ПРИЛОЖЕНИЕ № 20
к приказу
от 6 августа 2024 г.
№ 65-ос

ПРАВИЛА
защиты периметра информационных систем Государственного комитета по охране объектов животного мира Республики Тыва при их взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями

1. Общие положения

В информационных системах Государственного комитета по охране объектов животного мира Республики Тыва (далее – ИС Госкомохотнадзора РТ) осуществляется защита периметра (физических и (или) логических границ) при их взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями, предусматривающая:

- управление (контроль) входящими в ИС Госкомохотнадзора РТ и исходящими из ИС Госкомохотнадзора РТ информационными потоками на физической и (или) логической границе ИС Госкомохотнадзора РТ;
- обеспечение взаимодействия ИС Госкомохотнадзора РТ 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 ИС Госкомохотнадзора РТ (маршрутизаторов, межсетевых экранов, коммутаторов, прокси-серверов, шлюзов безопасности, средств построения виртуальных частных сетей и иных средств защиты информации).

Количество точек доступа в ИС Госкомохотнадзора РТ определяется администратором информационной безопасности с учетом функций ИС Госкомохотнадзора РТ при этом количество точек должно быть минимальным и должен обеспечиваться постоянный и всесторонний контроль входящих и исходящих информационных потоков.

2. Защита информации от раскрытия, модификации и навязывания при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны

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

3. Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств

В ИС Госкомохотнадзора РТ осуществляется запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств, в том числе путем сигнализации, индикации.

Запрет несанкционированной удаленной активации осуществляется в отношении всех периферийных устройств ввода (вывода) информации, которые имеют возможность управления (запуска, включения, выключения) через компоненты программного обеспечение, установленные на рабочем месте пользователя, коммуникационных сервисов сторонних лиц (провайдеров) (ICQ, Skype и иные сервисы).

Запрет несанкционированной удаленной активации осуществляется путем физического исключения такой возможности или путем управления программным обеспечением.

В исключительных случаях для решения установленных оператором отдельных задач, решаемых информационной системой, допускается возможность удаленной активации периферийных устройств.

4. Защита беспроводных соединений, применяемых в информационной системе

В ИС Госкомохотнадзора РТ обеспечена защита беспроводных соединений, применяемых в ИС. Защита беспроводных соединений включает:

- ограничение на использование в ИС беспроводных соединений (в частности 802.11xWi-Fi в соответствии с задачами (функциями) ИС, для решения которых такие соединения необходимы;
- предоставление доступа к параметрам (изменению параметров) настройки беспроводных соединений только администраторам ИС;

– 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.

При обеспечении защиты беспроводных соединений принимаются меры по идентификации и аутентификации в соответствии с Правилами ИАФ.

При невозможности исключения установления беспроводных соединений из-за пределов контролируемой зоны должны приниматься меры защищенного удаленного доступа в соответствии с Положением об управлении доступом субъектов доступа к объектам доступа в информационных системах Государственного комитета по охране объектов животного мира Республики Тыва и п. 2 настоящих Правил.

5. Защита мобильных технических средств, применяемых в ИС Госкомохотнадзора РТ

К мобильным техническим средствам в ИС Госкомохотнадзора РТ относятся:

– съемные машинные носители информации.

Защита мобильных технических средств включает:

– реализацию в зависимости от мобильного технического средства (типа мобильного технического средства) мер по:

o идентификации и аутентификации в соответствии с Правилами идентификации и аутентификации субъектов доступа и объектов доступа в информационных системах Государственного комитета по охране объектов животного мира Республики Тыва;

o управлению доступом в соответствии с Положением об управлении доступом субъектов доступа к объектам доступа в информационных системах Государственного комитета по охране объектов животного мира Республики Тыва;

o ограничению программной среды в соответствии с Правилами по ограничению программной среды в информационных системах Государственного комитета по охране объектов животного мира Республики Тыва;

o защите машинных носителей информации в соответствии с настоящими Правилами;

o регистрации событий безопасности в соответствии с Правилами регистрации событий безопасности в информационных системах Государственного комитета по охране объектов животного мира Республики Тыва;

- антивирусной защите в соответствии с Инструкцией по антивирусной защите в информационных системах Государственного комитета по охране объектов животного мира Республики Тыва;
- контролю (анализу) защищенности в соответствии с Инструкцией по контролю защищенности информации в информационных системах Государственного комитета по охране объектов животного мира Республики Тыва;

– очистку (удаление) информации в мобильном техническом средстве после завершения сеанса удаленного доступа к защищаемой информации или принятие иных мер, исключающих несанкционированный доступ к хранимой защищаемой информации;

– уничтожение съемных машинных носителей информации, которые не подлежат очистке;

– выборочные проверки мобильных технических средств (на предмет их наличия) и хранящейся на них информации (например, на предмет отсутствия информации, не соответствующей маркировке носителя информации);

– запрет возможности автоматического запуска (без команды пользователя) в информационной системе программного обеспечения на мобильных технических средствах;

– контроль использования в ИС мобильных технических средств.

В ИС допускаются проводные (коммутируемые), беспроводные и широкополосные доступы к объектам доступа информационной системы с использованием мобильных технических средств: съемных машинных носителей информации ({перечень_съемных_носителей}).

Контроль использования мобильных технических средств в ИС Госкомохотнадзор РТ включает:

– использование в составе ИС для доступа к объектам доступа мобильных технических средств (служебных мобильных технических средств), в которых реализованы меры защиты информации в соответствии с Правилами обращения с машинными носителями информации и мобильными техническими средствами в информационных системах Государственного комитета по охране объектов животного мира Республики Тыва;

– ограничение на использование мобильных технических средств в соответствии с задачами (функциями) ИС, для решения которых использование таких средств необходимо, и предоставление доступа с использованием мобильных технических средств;

– мониторинг и контроль применения мобильных технических средств на предмет выявления несанкционированного использования мобильных технических средств для доступа к объектам доступа ИС;

– запрет возможности запуска без команды пользователя в информационной системе ПО (программного кода), используемого для взаимодействия с мобильным техническим средством;

– применение мобильных технических средств, включая процедуры выдачи и возврата мобильных технических средств, а также их передачи на техническое обслуживание (процедура должна обеспечивать удаление или недоступность информации), в соответствии с требованиями Правил обращения с машинными носителями информации и мобильными техническими средствами в информационных системах Государственного комитета по охране объектов животного мира Республики Тыва.

Лист ознакомления
с Правилами защиты периметра информационных систем Государственного комитета по охране объектов животного мира Республики Тыва при их взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями

№ п/п	ФИО	Должность	Дата ознакомления	Подпись
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				