|  |  |
| --- | --- |
|  | УТВЕРЖДЕН  приказом ГКУ НСО ЦСПН города Бердска  от 07 апреля 2025 № 28 \_\_\_\_\_\_\_\_\_\_\_ |

**Регламент**

**защиты информационной системы, ее средств, систем связи и передачи данных**

1. Общие положения

1.1 Настоящий Регламент разработан в целях реализации мер по защите периметра (физических и (или) логических границ) информационных систем (далее – ИС) ГКУ НСО ЦСПН города Бердска с установленным **2-м классом защищенности** при их взаимодействии с иными ИС и информационно-телекоммуникационными сетями, предусматривающий:

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

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

1.3 Настоящий Регламент предназначена для обеспечения защиты информации, обрабатываемой в ИС, при функционировании ИС и определяет порядок действий администратора безопасности ИС при эксплуатации ИС.

1. Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода

2.1 В ИС осуществляется контроль санкционированного и исключение несанкционированного использования технологий мобильного кода (активного контента), в том числе регистрация событий, связанных с использованием технологии мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологии мобильного кода. Технология мобильного кода включает, в том числе использование Java, JavaScript, ActiveX, PDF, Postscript, Flash-анимация и VBScript и иных технологий.

2.2 При контроле использования технологий мобильного кода обеспечивается:

* определение перечня мобильного кода и технологий мобильного кода разрешенных и (или) запрещенных для использования в ИС;
* определение разрешенных мест распространения (серверы информационной системы) и использования мобильного кода;
* (автоматизированные рабочие места, мобильные технические средства информационной системы) и функций ИС, для которых необходимо применение технологии мобильного кода;
* регистрация и анализ событий, связанных с разработкой, приобретением или внедрением технологии мобильного кода;
* исключение возможности использования запрещенного мобильного кода в ИС, а также внедрение мобильного кода в местах, не разрешенных для его установки.

2.3 В ИС определены механизмы обнаружения и анализа мобильного кода для выявления фактов несанкционированного использования мобильного кода и выполнения действий по реагированию (оповещение администраторов, изоляция мобильного кода (перемещение в карантин), блокирование мобильного кода, удаление мобильного кода).

1. Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов

В ИС осуществляется обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов (защита от атак типа «человек посередине»).

Для подтверждения подлинности сторон сетевого соединения (сеанса взаимодействия) и защиты сетевых устройств и сервисов от подмены осуществляться их аутентификация в соответствии с Инструкцией идентификации и аутентификации субъектов доступа и объектов доступа.

1. Исключение возможности отрицания пользователем факта отправки/получения информации другому пользователю

В ИС обеспечивается исключение возможности отрицания пользователем факта отправки/получения информации другому пользователю.

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

* определение объектов или типов информации, для которых требуется обеспечение неотказуемости отправки/получения (например, сообщения электронной почты);
* обеспечение целостности информации при ее подготовке к передаче и непосредственной ее передаче по каналам связи в соответствии с п.2 настоящего Регламента;
* регистрация событий, связанных с отправкой/получением информации другому пользователю в соответствии с Инструкцией регистрации событий безопасности.

1. Исключение возможности отрицания пользователем факта получения информации от другого пользователя

В ИС обеспечивается исключение возможности отрицания пользователем факта получения информации от другого пользователя.

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 в соответствии с п.3 настоящего Регламента;
* регистрация событий, связанных с получением информации от другого пользователя в соответствии с Инструкцией регистрации событий безопасности.

1. Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации

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

Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации, обеспечивается принятием мер защиты информации, направленных на обеспечение их конфиденциальности и целостности.

Защита данных, не подлежащих изменению в процессе обработки информации, обеспечивается в отношении информации, хранящейся на жестких магнитных дисках, дисковых накопителях и иных накопителях в информационной системе.

1. Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании этой информационной системы

В ИС обеспечивается защита от угроз безопасности информации, направленных на отказ в обслуживании этой системы.

Защита от угроз безопасности информации, направленных на отказ в обслуживании, осуществляется посредством реализации в ИС мер защиты информационной системы в соответствии с настоящим Регламентом и повышенными характеристиками производительности телекоммуникационного оборудования и каналов передачи совместно с резервированием информации и технических средств, программного обеспечения, каналов передачи информации в соответствии с Инструкцией обеспечения доступности.

1. Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями

В ИС осуществляется защита периметра (физических и (или) логических границ) ИС при ее взаимодействии с иными ИС и информационно-телекоммуникационными сетями, предусматривающая:

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

В ИС обеспечена возможность размещения публичных общедоступных ресурсов (в частности, общедоступный веб-сервер), взаимодействующих с ИС через отдельные физические управляемые (контролируемые) сетевые интерфейсы.

Предоставление доступа во внутренние сегменты ИС (демилитаризованную зону) из внешних ИС и сетей возможно только через средства защиты периметра (за исключением внутренних сегментов, которые специально выделены для такого взаимодействия).

В ИС ограничено количество точек доступа в ИС из внешних ИС и сетей до минимально необходимого числа для решения постановленных задач, а также обеспечивающего постоянный и всесторонний контроль входящих и исходящих информационных потоков.

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

В ИС установлены правила управления информационными потоками для каждого физического управляемого (контролируемого) сетевого интерфейса.

В ИС 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 в соответствии с законодательством Российской Федерации.

В ИС обеспечивается удаление введенных исключений из правил управления информационными потоками после истечения установленного времени.

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

1. Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения

В ИС осуществляется завершение сетевых соединений (например, открепление пары порт/адрес (ТСР/IP)) по их завершении и (или) по истечении заданного оператором временного интервала неактивности сетевого соединения.

# Защита мобильных технических средств, применяемых в ИС

К мобильным техническим средствам в ИС относятся:

* съемные машинные носители информации,
* портативные вычислительные устройства и устройства связи с возможностью обработки информации.

Защита мобильных технических средств включает:

* реализацию в зависимости от мобильного технического средства (типа мобильного технического средства) мер по:
  + идентификации и аутентификации в соответствии с Инструкцией идентификации и аутентификации субъектов доступа и объектов доступа,
  + управлению доступом в соответствии с Инструкцией управления доступом субъектов доступа к объектам доступа;
  + ограничению программной среды в соответствии с Инструкцией ограничения программной среды;
  + защите машинных носителей информации в соответствии с настоящим Регламентом;
  + регистрации событий безопасности в соответствии с Инструкцией регистрации событий безопасности;
  + антивирусной защите в соответствии с Инструкцией антивирусной защиты и обнаружения вторжений;
  + контролю (анализу) защищенности в соответствии с Инструкцией контроля защищенности информации.
* 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 ИС 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 ИС с использованием мобильных технических средств: съемных машинных носителей информации (флэш-накопители, внешние накопители на жестких дисках), портативных вычислительных устройств и устройств связи с возможностью обработки информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства).

Контроль использования мобильных технических средств в ИС 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 Инструкцией обращения с машинными носителями информации и мобильными техническими средствами в ИС ГКУ НСО ЦСПН города Бердска;
* 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 Инструкцией обращения с машинными носителями информации и мобильными техническими средствами.

В ИС обеспечивается запрет использования в ИС не входящих в ее состав (находящихся в личном использовании) съемных машинных носителей информации.

В ИС обеспечивается запрет использования в ИС съемных машинных носителей информации, для которых не определен владелец (пользователь, организация, ответственные за принятие мер защиты информации).