**Политика по обеспечению защиты информации от несанкционированного доступа в локальной вычислительной сети Администрации Правительства Кузбасса**

Защита информации, обрабатываемой в локальной вычислительной сети Администрации Правительства Кузбасса (далее – ЛВС АПК) и Министерства цифрового развития и связи Кузбасса (далее - Министерство), от несанкционированного доступа реализуется комплексом программно-технических средств и организационных мероприятий, основными из которых являются:

- организация парольной защиты;
- регистрация и учет действий пользователя;
- проведение антивирусного контроля;
- включение хранителя экрана через 10 минут бездействия пользователя.

## 1. Общие положения

Министерство цифрового развития и связи Кузбасса – оператор ЛВС АПК.

Государственное казенное учреждение «Центр информационных технологий Кузбасса» - технический оператор, администратор ЛВС АПК.

Пользователи ЛВС АПК – государственные служащие, гражданские служащие органов государственной власти Кемеровской области – Кузбасса, иных государственных органов Кемеровской области - Кузбасса, использующие ЛВС АПК для исполнения своих полномочий.

Органы государственной власти Кемеровской области – Кузбасса, иные государственные органы Кемеровской области - Кузбасса при использовании ЛВС АПК обязаны заключить соглашение об информационном взаимодействии с Оператором ЛВС АПК. Соглашение заключается в электронном виде через информационную систему «Реестр государственных информационных систем Кемеровской области – Кузбасса» (ris.kemobl.ru).

Пользователи ЛВС АПК обязаны неукоснительно соблюдать требования информационной безопасности при работе в ЛВС АПК.

## 2. Создание учетных записей.

С целью соблюдения принципа персональной ответственности за свои действия каждому должностному лицу, допущенному к работе в ЛВС АПК, должно быть сопоставлено персональное уникальное имя (учетная запись) пользователя по принципу «фамилия-инициалы».

Аналогичное правило применяется для должностных лиц органов государственной власти Кемеровской области – Кузбасса, иных государственных органов Кемеровской области - Кузбасса при допуске в ЛВС АПК и к конфиденциальной информации. Использование несколькими должностными лицами, одного и того же имени пользователя («группового

имени»), равно как и работа под именем другого пользователя **запрещены**. Исключение составляет проведение процедуры проверки правильности настроек подсистем, выполняемой администраторами.

Учетные записи администраторов должны использоваться только для осуществления процедуры администрирования подсистем. Администраторам, если на них возложены обязанности по работе на одном из автоматизированных рабочих мест, сопоставляется другое уникальное имя. В таких случаях допуск осуществляется аналогично пользователям системы.

## 3. Организация парольной защиты

Идентификация и проверка подлинности пользователя ЛВС АПК при входе в систему осуществляется по идентификатору (персональному уникальному имени) и паролю условно-постоянного действия, дополнительно для идентификации пользователей могут применяться идентификаторы типа Рутокен, Touch Memory и др., соответствующие требованиям для управления ими с помощью средства защиты информации «Secret Net» или иных средств защиты от несанкционированного доступа, имеющих действующий сертификат ФСТЭК России.

Парольная защита устанавливается на:

- запуск программы конфигурации аппаратного обеспечения средств вычислительной техники (BIOS);
- процесс загрузки операционной системы (при необходимости выполнения соответствующих требований);
- вход в сетевую операционную систему;
- программу - хранитель экрана;
- доступ к многопользовательским прикладным программным системам и базам данных, содержащих механизмы идентификации и подтверждения подлинности пользователей по значениям паролей.

Программно - техническое обеспечение процесса организации парольной защиты осуществляется:

- сертифицированной системой защиты от несанкционированного доступа для защиты процесса загрузки операционной системы, входа в сетевую операционную систему, программы-хранителя экрана;
- штатными средствами программы конфигурации аппаратного обеспечения;
- штатными средствами прикладных программных систем и программ управления базами данных.

Организационное обеспечение процессов генерации, использования, смены и удаления паролей осуществляют администраторы в пределах их компетенции. Пароль на программу конфигурации (например, BIOS) аппаратного обеспечения устанавливает администратор ЛВС АПК.

