УТВЕРЖДАЮ
И.о. министра
_____ /Р.М. Самбу-Хоо
«05» августа 2021 г.

Положение об обеспечении мер защиты информации в государственной информационной системе Министерства по внешнеэкономическим связям и туризму Республики Тыва

Настоящее Положение определяет содержание и правила реализации организационных и технических мер защиты информации, применяемых в государственной информационной системе Министерства по внешнеэкономическим связям и туризму Республики Тыва в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11 февраля 2013 г. № 17.

В соответствии с актом классификации № ___ от 05.08.2021 г. для государственной информационной системы установлен 2-ой класс защищенности (К2).

1. Идентификация и аутентификация субъектов доступа и объектов доступа

1.1 В ГИС должна обеспечиваться идентификация и аутентификация пользователей, выполняющих свои должностные обязанности (функции) с использованием информации, информационных технологий и технических средств ГИС в соответствии с должностными регламентами (инструкциями), и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей.

1.2 Пользователи информационной системы должны однозначно идентифицироваться и аутентифицироваться для всех видов доступа.

1.3 Аутентификация пользователя осуществляется с использованием паролей, аппаратных средств.

1.4 В информационной системе до начала информационного взаимодействия (передачи защищаемой информации от устройства к устройству) должна осуществляться идентификация и аутентификация устройств (технических средств).

1.5 Идентификация устройств в информационной системе обеспечивается:

- по логическим именам (имя устройства и (или) ID);
- логическим адресам (например, IP-адресам);
- и (или) по физическим адресам (например, MAC- адресам) устройства;
- или по комбинации имени, логического и (или) физического адресов устройства.

1.6 Аутентификация устройств в информационной системе обеспечивается с использованием:

- соответствующих протоколов аутентификации;

– с применением в соответствии с законодательством Российской Федерации криптографических методов защиты информации.

1.7 В ГИС установлены и реализованы следующие функции управления идентификаторами пользователей и устройств:

– определение должностного лица (администратора), ответственного за создание, присвоение и уничтожение идентификаторов пользователей и устройств;

– формирование идентификатора, который однозначно идентифицирует пользователя и (или) устройство;

– присвоение идентификатора пользователю и (или) устройству;

– исключение повторного использования идентификатора пользователя в течение: не менее одного года;

– блокирование идентификатора пользователя через период времени неиспользования: не более 90 дней.

2. Защита машинных носителей информации

2.1 В ГИС <Наименование ИС> учету подлежат:

– съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства);

– портативные вычислительные устройства, имеющие встроенные носители информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства);

– машинные носители информации, встроенные в корпус средств вычислительной техники (накопители на жестких дисках).

2.2 Носителям присваиваются регистрационные (учетные) номера. В качестве регистрационных номеров используются:

– идентификационные (серийные) номера машинных носителей, присвоенные производителями этих машинных носителей информации;

– номера инвентарного учета, в том числе инвентарные номера технических средств, имеющих встроенные носители информации;

– иные номера.

2.3 Учет съемных машинных носителей информации ведется в журнале учета машинных носителей информации.

2.4 Учет встроенных в портативные или стационарные технические средства машинных носителей информации ведется в журналах материально- технического учета в составе соответствующих технических средств. При использовании в составе одного технического средства информационной системы нескольких встроенных машинных носителей информации, конструктивно объединенных в единый ресурс для хранения информации, присваивается регистрационный номер техническому средству в целом.

2.5 Регистрационные или иные номера подлежат занесению в журнал учета машинных носителей информации или журналы материально-технического учета с указанием пользователя или группы пользователей, которым разрешен доступ к машинным носителям информации.

2.6 Раздельному учету в журналах учета подлежат съемные (в том числе портативные) перезаписываемые машинные носители информации (флэш- накопители, съемные жесткие диски).

2.7 Обеспечивается маркировка машинных носителей информации (технических средств), дополнительно включающая информацию о возможности использования машинного носителя информации вне информационной системы.

2.8 Физический доступ к машинным носителям предоставляется только тем лицам, которым он необходим для выполнения своих должностных обязанностей (функций).

