационно-коммуникационными технологиями; 3. Организация основного и резервного серверных помещений, учитывающая требования законодательства; 4. Оснащение основного и резервного серверных	*1. Места размещения серверного, телекоммуникационного оборудования, систем хранения данных (основного и резервного) должны соответствовать требованиям подпункта 1) пунктов 49, 108, 141, 153 ППРК ЕТ.* *2. Физический периметр безопасности для зон, в которых размещены серверное, телекоммуникационное оборудование, системы хранения данных (основные и резервные) должны соответствовать требованиям*

		помещений системами обеспечения, учитывающее требования законодательства; 5. Организация контролируемого доступа в серверные помещения; 6. Организация работ в серверном помещении; 7. Организация работ по техническому сопровождению и обслуживанию серверного и телекоммуникационного оборудования, систем хранения данных и систем обеспечения; 8. Способы защиты оборудования от отказов в системе электроснабжения и других нарушений, вызываемых сбоями в работе коммунальных служб; 9. Обеспечение безопасности кабельной системы.	*подпунктов 11.1.1 - 11.1.3 СТ РК 27002-2015.* *3. Серверные помещения должны соответствовать требованиям пунктов 142-148, 151, и пункта 11.2.1 СТ РК 27002-2015.* *4. Серверные помещения должны соответствовать требованиям пунктов 156-162 ПП РК ЕТ.* *5. Контролируемый доступ в серверные помещения должен соответствовать требованиям пункта 155 ППРК ЕТ и пункта 11.1.2 СТ РК 27002-2015.* *6. Процедуры проведения работ в серверном помещении должны соответствовать положениям, определенным в Правилах организации физической защиты средств обработки информации и безопасной среды функционирования информационных ресурсов и требованиям пункта 11.1.5 СТ РК 27002-2015. Проведение регламентных работ, действия в аварийных ситуациях, доступ в серверные помещения (физический и организационный), вопросы охраны труда при проведении работ должны регламентироваться владельцем серверного помещения. Если работы осуществляются представителями сторонних организаций, то выполнение этих работ должно контролироваться владельцем серверного помещения.* *7. Если процесс технического обслуживания осуществляется сторонней организацией, то необходимо предоставить договор. В договоре должны содержаться положения:* *- обязательств, применяемых к поставщикам для защиты информации;* *- обработки инцидентов ИБ, возникающих в процессе технического обслуживания;* *- восстановления работоспособности оборудования;* *Выполнение и полнота реализации процедуры технического обслуживания должны подтверждаться*

			документально (актами/протоколами). *8. Применяемые меры защиты в системе электроснабжения и других нарушений, вызываемых сбоями в работе коммунальных служб должны соответствовать требованиям пункта 145 ППРК ЕТ и пункта 11.2.2 СТ РК 27002-2015.* *9. Необходимо предоставить схему ведомственной (корпоративной) сети телекоммуникаций, определить ответственного лица за актуализацию документации СКС. СКС должен соответствовать требованиям пункта 11.2.3 СТ РК 27002-2015 и СН РК 3.02-17-2011.* *Силовые и телекоммуникационные сети должны быть разделены и соответствовать требованиям п. 146 ЕТ. Кабельные соединения должны регистрироваться в журнале/реестре. Маркировка элементов СКС должна осуществляться на регулярной основе.*
11	Эксплуатационные процедуры обеспечения ИБ	1. Разработка (актуализация), документирование, ознакомление пользователей с инструкциями, регламентирующими эксплуатационные процедуры обеспечения информационной безопасности; 2. Применение средств и систем обеспечения информационной безопасности; 3. Процедуры резервного копирования информации и тестирование результатов копирования. Безопасность мест хранения резервных копий; 4. Синхронизация времени журналов регистрации событий с единым источником времени; 5. Процедуры управления изменениями при установке новых версий прикладного и системного ПО в эксплуатируемых системах; 6. Контроль и управление уязвимостями ПО; 7. Ознакомление сотрудников и реализация положений Правил использования мобильных устройств и носителей информации; 8. Разработка (актуализация), ознакомление	*1. Если в организации практикуется удаленная работа, то необходимо чтобы применяемые меры и процедуры защиты информации, размещенной на удаленных рабочих местах, соответствовали рекомендациям пункта 6.2.2 СТ РК 27002-2015. Необходимо разработать и предоставить утвержденные инструкции (или иные виды документов), регламентирующие эксплуатационные процедуры обеспечения ИБ, соответствующие требованиям пункта 12.1.1 СТ РК 27002-2015.* *2. Среда, где функционирует ОИ средства и системы обеспечения ИБ должна соответствовать требованиям пункта 54 и 54-1 ППРК ЕТ и пункта 12.2.1 СТ РК 27002-2015.* *3. Процедура резервного копирования информации должна выполняться в соответствии с графиком, определенным в Регламенте резервного копирования информации. Необходимо предоставить журналы или отчеты о выполнении процедур резервного копирования. Применяемая процедура резервного копирования должна*