Пароли выбираются пользователями ЛВС АПК самостоятельно.

Пользователю ЛВС АПК **запрещается** сообщать кому-либо свой личный пароль.

Назначаемые пароли должны отвечать следующим требованиям:

- длина пароля должна быть не менее восьми символов;

- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, дни рождения и другие памятные даты, номера телефонов, автомобилей, адреса места жительства, наименования автоматизированного рабочего места и т.д.), а также общепринятые сокращения (USER, ADMIN, ALEX, ЭВМ, ЛВС, GUEST, ADMINISTRATOR и т.д.) и другие данные, которые могут быть подобраны злоумышленником путем анализа информации о пользователе;

– не использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

- не использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);

- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;

- не использовать ранее использованные пароли.

При отсутствии функционала программного обеспечения в части установки указанных выше требований к паролям, устанавливаются требования максимально к ним приближенные.

Пользователю автоматизированной системы запрещается:

- до идентификации и аутентификации начинать обработку конфиденциальной информации в ЛВС АПК;

- записывать свои пароли в очевидных местах, внутренности ящика стола, на мониторе, на обратной стороне клавиатуры и т.д.;

- хранить пароли в записанном виде на отдельных листах бумаги;

- сообщать свои пароли посторонним лицам;

- произносить свой пароль вслух;

- использовать общие пароли совместно с другими коллегами по работе;

- предпринимать какие-либо действия по получению (раскрытию) паролей других пользователей.

Смена пароля должна проводиться не реже, чем 1 раз в 90 календарных дней.

Число совершенных подряд неудачных попыток ввода пароля не должно превышать 10.

В случае отсутствия технической возможности установки пароля пользователем самостоятельно, установка пароля производится при участии администраторов.

О случаях компрометации пароля пользователи ЛВС АПК обязаны немедленно сообщать администраторам. Администраторы должны незамедлительно принять меры для предотвращения утечки информации (блокировка учетной записи пользователя, просмотр системных журналов, выявление фактов несанкционированного доступа и т.д.).

К событиям, связанным с компрометацией паролей, относятся:

- разглашение паролей пользователями ЛВС АПК или визуальное ознакомление с паролем посторонними лицами;
- регистрация пользователя во время его отсутствия;
- утрата устройств идентификации пользователей ЛВС АПК;
- использование устройств идентификации посторонними лицами без контроля со стороны владельца.

По всем фактам компрометации паролей проводится служебное расследование.

Внеплановая смена (удаление) личного пароля пользователя автоматизированной системы (далее - АС) или блокировка учетной записи пользователя ЛВС АПК производится в случае:

- прекращения полномочий пользователя ЛВС АПК (увольнение, переход на другую работу внутри органов государственной власти Кемеровской области – Кузбасса, иных государственных органов Кемеровской области - Кузбасса) непосредственно после окончания последнего сеанса работы данного пользователя ЛВС АПК с системой;
- компрометации пароля пользователя ЛВС АПК.

Полная внеплановая смена паролей производится в случае прекращения полномочий (увольнение, переход на другую работу внутри органов государственной власти Кемеровской области – Кузбасса, иных государственных органов Кемеровской области - Кузбасса и другие обстоятельства) администраторов, которым были предоставлены либо полномочия по управлению ЛВС АПК в целом или отдельными ее частями, либо полномочия по управлению подсистемой защиты информации.

При длительном бездействии (неактивности) пользователя ЛВС АПК производится блокирование в информационной системе сеанса работы пользователя по истечению времени, заданного в параметрах настроек - не более 10 минут, для возобновления сеанса работы пользователю необходимо повторно пройти аутентификацию по паролю.

Если пользователю необходимо отойти на некоторое время и не завершать свой сеанс, можно заблокировать компьютер, выполнив следующие действия:

– использовать «горячие клавиши» - нажать комбинацию клавиш <Ctrl> + <Alt> + <Del>;

– далее, в появившемся на экране окне, нажать кнопку «Блокировка».

При возобновлении сеанса работы пользователю необходимо ввести свой пароль.