2.9 В ГИС осуществляется контроль использования интерфейсов ввода (вывода) путем определения интерфейсов средств вычислительной техники, которые могут использоваться для ввода (вывода) информации.

2.10 В качестве мер, исключающих возможность использования запрещенных интерфейсов ввода (вывода), применяются:

– опечатывание интерфейсов ввода (вывода);

– использование механических запирающих устройств;

– удаление драйверов, обеспечивающих работу интерфейсов ввода (вывода);

– применение средств защиты информации, обеспечивающих контроль использования интерфейсов ввода (вывода).

2.11 При передаче машинных носителей между пользователями, в сторонние организации для ремонта и утилизации обеспечивается уничтожение (стирание) информации, исключающее возможность восстановления защищаемой информации путем очистки всего физического пространства машинного носителя информации, включая сбойные и резервные элементы памяти специализированными программами или утилитами производителя.

2.12 В ГИС обеспечивается регистрация и контроль действий по удалению защищаемой информации и уничтожению машинных носителей информации следующим образом:

– ....

3. Регистрация событий безопасности

3.1 В ГИС подлежат регистрации следующие события безопасности:

– при регистрации входа (выхода) субъектов доступа в информационную систему и загрузки (останова) операционной системы: дата и время входа (выхода) в систему (из системы) или загрузки (останова) операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки (останова) операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа;

– при регистрации подключения машинных носителей информации и вывода информации на носители информации: дата и время подключения машинных носителей информации и вывода информации на носители информации, логическое имя (номер) подключаемого машинного носителя информации, идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации;

– при регистрации запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации: дата и время запуска, имя

(идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный);

– при регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам: дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификация защищаемого файла (логическое имя, тип);

– при регистрации попыток доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, записям, полям записей): дата и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификация защищаемого объекта доступа (логическое имя (номер);

– при регистрации попыток удаленного доступа к информационной системе: дата и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к информационной системе;

– события, связанные с изменением привилегий учетных записей.

3.2 Пересмотр перечня событий безопасности, подлежащих регистрации, осуществляется не менее чем один раз в год и по результатам контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе.

3.3 Срок хранения информации о зарегистрированных событиях безопасности составляет не менее трех месяцев, при этом осуществляется хранение только записей о выявленных событиях безопасности.

3.4 В информационной системе обеспечивается запись дополнительной информации о событиях безопасности, включающая полнотекстовую запись привилегированных команд (команд, управляющих системными функциями).

3.5 Объем памяти для хранения информации о событиях безопасности рассчитан и выделен с учетом типов событий безопасности, подлежащих регистрации, составом и содержанием информации о событиях безопасности, подлежащих регистрации, прогнозируемой частоты возникновения подлежащих регистрации событий безопасности, срока хранения информации о зарегистрированных событиях безопасности.

3.6 В информационной системе обеспечено централизованное автоматизированное управление сбором, записью и хранением информации о событиях безопасности.

3.7 Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти предусматривает:

– предупреждение (сигнализация, индикация) администраторов о сбоях (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (емкости) памяти) при регистрации событий безопасности;

– реагирование на сбои при регистрации событий безопасности путем изменения администраторами параметров сбора, записи и хранения информации о событиях безопасности, в том числе отключение записи информации о событиях

безопасности от части компонентов информационной системы, запись поверх устаревших хранимых записей событий безопасности.

3.8 В случае выявление признаков инцидентов безопасности в информационной системе осуществляется планирование и проведение мероприятий по реагированию на выявленные инциденты безопасности.

3.9 Получение меток времени, включающих дату и время, используемых при генерации записей регистрации (аудита) событий безопасности в информационной системе достигается посредством применения внутренних системных часов информационной системы.

3.10 В информационной системе обеспечивается резервное копирование записей регистрации (аудита).

3.11 Доступ к записям аудита и функциям управления механизмами регистрации (аудита) предоставляется только уполномоченным должностным лицам.

3.12 Защита информации о событиях безопасности (записях регистрации (аудита)) обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, и в том числе включает защиту средств ведения регистрации (аудита) и настроек механизмов регистрации событий.

