|  |
| --- |
| **Перечень запрашиваемых организационно-распорядительных и технических документов, подлежащих изучению в ходе обследования процессов обеспече****ния информационной безопасности в рамках испытаний** |
| 1.
 | Политика информационной безопасности |
|  | Правила идентификации, классификации и маркировки активов, связанных со средствами обработки информации |
|  | Методика оценки рисков информационной безопасности |
|  | Правила по обеспечению непрерывной работы активов, связанных со средствами обработки информации |
|  | Правила инвентаризации и паспортизации средств вычислительной техники, телекоммуникационного оборудования и программного обеспечения |
|  | Правила проведения внутреннего аудита информационной безопасности |
|  | Правила использования средств криптографической защиты информации |
|  | Правила разграничения прав доступа к электронным информационным ресурсам |
|  | Правила использования Интернет и электронной почты |
|  | Правила организации процедуры аутентификации |
|  | Правила организации антивирусного контроля |
|  | Правила использования мобильных устройств и носителей информации |
|  | Правила организации физической защиты средств обработки информации и безопасной среды функционирования информационных ресурсов |
|  | Регламент резервного копирования и восстановления информации |
|  | Руководство администратора по сопровождению объекта информатизации |
|  | Инструкцию о порядке действий пользователей по реагированию на инциденты информационной безопасности и во внештатных (кризисных) ситуациях |
|  | Приказ об утверждении технической документации по информационной безопасности (ТД ИБ) |
|  | Реестр активов |
|  | Расчет класса ИС ОИ *(ТЭО, ТЗ либо Утвержденный расчет класса ИС согласно Правилам классификации объектов информатизации и классификатор объектов информатизации» утвержденные Приказом и.о. Министра по инвестициям и развитию Республики Казахстан от 28 января 2016 года № 135 или информация с*[*архитектурного портала*](http://adilet.zan.kz/rus/docs/Z1500000418#z31)*«электронного правительства»).* |
|  | Приказ о проведении инвентаризации активов |
|  | Паспорта на средства вычислительной техники, телекоммуникационного оборудования и ПО |
|  | Документирование процедуры утилизации и(или) подготовки к повторному использованию серверного и телекоммуникационного оборудования, систем хранения данных, рабочих станций, носителей информации *(например, акты, приказы или другое)* |
|  | Документирование функционального назначения подразделения ИБ или функциональных обязанностей ответственного за ИБ *(например, должностные инструкции)* |
|  | Подтверждение компетентности специалистов в сфере обеспечения ИБ *(например, сертификаты, дипломы о полученном образовании и прочее)* |
|  | Документирование и функционирование рабочих групп по проведению совещаний в сфере обеспечения ИБ *(например, протоколы, приказы и прочее)* |
|  | Документирование взаимодействия с профессиональными сообществами, профессиональными ассоциациями или форумами специалистов по ИБ *(например, письма, переписка, меморандумы)* |
|  | Листы ознакомления работников, в том числе сторонних организаций, с процедурами обеспечения ИБ описанных в ТД по ИБ и их ответственностью за несоблюдение этих процедур  |
|  | Листы соглашения о конфиденциальности и неразглашении служебной информации |
|  | Документальная проверка кандидатов при приеме на работу в случае, если работник принимается на должность, связанную с ИБ |
|  | Документальное подтверждение исполнения процедуры увольнения работников, имеющих обязательства в области обеспечения ИБ |
|  | Документальное подтверждение предпринятых действий (процедур), которые будут предприняты к нарушителям требований ИБ |
|  | Документы подтверждающие осведомленность работников и привлекаемых со стороны исполнителей об их обязанностях и ответственности, связанными с обеспечением ИБ в период их занятости, изменений или прекращений трудовых отношений |
|  | Документы подтверждающие проведение обучения (инструктажа) по вопросам ИБ |
|  | Утвержденная процедура по реагированию на инциденты ИБ? Ознакомлены ли работники и привлекаемые со стороны исполнители с этой процедурой |
