# Перечень обследования сетевой инфраструктуры

| № пп | Наименование параметров и характеристик | Комментарий |
|---|---|---|
| 1.1 | Использование уникальных идентификаторов пользователей для определения связи пользователей с их действиями и ответственностью за них. | *На сетевом оборудовании должны использоваться персонифицированные учетные записи администраторов ИС.* |
| 1.2 | Привилегированные права доступа должны быть предназначены администраторам на основе потребности их использования. | *Привилегии администраторов должны быть предназначены на основе потребности их использования.* |
| 1.3 | Регистрация неудачных и успешных попыток входа. | *Авторизация успешных и неудачных попыток входа должна регистрироваться в системе мониторинга и управления инцидентами и событиями ИБ.* |
| 1.4 | Обеспечение не отображения паролей на экране, будучи введенными. | *Обеспечить сокрытие пароля при введении на сетевом оборудовании.* |
| 1.5 | Ограничение времени подключения. | *Необходимо реализовать блокировку сессии администратора по истечению определенного времени бездействия.*<br>*Необходимо настроить блокировку учетной записи по достижению определенного количества неуспешных попыток доступа.* |
| 1.6 | Использование и выбор качественных паролей. | *Необходимо настроить парольную политику следующим образом:*<br>*длина пароля не должна составлять менее 8 символов; в числе символов должны присутствовать буквенные символы (верхнего и нижнего регистра), цифры и специальные символы.* |
| 1.7 | Реализация регулярных изменений пароля, а также – по мере необходимости. | *Необходимо устанавливать минимальный срок жизни пароля, для реализации регулярной смены пароля.* |
| 2.1 | Журналы событий должны включать:<br>– идентификаторы пользователей;<br>– системные действия;<br>– даты, времена и детали ключевых событий, например, вход в систему и выход;<br>– отчеты успешных и отклоненных попыток доступа;<br>– изменения системной конфигурации;<br>– использование привилегий; | *События полного перечня сетевого оборудования должны быть зарегистрированы в системе мониторинга и управления инцидентами и событиями ИБ.*<br>*Типы событий сетевого оборудования, подлежащие журналированию:*<br>*1) запуск/остановка системы;*<br>*2) изменение системной конфигурации;*<br>*3) создание, удаление, модификация локальных учетных записей;*<br>*4) использование привилегированных учетных записей;*<br>*5) подключение/отключение устройства ввода/вывода;*<br>*6) неудавшиеся или отвергнутые действия пользователя;*<br>*7) запуск, падение, остановка сетевых линков (коннектов).* |