4. Обнаружение вторжений

4.1 Обеспечение обнаружения (предотвращения) вторжений (компьютерных атак), направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней, осуществляется с использованием систем обнаружения вторжений.

4.2 Применяемая система обнаружения вторжений включает компоненты регистрации событий безопасности (датчики), компоненты анализа событий безопасности и распознавания компьютерных атак (анализаторы) и базу решающих правил, содержащую информацию о характерных признаках компьютерных атак.

4.3 Обнаружение (предотвращение) вторжений осуществляется на внешней границе информационной системы (системы обнаружения вторжений уровня сети) и (или) на внутренних узлах (системы обнаружения вторжений уровня узла) сегментов информационной системы (автоматизированных рабочих местах, серверах и иных узлах).

4.4 Права по управлению (администрированию) системами обнаружения вторжений предоставляются только уполномоченным должностным лицам.

4.5 В информационной системе обеспечивается централизованное управление (администрирование) компонентами системы обнаружения вторжений, установленными в различных сегментах информационной системы.

4.6 Обновление базы решающих правил системы обнаружения вторжений предусматривает:

– получение уведомлений о необходимости обновлений и непосредственном обновлении базы решающих правил;

– получение из доверенных источников и установку обновлений базы решающих правил;

– контроль целостности обновлений базы решающих правил.

4.7 В информационной системе обеспечивается возможность редактирования базы решающих правил (добавление и (или) исключение решающих правил) со стороны уполномоченных должностных лиц (администраторов).

5. Контроль (анализ) защищенности информации

5.1 При выявлении (поиске), анализе и устранении уязвимостей в информационной системе должны проводиться:

– выявление (поиск) уязвимостей, связанных с ошибками кода в программном (микропрограммном) обеспечении (общесистемном, прикладном, специальном), а также программном обеспечении средств защиты информации, правильностью установки и настройки средств защиты информации, технических средств и программного обеспечения, а также корректностью работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением;

– разработка по результатам выявления (поиска) уязвимостей отчетов с описанием выявленных уязвимостей и планом мероприятий по их устранению;

– анализ отчетов с результатами поиска уязвимостей и оценки достаточности реализованных мер защиты информации;

– устранение выявленных уязвимостей, в том числе путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств;

– информирование должностных лиц (пользователей, администраторов, подразделения по защите информации) о результатах поиска уязвимостей и оценки достаточности реализованных мер защиты информации.

5.2 В качестве источников информации об уязвимостях используются опубликованные данные разработчиков средств защиты информации, общесистемного, прикладного и специального программного обеспечения, технических средств, а также другие базы данных уязвимостей.

5.3 В случае невозможности устранения выявленных уязвимостей путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств необходимо предпринять действия (настройки средств защиты информации, изменение режима и порядка использования информационной системы), направленные на устранение возможности использования выявленных уязвимостей.

5.4 Для выявления (поиска) уязвимостей используется средство анализа (контроля) защищенности (сканер безопасности), имеющий стандартизованные (унифицированные) в соответствии с национальными стандартами описание и перечни программно- аппаратных платформ, уязвимостей программного обеспечения, ошибочных конфигураций, правил описания уязвимостей, проверочных списков, процедур тестирования и языка тестирования информационной системы на наличие уязвимостей, оценки последствий уязвимостей, имеющих возможность оперативного обновления базы данных выявляемых уязвимостей;

5.5 Уточнение перечня сканируемых в информационной системе уязвимостей с происходит с периодичностью: …, а также после появления информации о новых уязвимостях.

5.6 Доступ к функциям выявления (поиска) уязвимостей (предоставление такой возможности только администраторам безопасности) предоставляется только администраторам.

5.7 Контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода проводится с периодичностью: … и фиксируется в соответствующих журналах.

5.8 Получение обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода, осуществляется из доверенных источников.

5.9 При контроле установки обновлений осуществляются проверки соответствия версий общесистемного, прикладного и специального программного (микропрограммного) обеспечения, включая программное обеспечение средств защиты информации, установленного в информационной системе и выпущенного разработчиком, а также наличие отметок в эксплуатационной документации (формуляр или паспорт) об установке (применении) обновлений.