		сотрудников, реализация положений инструкции по организации удаленной работы; 9. Мониторинг работоспособности объекта испытаний; 10. Разделение сред разработки, тестирования и эксплуатации; 11. Обеспечение конфиденциальности при передаче сообщений электронной почты и информации посредством Интернет; 12. Способы предоставления Интернета и взаимодействия с внешними электронными почтовыми системами в соответствии с требованиями законодательства; 13. Ограничения и порядок фильтрации при доступе к ресурсам Интернета.	*соответствовать требованиям пункта 12.3.1 СТ РК 2702-2015. Необходимо осуществлять тестирование резервных копий и фиксировать результаты.* *4. Необходимо синхронизировать время журналов регистрации событий ОС, СУБД, ППО, телекоммуникационного оборудования с единым источником времени, согласно требованиям пункта 12.4.4 СТ РК.* *5. Процедуры установки (обновления) ПО (прикладного и системного), соответствующие требованиям пунктов 12.5.1,12.6.2, 14.2.2 – 14.2.4 СТ РК 27002-2015, должны быть задокументированы и утверждены. Необходимо вести учет изменений и версионности установленного (обновленного) ПО и фиксировать результаты. Необходимо осуществлять тестирование (проверка) работоспособности ОИ после переустановки ПО.* *6. Необходимо выполнять работы по выявлению и устранению технических уязвимостей в ОИ и фиксировать результаты.* *7. Необходимо ответственному лицу за обеспечение ИБ осуществлять контроль реализации положений Правил использования мобильных устройств и носителей информации.* *8. Если в организации практикуется удаленная работа, то необходимо регламентировать процедуры безопасной удаленной работы. Необходимо ответственному лицу за обеспечение ИБ осуществлять контроль исполнения этих процедур.* *9. Необходимо осуществлять мониторинг работоспособности ОИ, соответствующий требованиям пункта 12.1.3 СТ РК 27002-2015. Необходимо продемонстрировать ресурсы, которые подвергаются мониторингу и средства для мониторинга работоспособности ОИ.* *10. Необходимо выполнять требование подпункта 3)*

			пункта 98 ППРК ЕТ и пункта 12.1.4 СТ РК 27002-2015 по вопросу разделения сред разработки, тестирования и эксплуатации. Процесс перевода ПО из среды разработки в среду тестирования и в среду эксплуатации. *11. Необходимо обеспечивать защиту служебной информации, передаваемой посредством электронной почты и Интернет, согласно рекомендациям пункта 13.2.1 СТ РК 27002-2015. Необходимо обеспечить реализацию требований подпункта 5) пункта 128 ППРК ЕТ.* *12. Необходимо обеспечить реализацию требований подпункта 6) пункта 128 ППРК ЕТ и пунктов 24, 25, 25-1 ППРК ЕТ.* *13. Необходимо обеспечить реализацию требований пункта 133 ППРК ЕТ. Необходимо определить перечень Интернет-ресурсов, доступ к которым должен быть ограничен и утвердить данный документ руководителем организации. Реализовать технически ограничения доступа к Интернет-ресурсам и продемонстрировать процедуры реализации. Необходимо ответственному лицу за обеспечение ИБ осуществлять контроль за реализацией ограничений доступа к Интернет-ресурсам.*
12	Соответствие законодательным и договорным требованиям	1. Определение (актуализация), документирование законодательных, нормативных, иных обязательных, договорных требований для объекта испытаний; 2. Внедрение процедур, реализующих соответствие законодательным, нормативным и договорным требованиям, связанным с правами на интеллектуальную собственность; 3. Разработка и реализация политик защиты конфиденциальных и персональных данных, соответствующих нормам законодательства; 4. Соответствие применяемых криптографических методов и средств требованиям законодательства и соглашениям (договорам); 5. Проведение аудита информационной	*1. Необходимо предоставить документы, где определены законодательные, нормативные, иные обязательные, договорные требования к обеспечению ИБ для ОИ (ТЗ, ТЭО, СТПО, ДТЗ, концепция). Необходимо реализовать положения подпункта 1) пункта 2-1 статьи 38 Закона и пункта 2 статьи 39 Закона.* *2. Необходимо утвердить процедуры, реализующие соответствие законодательным, нормативным и договорным требованиям, связанным с правами на интеллектуальную собственность ПО или информационных продуктов и сервисов. Предоставить документ, где отражены сведения об активах в отношении которых действует требование по защите прав интеллектуальной собственности (либо внести перечень лицензионных ПО в*