| № пп | Наименование параметров и характеристик | Комментарий |
|---|---|---|
| | – сетевые адреса и протоколы. | |
| 2.2 | Проведение мониторинга событий, связанных с нарушением ИБ, и анализ результатов мониторинга. | *Необходимо настроить мониторинг событий нарушений ИБ и анализ результатов мониторинга на сетевом оборудовании.* |
| 2.3 | Регистрация событий, связанных с состоянием ИБ, и выявление нарушений путем анализа журналов событий телекоммуникационного оборудования. | *Необходимо чтобы события, связанные с состоянием ИБ, и выявление нарушений путем анализа журналов сетевого оборудования регистрировались в системе мониторинга и управления инцидентами и событиями ИБ.* |
| 2.4 | Хранение журналов регистрации событий в течение срока, указанного в ТД ИБ, но не менее трех лет и нахождение их в оперативном доступе не менее двух месяцев. | *Необходимо настроить хранение журналов регистрации событий сетевого оборудования в системе мониторинга и управления инцидентами и событиями ИБ в течение срока, указанного в ТД ИБ, но не менее трех лет и нахождение их в оперативном доступе не менее двух месяцев.* |
| 2.5 | Обеспечение защиты журналов регистрации событий от вмешательства и неавторизированного доступа. Не допускается наличие у системных администраторов полномочий на изменение, удаление и отключение журналов. Для конфиденциальных ИС требуется создание и ведение резервного хранилища журналов. | *Необходимо распределить права доступа к системе мониторинга и управления инцидентами и событиями ИБ, не допускается наличие у сетевого и системного администратора полномочий на изменение, удаление и отключение журналов.* |
| 2.6 | Обеспечение синхронизации времени журналов регистрации событий с инфраструктурой источника времени. | *Необходимо обеспечить синхронизацию времени журналов регистрации событий с инфраструктурой источника времени с эталоном времени и частоты, воспроизводящим национальную шкалу всемирного координированного времени UTC(kz).* |
| 3.1 | Обеспечение наличия средств, позволяющих прогнозировать вторжения (потенциальные вторжения в сети телекоммуникаций), выявлять их в реальном масштабе времени и поднимать соответствующую тревогу | *Наличие средств защиты обнаружения и предотвращения вторжений. Система обнаружения/предотвращения вторжений должна иметь актуальную лицензию. Может быть как программным средством, так и программно-аппаратным комплексом.* |
| 3.2 | Ведение журнала аудита (в том числе осуществление регистрации попыток изменения конфигурации, а также попыток доступа к компонентам и данным) | *Необходимо настроить журналирование событий в системе обнаружения и предотвращения вторжения.* |
| 3.3 | Возможность автоматизированного | *В системе обнаружения и предотвращения вторжения необходимо настроить* |

| № пп | Наименование параметров и характеристик | Комментарий |
|---|---|---|
| | обновления базы правил. | *автоматическое обновления базы правил. Базы правил должны быть в актуальном состоянии.* |
| 3.4 | Обеспечение синхронизации по времени между компонентами ОИ, а также между ОИ и средой его функционирования. | *Необходимо обеспечить синхронизацию времени журналов регистрации событий системы обнаружения/предотвращения вторжений с инфраструктурой источника времени с эталоном времени и частоты, воспроизводящим национальную шкалу всемирного координированного времени UTC(kz).* |
| 3.5 | Генерация сигнала с использованием выбранного метода и оповещение администратора. | *Необходимо настроить оповещение ответственным лицам ИС о событиях и инцидентах ИБ (например, на ведомственную электронную почту, телеграмм канал, SMS).* |
| 4.1 | Неиспользуемые порты кабельной системы локальной сети физически должны отключаться от активного оборудования. | *Необходимо физически отключить неиспользуемые порты на сетевом оборудовании.* |
| 4.2 | Обеспечение взаимодействия локальных сетей центрального исполнительного государственного органа и его территориальных подразделений между собой только через ЕТС ГО, за исключением сетей телекоммуникаций специального назначения и/или правительственной, засекреченной, шифрованной и кодированной связи. | *Необходимо обеспечить взаимодействия локальных сетей центрального исполнительного ГО и его территориальных подразделений между собой только через ЕТС ГО.* |
| 4.3 | Управление программно-аппаратным обеспечением ИС ГО и МИО должно осуществляться из внутренней локальной сети владельца ИС. | *Управление программно-аппаратным обеспечением ИС ГО и МИО должно осуществляться из внутренней локальной сети владельца ИС.* |
| 4.4 | Изоляция и сегментирование сетей объектов информатизации. | *Необходимо использовать средства физического и логического сегментирования сети для разделения и изоляции информационных потоков. Каждая ИС должна быть изолирована от других ИС на уровне сети.* |
| 5.1 | Обеспечение фильтрации входящих и исходящих пакетов на каждом интерфейсе. | *Необходимо обеспечить фильтрацию входящих и исходящих пакетов на каждом интерфейсе сетевого оборудования с помощью (Access list).* |
| 5.2 | В настройках оборудования неиспользуемые порты должны блокироваться. | *На сетевом оборудовании необходимо закрыть(блокировать) неиспользуемые порты с помощью (Access list)* |
| 5.3 | Обеспечение регистрации событий безопасности. | *Журналы событий межсетевого экрана должны регистрироваться в системе мониторинга и управления инцидентами и событиями ИБ.* |