5.10 При контроле работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации осуществляется:

– контроль работоспособности (неотключения) программного обеспечения и средств защиты информации;

– проверка правильности функционирования (тестирование на тестовых данных, приводящих к известному результату) программного обеспечения и средств защиты информации, объем и содержание которой определяется оператором;

– контроль соответствия настроек программного обеспечения и средств защиты информации параметрам настройки, приведенным в эксплуатационной документации на систему защиты информации и средства защиты информации;

– восстановление работоспособности (правильности функционирования) и параметров настройки программного обеспечения и средств защиты информации (при необходимости), в том числе с использованием резервных копий и (или) дистрибутивов.

5.11 Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации проводится с периодичность: ….

5.12 В информационной системе обеспечивается регистрация событий и оповещение (сигнализация, индикация) администратора безопасности о событиях, связанных с нарушением работоспособности (правильности функционирования) и параметров настройки программного обеспечения и средств защиты информации.

5.13 При контроле состава технических средств, программного обеспечения и средств защиты информации осуществляется:

– контроль соответствия состава технических средств, программного обеспечения и средств защиты информации приведенному в эксплуатационной документации с целью поддержания актуальной (установленной в соответствии с

эксплуатационной документацией) конфигурации информационной системы и принятие мер, направленных на устранение выявленных недостатков;

– контроль состава технических средств, программного обеспечения и средств защиты информации на соответствие сведениям действующей (актуализированной) эксплуатационной документации и принятие мер, направленных на устранение выявленных недостатков;

– контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принятие мер, направленных на устранение выявленных недостатков;

– исключение (восстановление) из состава информационной системы несанкционированно установленных (удаленных) технических средств, программного обеспечения и средств защиты информации.

5.14 Контроль состава технических средств, программного обеспечения и средств защиты информации проводится с периодичностью: ….

5.15 В информационной системе обеспечивается регистрация событий безопасности, связанных с изменением состава технических средств, программного обеспечения и средств защиты информации.

5.16 При контроле правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе осуществляется:

– контроль правил генерации и смены паролей пользователей;

– контроль заведения и удаления учетных записей пользователей;

– контроль реализации правил разграничения доступом;

– контроль реализации полномочий пользователей;

– контроль наличия документов, подтверждающих разрешение изменений учетных записей пользователей, их параметров, правил разграничения доступом и полномочий пользователей;

– устранение нарушений, связанных с генерацией и сменой паролей пользователей, заведением и удалением учетных записей пользователей, реализацией правил разграничения доступом, установлением полномочий пользователей.

5.17 Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе проводится с периодичностью: ….

5.18 В информационной системе обеспечивается регистрация событий, связанных со сменой паролей пользователей, заведением и удалением учетных записей пользователей, изменением правил разграничения доступом и полномочий пользователей.

6. Обеспечение целостности информационной системы и информации

6.1 Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации, предусматривает:

– контроль целостности программного обеспечения средств защиты информации, включая их обновления, по наличию имен (идентификаторов) и (или) по контрольным суммам компонентов средств защиты информации в процессе загрузки и (или) динамически в процессе работы информационной системы;

– контроль целостности компонентов программного обеспечения (за исключением средств защиты информации), определяемого оператором исходя из возможности реализации угроз безопасности информации, по наличию имен (идентификаторов) компонентов программного обеспечения и (или) по контрольным суммам в процессе загрузки и (или) динамически в процессе работы информационной системы;

– контроль применения средств разработки и отладки программ в составе программного обеспечения информационной системы;

– тестирование с периодичностью: … функций безопасности средств защиты информации, в том числе с помощью тест-программ, имитирующих попытки несанкционированного доступа, и (или) специальных программных средств;

– обеспечение физической защиты технических средств информационной системы.

6.2 Контроль целостности средств защиты информации осуществляется по контрольным суммам всех компонентов средств защиты информации, как в процессе загрузки, так и динамически в процессе работы системы;

6.3 Исключается возможность использования средств разработки и отладки программ во время обработки и (или) хранения информации в целях обеспечения целостности программной среды.

6.4 Оператором должна быть предусмотрена возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций.