## 4. Регистрация и учет действий пользователей

Для контроля за действиями пользователей АС осуществляется регистрация событий происходящих на средства вычислительной техники объекта информатизации Министерства и АПК. Программно - техническое обеспечение данного процесса осуществляется подсистемами регистрации и учета (аудита) средств защиты информации, сетевой операционной системы и прикладных программных систем.

Регистрации подлежат события связанные с обеспечением безопасности информации, такие как: вход (выход) пользователя АС в систему (из системы), изменение полномочий пользователя АС, запуск (завершение) программ, предназначенных для обработки защищаемой информации, доступ к защищаемым информационным ресурсам, вывод информации на машинный носитель информации, факты попыток несанкционированного доступа.

Регистрация действий пользователей осуществляется в специальных электронных журналах. Копии электронных журналов должны хранится не менее 1 года со дня внесения в них последней записи.

Доступ к электронным журналам должен быть организован таким образом, чтобы исключить возможность внесения изменений (удаления записей) пользователями ЛВС АПК.

Электронные журналы используются при разборе конфликтных ситуаций, для проверки правильности (корректности) работы программных и технических средств, а также при определении попыток несанкционированного доступа.

## 5. Порядок проведения антивирусного контроля

Для предотвращения частичного или полного уничтожения или изменения информации, циркулирующей на объекте информатизации АПК и Министерства от воздействия вредоносных программ – «закладок» и других компьютерных вирусов на средства вычислительной техники устанавливаются антивирусные средства.

К использованию допускаются только лицензионные антивирусные средства, имеющие сертификат соответствия требованиям по безопасности информации ФСТЭК России.

Установка средств управления средствами антивирусной защиты осуществляется Администратором ЛВС АПК в соответствии с технической документацией на используемые средства защиты от вредоносного программного обеспечения.

Настройка средств управления средствами антивирусной защиты осуществляется Администратором информационной безопаснсоти Министерства.

Установка и настройка клиентских частей средств антивирусной защиты на серверах и автоматизированных рабочих местах (далее – АРМ) сотрудников осуществляется администратором соответствующего

прикладного программнного обеспечения, назначаемого из числа сотрудников ГКУ «ЦИТ Кузбасса». Установка и настройка осуществляется в соответствии с технической документацией и рекомендациями отдела информационной безопасности управления информационной безопасности и связи Министерства.

На всех серверах и АРМ работников необходимо использовать настройки средств защиты от вредоносных программ, позволяющие:

- осуществлять автоматическую антивирусную проверку и «лечение» файлов в момент попытки записи или считывания файла;
- проверять каталоги и файлы по расписанию (с учетом нагрузки на сервер).

Работникам запрещается отключать средства антивирусной защиты и самостоятельно вносить изменения в настройки антивирусного программного обеспечения.

Актуализация антивирусных баз, администрирование и управление компонентами подсистемы антивирусной защиты выполняются централизованно. Обновление антивирусных баз с использованием доступа в сеть Интернет разрешено только с использованием средств криптографической защиты информации, имеющими сертификат соответствия ФСБ России и ФСТЭК России.

Полная антивирусная проверка рабочих станций и серверов должна осуществляться не реже 1 раза в неделю. Администратор информационной безопасности обязан проводить постоянный контроль результатов проверки и в случае обнаружения вирусной активности докладывать начальнику отдела информационной безопасности управления информационной безопасности и связи Министерства.

В случае обнаружения высокой активности вредоносного программного обеспечения необходимо перейти в режим усиленного контроля с ежедневной антивирусной проверкой. Режим усиленного антивирусного контроля необходимо отменять только после определения и локализации каналов реализации угроз информационной безопасности, через которые возможно распространение данного вредоносного программного обеспечения.

Обновление антивирусных баз должно осуществляться ежедневно.

Не реже 1 раза в квартал уполномоченным администратором ГКУ «ЦИТ Кузбасса» с помощью средств антивирусной защиты готовится отчет о вирусной активности на объекта информатизации АПК и Министерства, который предоставляется для анализа начальнику отдела информационной безопасности управления информационной безопасности и связи Министерства.