|  | Документальная стратегия или процесс, обеспечивающий непрерывность ИБ в организации |
|  | План (процедур и процессов) обеспечения непрерывности ИБ и бизнес-процессов и восстановления после внештатной (кризисной) ситуации |
|  | Документальное подтверждение тестирования планов (процедур и процессов) обеспечения непрерывности ИБ и бизнес-процессов и восстановления после внештатной (кризисной) ситуации *(например, акты, протоколы и прочее)* |
|  | Документы фиксирующие выполнение процедур резервного копирования информации *(например, акты, протоколы и прочее)* |
|  | Документы фиксирующие тестирование резервных копий *(например, акты, протоколы и прочее)* |
|  | Утвержденный перечень портов управления сетевого оборудования |
|  | Документальное подтверждение на получение доступа к сетевым ресурсам и сервисам |
|  | Документированная утвержденная схема локальной сети |
|  | Документирование каталога угроз (рисков) активов, связанных со средствами обработки информации |
|  | Документирование утвержденного плана обработки рисков |
|  | Документирование матрицы доступа |
|  | Документирование окончания срока трудового соглашения |
|  | Документирование процесса применения утилит с привилегированными правами в ОИ |
|  | Документируется ли процесс обслуживания и копирования исходных кодов в ОИ |
|  | Документирование проведения работ в серверном помещении |
|  | Регламентирование проведения регламентных работ, действия в аварийных ситуациях, доступ в серверные помещения (физический и организационный), вопросы охраны труда при проведении работ |
|  | Документирование о фактических неисправностях оборудования и видах восстановительных работ |
|  | Документально подтверждение компетентности работников, осуществляющих техническое обслуживание оборудования *(например, сертификаты, дипломы и прочее)* |
|  | Документированная схема ведомственной (корпоративной) сети телекоммуникаций |
|  | Документирование кабельных соединений |
|  | Документированные процедуры установки (обновления) (ПО (прикладного и системного)) в эксплуатируемых ОИ *(например, акты, журналы, реестры и прочее)* |
|  | Документирование процесса перевода ПО из среды разработки, в среду тестирования и в среду эксплуатации *(например, акты, журналы, реестры и прочее)* |
|  | Документирование перечня интернет-ресурсов, доступ к которым должен быть ограничен |
|  | Документирование процедуры, реализующих соответствие законодательным, нормативным и договорным требованиям, связанным с правами на интеллектуальную собственность ПО или информационных продуктов и сервисов |
|  | Листы ознакомления системных администраторов и пользователей ОИ с политикой организации в отношении соблюдения прав интеллектуальной собственности |
|  | Документирование процедуры безопасной утилизации (или передачи) лицензионного ПО |
|  | Документирование свидетельства обладания лицензиями ПО |
|  | Документирование методов защиты конфиденциальных и персональных данных, соответствующих нормам законодательства |
|  | Документирование анализа ОИ на предмет соответствия требованиям законодательства, стандартов и технической документации по ИБ |
|  | Документирование результата анализа ОИ на предмет соответствия требованиям законодательства, стандартов и технической документации по ИБ |
|  | Документирование процедур регламентирующих безопасную разработку (модернизацию) ПО, интеграцию ОИ |
|  | Документирование в технической документации на создание и модернизацию ОИ требования по ИБ |
|  | Задокументированная процедура управления изменениями ПО (системного и прикладного) для эксплуатируемых систем |
|  | Документирование осведомленности работников владельца (собственника) ОИ с содержанием документа, регламентирующего вопросы безопасной разработки ПО |
|  | Договор на разработку ПО в случае, если процесс разработки ПО осуществляется сторонней организацией |
|  | Договор на техническое сопровождение ПО в случае, если процесс разработки ПО осуществляется сторонней организацией |
|  | Приказ о назначении ответственного за ИБ |
|  | Положения о службе и должностные инструкции ответственного за ИБ |
|  | Должностные инструкции администраторов ОИ |
|  | Договор аренды серверного помещения/коллокейшн (при необходимости) |