6.5 Возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций предусматривает:

– восстановление программного обеспечения, включая программное обеспечение средств защиты информации, из резервных копий (дистрибутивов) программного обеспечения;

– восстановление и проверка работоспособности системы защиты информации, обеспечивающие необходимый уровень защищенности информации;

– возврат информационной системы в начальное состояние (до возникновения нештатной ситуации), обеспечивающее ее штатное функционирование, или восстановление отдельных функциональных возможностей информационной системы, определенных оператором, позволяющих решать задачи по обработке информации.

6.6 Защита от спама реализуется на точках входа в информационную систему (выхода) информационных потоков (межсетевые экраны, почтовые серверы, Web-серверы, прокси-серверы и серверы удаленного доступа), а также на автоматизированных рабочих местах, серверах, подключенных к сетям связи общего пользования, для обнаружения и реагирования на поступление по электронной почте незапрашиваемых электронных сообщений (писем, документов) или в приложениях к электронным письмам.

7. Защита среды виртуализации

7.1 При реализации мер по идентификации и аутентификации субъектов доступа и объектов доступа в виртуальной инфраструктуре обеспечивается:

– идентификация и аутентификация администраторов управления средствами виртуализации;

– идентификация и аутентификация субъектов доступа при их локальном и удалённом обращении к объектам доступа в виртуальной инфраструктуре;

– блокировка доступа к компонентам виртуальной инфраструктуры для субъектов доступа, не прошедших процедуру аутентификации;

– защита аутентификационной информации субъектов доступа, хранящейся в компонентах виртуальной инфраструктуры от неправомерных доступа к ней, уничтожения или модифицирования;

– защита аутентификационной информации в процессе ее ввода для аутентификации в виртуальной инфраструктуре от возможного использования лицами, не имеющими на это полномочий; идентификация и аутентификация субъектов доступа при осуществлении ими попыток доступа к средствам управления параметрами аппаратного обеспечения виртуальной инфраструктуры.

7.2 Обеспечивается взаимная идентификация и аутентификация пользователя и сервера виртуализации (виртуальных машин) при удалённом доступе.

7.3 Обеспечивается управление доступом субъектов доступа к объектам доступа, в том числе внутри виртуальных машин.

7.4 По управлению доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре информационной системы обеспечивается:

– контроль доступа субъектов доступа к средствам управления компонентами виртуальной инфраструктуры;

– контроль доступа субъектов доступа к файлам-образам виртуализированного программного обеспечения, виртуальных машин, файлам-образам, служебным данным, используемым для обеспечения работы виртуальных файловых систем, и иным служебным данным средств виртуальной среды;

– управление доступом к виртуальному аппаратному обеспечению информационной системы, являющимся объектом доступа;

– контроль запуска виртуальных машин на основе заданных оператором правил (режима запуска, типа используемого носителя и иных правил)

– разграничение доступа субъектов доступа, зарегистрированных на виртуальных машинах, к объектам доступа, расположенным внутри виртуальных машин, в соответствии с правилами разграничения доступа пользователей данных виртуальных машин (потребителей облачных услуг);

– разграничение доступа субъектов доступа, зарегистрированных на виртуальных машинах, к ресурсам информационной системы, размещенным за пределами виртуальных машин, в соответствии с правилами разграничения доступа принятыми в информационной системе в целом.

7.5 В информационной системе обеспечивается доступ к операциям, выполняемым с помощью средств управления виртуальными машинами, в том числе к операциям создания, запуска, останова, создания копий, удаления виртуальных машин, который должен быть разрешен только администраторам виртуальной инфраструктуры;

7.6 Доступ к конфигурации виртуальных машин предоставляется только администраторам виртуальной инфраструктуры.

7.7 В виртуальной инфраструктуре дополнительно к событиям, установленным в п. 3.1 Настоящего положения, подлежат регистрации следующие события:

– запуск (завершение) работы компонентов виртуальной инфраструктуры;

– доступ субъектов доступа к компонентам виртуальной инфраструктуры;

– изменения в составе и конфигурации компонентов виртуальной инфраструктуры во время их запуска, функционирования и аппаратного отключения;

– изменения правил разграничения доступа к компонентам виртуальной инфраструктуры.