| № пп | Наименование параметров и характеристик | Комментарий |
|---|---|---|
| 5.4 | Наличие оповещения о критичных видах событий безопасности. | *Необходимо настроить оповещение ответственным лицам ИС о событиях и инцидентах ИБ (например, на ведомственную электронную почту, телеграмм канал, SMS).* |
| 5.5 | Преобразование сетевых адресов. | *На межсетевом экране/пограничном сетевом оборудовании необходимо настроить преобразование сетевых адресов(NAT).* |
| 6.1 | При организации выделенного канала связи, объединяющего локальные сети, должны применяться программно-технические средства защиты информации, в том числе криптографического шифрования, с использованием СКЗИ. | *При организации канала связи между основным и резервным ЦОД ИС должны применяться программно-технические средства защиты информации.* |
| 6.2 | Обеспечение целостности/подлинности: использования цифровых подписей или кодов аутентификации сообщения, чтобы проверить подлинность или целостность сохраненной, или переданной чувствительной или важной информации. | *Использование цифровых подписей или кодов аутентификации сообщения, чтобы проверить подлинность или целостность сохраненной, или переданной чувствительной или важной информации.* |
| 7.1 | Наличие защитных мер представления свидетельства передачи информации по сети. | *Необходимо обеспечить сбор всех событий сетевого оборудования и мониторинг сетевого трафика.* |
| 8.1 | Для обеспечения доступности и отказоустойчивости должно использоваться резервирование аппаратно-программных средств обработки данных, систем хранения данных, компонентов сетей хранения данных и каналов передачи данных. | *Для обеспечения доступности и отказоустойчивости владельцами объектов информатизации ЭП обеспечиваются:*<br>*Наличие резервного собственного или арендованного серверного помещения для объектов информатизации ЭП первого и второго классов в соответствии с классификатором.*<br>*Резервирование аппаратно-программных средств обработки данных, систем хранения данных, компонентов сетей хранения данных и каналов передачи данных, в том числе для объектов информатизации ЭП:*<br>*первого класса в соответствии с классификатором – нагруженное (горячее) в резервном серверном помещении;*<br>*второго класса в соответствии с классификатором – не нагруженное (холодное) в резервном серверном помещении;*<br>*третьего класса в соответствии с классификатором – хранение на складе в непосредственной близости от основного серверного помещения.* |
| 9.1 | Предоставление для связи с удаленным | *Канал связи в рамках ИС, а также между основным и резервным ЦОД ИС должны* |

| № пп | Наименование параметров и характеристик | Комментарий |
|---|---|---|
| | доверенным ИТ продуктом канала, который логически отличим от других и обеспечивает надежную аутентификацию его сторон, а также защиту данных от модификации и раскрытия. Обеспечение у обеих сторон возможности инициировать связь через доверенный канал. | *применяться программно-технические средства защиты информации.* |
| 10.1 | Предоставление для связи с удаленным пользователем маршрута, который логически отличим от других и обеспечивает надежную аутентификацию его сторон, а также защиту данных от модификации и раскрытия. Обеспечение у пользователя возможности инициировать связь через доверенный маршрут. | *Удаленное управление ресурсами ИС должно быть реализовано посредством защищенного шлюза или списка разрешенных сетевых адресов отправителей.* |

**Перечень сокращений и аббревиатур:**

ОИ – объект испытаний по заявке в целом;
ИС – информационная система;
ЭП – электронное правительство;
ИБ – информационная безопасность;
ЦОД – центр обработки данных;
ЕТС ГО – единая транспортная среда государственных органов Республики Казахстан;
ППРК ЕТ – Единые требования в области информационно-коммуникационных технологий и обеспечения информационной безопасности, утвержденные постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832;
СКЗИ – средства криптозащиты информации.