		безопасности; 6. Проведение анализа объекта испытаний на предмет соответствия требованиям законодательства, стандартов и технической документации по информационной безопасности; 7. Защита записей от потери, повреждения, фальсификации, несанкционированного доступа и несанкционированного выпуска в соответствии с законодательными, нормативными, договорными требованиями.	*реестр активов). Процедуры безопасной утилизации (или передачи) лицензионного ПО необходимо определить в ТД по ИБ. Необходимо обеспечить реализацию требований пункта 79 ППРК ЕТ.* *3. Необходимо методы защиты конфиденциальных и персональных данных, соответствующих нормам законодательства определить в ТД по ИБ и продемонстрировать в ОИ методы защиты конфиденциальных и персональных данных.* *4. Необходимо продемонстрировать криптографические методы преобразования информации в ОИ, соответствующие требованиям законодательства и соглашениям (договорам).* *5. Необходимо проводить внутренний аудит ИБ, согласно плану-графику и предоставить результаты (отчеты).* *6. Необходимо проводить анализ ОИ на предмет соответствия требованиям законодательства, стандартов и технической документации по ИБ с фиксацией результатов. Осуществлять актуализацию документации, регламентирующей процессы обеспечения ИБ и самих процессов обеспечения ИБ.* *7. Необходимо продемонстрировать способы защиты записей от потери, повреждения, фальсификации, несанкционированного доступа и несанкционированного выпуска в соответствии с законодательными, нормативными, договорными требованиями.*
13	Приобретение, разработка и обслуживание систем	1. Включение (актуализация) требований, связанных с информационной безопасностью и соответствующих действующему законодательству и стандартам в состав технической документации на объект испытаний; 2. Определение и применение безопасных процедур управления изменениями ПО (системного и прикладного) для эксплуатируемых систем;	*1. Необходимо предоставить документы:* *- регламентирующие безопасную разработку (модернизацию) ПО, интеграцию ОИ, включающие, в том числе, требования пункта 14.2.1 СТ РК 27002-2015. Разработка ПО должна осуществляться в среде, отделенной от среды промышленной эксплуатации.* *– где проводилась оценка рисков ИБ в отношении ОИ*

		3. Контроль процесса разработки ПО объекта испытаний, в том числе, осуществляемого сторонней организацией; 4. Контроль процесса технического сопровождения системы, осуществляемого сторонней организацией; 5. Тестирование функций безопасности системы.	*на этапе его проектирования* *– где учтены требования по ИБ в технической документации на создание и модернизацию ОИ (ТЗ, ДТЗ, ЧТЗ, ТС, ЗНП ИКУ, Концепция ГЧП, ТЭО и др.), в том числе, требования подпунктов 1) и 2) пункта 78 ППРК ЕТ.* *– требования по ИБ и критерии принятия ПО в договорах (ТС) на закуп готового ПО, в том числе, требования подпунктов 1) и 2) пункта 78 ППРК ЕТ* *– класс ЭИР и ПО при формировании требований по ИБ в технической документации на создание и модернизацию ОИ или в договорах (ТС) на закуп готового ПО.* *2. Необходимо предоставить документы, где описывается и выполняется процедура управления изменениями ПО (системного и прикладного) для эксплуатируемых систем. Необходимо осуществлять проверку работоспособности прикладного ПО после внесения изменений в системное ПО и проводить анализ результатов изменений ПО (системного и прикладного) для эксплуатируемых систем.* *3. Необходимо предоставить договор на разработку ПО в случае, если процесс разработки ПО осуществляется сторонней организацией, включающий в том числе требования пункта 14.2.1 СТ РК 27002-2015.* *Необходимо осуществлять контроль процесса разработки ПО, осуществляемого сторонней организацией.* *4. Необходимо предоставить договор на техническое сопровождение ПО в случае, если процесс разработки ПО осуществляется сторонней организацией, содержащий положения, связанные с:* *– регламентацией доступа поставщика к документации и активам, связанным с ИКТ;* *– обязательствами, применяемыми к поставщикам для защиты информации;*

			– *обработкой инцидентов ИБ, возникающих в процессе технического сопровождения;* – *восстановлением работоспособности ПО;* *Необходимо обеспечить реализацию требований пунктов 149-150 ППРК ЕТ и пункта 11.2.4 СТ РК 27002-2015.* *5. Необходимо осуществлять проверки (тестирование) функций безопасности и требований ИБ, определенных в технической документации на ОИ или договорах (ТС) при разработке системы и приемке системы либо покупке готового продукта (с оформлением результатов).* *Осуществлять тестирование ПО в среде, отделенной от среды промышленной эксплуатации. При тестировании ПО не использовать реальные учетные записи пользователей систем, находящихся в среде промышленной эксплуатации.*

Перечень сокращений и аббревиатур:

ОИ – объект испытаний;
ОС – операционная система;
СУБД – система управления базами данных;
ТД ИБ – техническая документация по информационной безопасности;
ТЭО – технико - экономические обоснование
ТЗ – техническое задание;
ППО – прикладное программное обеспечение;
СВТ – средства вычислительной техники;
ПО – программное обеспечение;
ИКТ – информационно - коммуникационные технологии;
ИС – информационная система;
ИБ – информационная безопасность;
ФБ – функции безопасности;
СКУД – система контроля и управления доступом;

ГО – государственный орган;
МИО – местный исполнительный орган;
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.