7.8 При регистрации запуска (завершения) работы компонентов виртуальной инфраструктуры состав и содержание информации, подлежащей регистрации, включают дату и время запуска (завершения) работы гипервизора и виртуальных машин, хостовой операционной системы, программ и процессов в виртуальных машинах, результат запуска (завершения) работы указанных компонентов виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке запуска (завершения) работы указанных компонентов виртуальной инфраструктуры.

7.9 При регистрации входа (выхода) субъектов доступа в компоненты виртуальной инфраструктуры состав и содержание информации, подлежащей регистрации, включают дату и время доступа субъектов доступа к гипервизору и виртуальной машине, к хостовой операционной системе, результат попытки доступа субъектов доступа к указанным компонентам виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке доступа субъектов доступа к указанным компонентам виртуальной инфраструктуры.

7.10 При изменении в составе и конфигурации компонентов виртуальной инфраструктуры во время запуска, функционирования и в период её аппаратного отключения состав и содержание информации, подлежащей регистрации, включают дату и время изменения в составе и конфигурации виртуальных машин, виртуального аппаратного обеспечения, виртуализированного программного обеспечения, виртуального аппаратного обеспечения в гипервизоре и в виртуальных машинах, в хостовой операционной системе, виртуальном сетевом оборудовании, результат попытки изменения в составе и конфигурации указанных компонентов виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке изменения в составе и конфигурации указанных компонентов виртуальной инфраструктуры.

7.11 При изменении правил разграничения доступа к компонентам виртуальной инфраструктуры состав и содержание информации, подлежащей регистрации, включают изменения правил разграничения доступа к виртуальному и физическому аппаратному обеспечению, к файлам- образам виртуализированного программного обеспечения и виртуальных машин, к файлам-образам, используемым для обеспечения работы виртуальных файловых систем, к виртуальному сетевому оборудованию, к защищаемой информации, хранимой и обрабатываемой в гипервизоре и виртуальных машинах, в хостовой операционной системе, результат попытки изменения правил разграничения доступа к указанным компонентам виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке изменения правил разграничения доступа к указанным компонентам виртуальной инфраструктуры.

7.12 При управлении потоками информации между компонентами виртуальной инфраструктуры обеспечиваются:

– фильтрация сетевого трафика между компонентами виртуальной инфраструктуры, в том числе между внешними по отношению к серверу виртуализации сетями и внутренними по отношению к серверу виртуализации сетями, в том числе при организации сетевого обмена с сетями связи общего пользования;

– обеспечение доверенных канала, маршрута внутри виртуальной инфраструктуры между администратором, пользователем и средствами защиты информации (функциями безопасности);

– контроль передачи служебных информационных сообщений, передаваемых в виртуальных сетях гипервизора, хостовой операционной системы, по составу, объёму и иным характеристикам;

– отключение неиспользуемых сетевых протоколов компонентами виртуальной инфраструктуры гипервизора, хостовой операционной системы, виртуальной вычислительной сети; обеспечение подлинности сетевых соединений (сеансов взаимодействия) внутри виртуальной инфраструктуры, в том числе для защиты от подмены сетевых устройств и сервисов;

– обеспечение изоляции потоков данных, передаваемых и обрабатываемых компонентами виртуальной инфраструктуры (гипервизором, хостовой операционной системой) и сетевых потоков виртуальной вычислительной сети;

– семантический и статистический анализ сетевого трафика виртуальной вычислительной сети.

7.13 При управлении перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных обеспечиваются:

– регламентирование порядка перемещения (определение ответственных за организацию процесса, объектов перемещения, ресурсов инфраструктуры, задействованных в перемещении, а также способов перемещения);

– управление размещением и перемещением файлов-образов виртуальных машин (контейнеров) между носителями (системами хранения данных);

– управление размещением и перемещением исполняемых виртуальных машин (контейнеров) между серверами виртуализации; управление размещением и перемещением данных, обрабатываемых с использованием виртуальных машин, между носителями (системами хранения данных).

7.14 Управление перемещением виртуальных машин (контейнеров) предусматривает:

– полный запрет перемещения виртуальных машин (контейнеров);

– ограничение перемещения виртуальных машин (контейнеров) в пределах информационной системы (сегмента информационной системы);

– ограничение перемещения виртуальных машин (контейнеров) между сегментами информационной системы.

7.15 Перемещение виртуальных машин (контейнеров) и обрабатываемых на них данных осуществляется в пределах информационной системы только на контролируемые технические средства (сервера виртуализации, носители, системы хранения данных).

7.16 В информационной системе должен обеспечиваться контроль целостности компонентов виртуальной инфраструктуры в соответствии с гл. 6 настоящего Положения.

7.17 При контроле целостности компонентов виртуальной инфраструктуры обеспечивается:

– контроль целостности компонентов, критически важных для функционирования хостовой операционной системы, гипервизора, гостевых операционных систем и (или) обеспечения безопасности обрабатываемой в них информации (загрузчика, системных файлов, библиотек операционной системы и иных компонентов);

– контроль целостности состава и конфигурации виртуального оборудования;

– контроль целостности файлов, содержащих параметры настройки виртуализированного программного обеспечения и виртуальных машин;

– контроль целостности файлов-образов виртуализированного программного обеспечения и виртуальных машин, файлов-образов, используемых для обеспечения работы виртуальных файловых систем (контроль файлов-образов должен проводиться во время, когда файлы-образы не задействованы).

7.18 В информационной системе обеспечивается контроль целостности резервных копий виртуальных машин (контейнеров).

7.19 В информационной системе обеспечивается контроль состава аппаратной части компонентов виртуальной инфраструктуры.

7.20 В информационной системе обеспечивается резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры и каналов связи внутри виртуальной инфраструктуры в соответствии с Инструкцией о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты в ГИС.

7.21 При реализации мер по резервному копированию данных, резервированию технических средств, программного обеспечения виртуальной инфраструктуры обеспечивается:

– определение мест хранения резервных копий виртуальных машин (контейнеров) и данных, обрабатываемых в виртуальной инфраструктуре;

– резервное копирование виртуальных машин (контейнеров);

– резервное копирование данных, обрабатываемых в виртуальной инфраструктуре;

– резервирование программного обеспечения виртуальной инфраструктуры; резервирование каналов связи, используемых в виртуальной инфраструктуре;

– периодическая проверка резервных копий и возможности восстановления виртуальных машин (контейнеров) и данных, обрабатываемых в виртуальной инфраструктуре с использованием резервных копий.

7.22 Реализация и управление антивирусной защитой в виртуальной инфраструктуре обеспечивается в соответствии с Инструкцией по организации антивирусной защиты в ГИС, при этом обеспечивается:

– проверка наличия вредоносных программ (вирусов) в хостовой операционной системе, включая контроль файловой системы, памяти, запущенных приложений и процессов;

– проверка наличия вредоносных программ в гостевой операционной системе, в процессе ее функционирования, включая контроль файловой системы, памяти, запущенных приложений и процессов.

7.23 В информационной системе обеспечивается разграничение доступа к управлению средствами антивирусной защиты.

8. Защита технических средств

8.1 Оператором обеспечивается контролируемая зона, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования.

8.2 Контролируемая зона включает пространство (территорию, здание, часть здания), в котором исключено неконтролируемое пребывание работников (сотрудников) оператора и лиц, не имеющих постоянного допуска на объекты информационной системы (не являющихся работниками оператора), а также транспортных, технических и иных материальных средств.

8.3 Границы контролируемой зоны определены в Приказе об определении границ контролируемой зоны.

8.4 Контроль и управление физическим доступом предусматривают:

– определение лиц, допущенных к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены;

– санкционирование физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены;

– учет физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены.

8.5 Размещение устройств вывода (отображения, печати) информации исключает возможность несанкционированного просмотра выводимой информации, как из-за пределов контролируемой зоны, так и в пределах контролируемой зоны.

9. Защита информационной системы, ее средств и систем связи и передачи данных

9.1 В информационной системе обеспечивается разделение функциональных возможностей по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации (функций безопасности) и функциональных возможностей пользователей по обработке информации.

9.2 Функциональные возможности по управлению (администрированию) информационной системой и управлению (администрированию) системой защиты информации включают функции по управлению базами данных, прикладным программным обеспечением, телекоммуникационным оборудованием, рабочими

станциями, серверами, средствами защиты информации и иные функции, требующие высоких привилегий.

9.3 Разделение функциональных возможностей обеспечивается на физическом и (или) логическом уровне путем выделения части программно-технических средств информационной системы, реализующих функциональные возможности по управлению (администрированию) информационной системой и управлению (администрированию) системой защиты информации, в отдельный домен, использования различных автоматизированных рабочих мест и серверов, различных типов операционных систем, разных способов аутентификации, различных сетевых адресов, выделенных каналов управления и (или) комбинаций данных способов, а также иными методами.

9.4 В информационной системе обеспечивается выделение автоматизированных рабочих мест для администраторов безопасности.

9.5 Защита информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны обеспечивается путем защиты каналов связи от несанкционированного физического доступа (подключения) к ним и (или) применения в соответствии с законодательством Российской Федерации средств криптографической защиты информации или иными методами.

9.6 Для исключения возможности отрицания пользователем факта отправки информации другому пользователю осуществляется:

– определение объектов или типов информации, для которых требуется обеспечение неотказуемости отправки (например, сообщения электронной почты);

– обеспечение целостности информации при ее подготовке к передаче и непосредственной ее передаче по каналам связи;

– регистрация событий, связанных с отправкой информации другому пользователю.

9.7 Для исключения возможности отрицания пользователем факта получения информации осуществляется:

– определение объектов или типов информации, для которых требуется обеспечение неотказуемости получения (сообщения электронной почты);

– обеспечение целостности полученной информации;

– регистрация событий, связанных с получением информации от другого пользователя.

9.8 В информационной системе обеспечивается защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения, иных данных, не подлежащих изменению в процессе обработки информации.

9.9 Оператором должна быть обеспечена защита беспроводных соединений, применяемых в информационной системе.

9.10 Защита беспроводных соединений включает:

– предоставление доступа к параметрам(изменению параметров) настройки беспроводных соединений только администраторам информационной системы;

– обеспечение возможности реализации беспроводных соединений только через контролируемые интерфейсы (в том числе, путем применения средств защиты информации);

– регистрация и анализ событий, связанных с использованием беспроводных соединений, в том числе для выявления попыток несанкционированного подключения к информационной системе через беспроводные соединения.

9.11 В информационной системе осуществляется защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями, предусматривающая:

– управление (контроль) входящими в информационную систему и исходящими из информационной системы информационными потоками на физической и (или) логической границе информационной системы (сегментов информационной системы);

– обеспечение взаимодействия информационной системы и (или) ее сегментов с иными информационными системами и сетями только через сетевые интерфейсы, которые обеспечивают управление (контроль) информационными потоками с использованием средств защиты информации (управляемые (контролируемые) сетевые интерфейсы), установленных на физическом и (или) логическом периметре информационной системы или ее отдельных сегментов (маршрутизаторов, межсетевых экранов, коммутаторов, прокси-серверов, шлюзов безопасности, средств построения виртуальных частных сетей и иных средств защиты информации).

9.12 В информационной системе должно быть обеспечено предоставление доступа во внутренние сегменты информационной системы (демилитаризованную зону) из внешних информационных систем и сетей только через средства защиты периметра (за исключением внутренних сегментов, которые специально выделены для такого взаимодействия).

9.13 В информационной системе применяется отдельный физический управляемый (контролируемый) сетевой интерфейс для каждого внешнего телекоммуникационного сервиса.

9.14 В информационной системе обеспечивается защита информации при ее передаче по каналам связи, имеющим выход за пределы контролируемой зоны (при необходимости), путем применения организационно-технических мер или криптографических методов.

9.15 В информационной системе исключается выход (вход) через управляемые (контролируемые) сетевые интерфейсы информационных потоков по умолчанию (реализация принципа «запрещено все, что не разрешено»).

Консультант _____ Ч.К. Сарыглар