### 5.1. Действия при обнаружении вредоносных программ

При обнаружении сотрудником некорректной работы АРМ или возникновении подозрения на заражение вирусными программами, необходимо обязательно сообщать уполномоченному сотруднику за

мониторинг инцидентов ГКУ «ЦИТ Кузбасса». При этом до момента осмотра рабочей станции уполномоченному сотруднику за мониторинг инцидентов ГКУ «ЦИТ Кузбасса» необходимо исключить использование АРМ и служебных флэш-накопителей.

В случае обнаружения средствами защиты от вредоносных программ зараженных файлов необходимо:

- немедленно поставить в известность о факте обнаружения вредоносного программного обеспечения уполномоченного сотрудника за мониторинг инцидентов ГКУ «ЦИТ Кузбасса», владельца зараженных файлов, а также смежные подразделения, использующие данные файлы в работе;

- немедленно, совместно с администратором сети из сотрудников ГКУ «ЦИТ Кузбасса», отключить рабочую станцию от локальной вычислительной сети, путем блокировки порта сетевого активного оборудования, при невозможности данной блокировки отключение кабеля от рабочей станции;

- уполномоченному сотруднику за мониторинг инцидентов ГКУ «ЦИТ Кузбасса» совместно с пользователем, у которого обнаружены зараженные файлы, провести анализ необходимости дальнейшего их использования;

- провести «лечение» или уничтожение зараженных файлов;

- провести внеплановую проверку всех компонентов (серверы, АРМ), которые могли быть подвержены деструктивному воздействию со стороны обнаруженного вредоносного программного обеспечения;

- принять меры по предотвращению подобного инцидента безопасности.

### 5.2. Меры безопасности для недопущения заражения вредоносным кодом

При использовании рабочих станций в сети «Интернет» необходимо соблюдать следующие меры безопасности:

- при осуществлении почтового обмена необходимо исключать открытие сообщений, полученных от неизвестных адресатов или имеющих признаки массовой рассылки (тема письма содержит информацию рекламного характера, предложения дополнительного дохода, просьбы о помощи и другие варианты, рассчитанные на проявление интереса к содержанию сообщения). Сообщения, содержащие указанные выше признаки, необходимо удалять без предварительного прочтения;

- исключить загрузку программного обеспечения, видео или фотоматериалов, а также других материалов, использование которых не требуется для исполнения служебных обязанностей;

- при появлении в окне браузера сообщений, призывающих перейти по указанной ссылке, их необходимо закрывать. При случайном нажатии на такую ссылку необходимо оперативно закрыть открывающуюся страницу или страницы.

## 6. Требования к автоматизированным рабочим местам ЛВС АПК.

В сети допускаются АРМ на операционных системах:

1. Windows версии не ниже 10, если на них установлены:
   - СЗИ от НСД Secret Net Studio версии не ниже 8.6;
   - Антивирус.
2. Astra Linux (Воронеж) с установленным антивирусом и произведенными настройками политики пароля:

Длина и алфавит:

- В файле /etc/pam.d/common-password, в строке *password requisite pam cracklib.so* установить значение *minlen=8* и добавить параметры *dcredit=-1, ucredit=-1 и lcredit=-1* (minlen – длина пароля, последние 3 параметра отвечают за алфавит (количество строчных, заглавных и цифр в пароле))

- Количество дней между сменами пароля, попыток и время блокировки в файле /etc/login.defs:

*# Количество дней между сменами пароля (дней)*
PASS_MAX_DAYS 90
*# Количество неуспешных попыток до блокировки*
LOGIN_RETRIES 6
*# Период блокировки в секундах после неудачных попыток (в секундах)*
LOGIN_TIMEOUT 1800

Опционально:

- Запрет повторного использования паролей:

В файле /etc/pam.d/common-password, в строке «...pam_unix.so» добавить параметр remember=x, где x – число последних используемых паролей

- Постоянный запрос пароля для команды sudo:

В терминале ввести команду sudo visudo, в открывшемся файле добавляем строку «Defaults timestamp_timeout=0»

- Блокирование сеанса по времени неактивности пользователя:

В терминале запустить программу sudo fly-admin-theme
Затем перейти в категорию «Блокировка»
Убедиться, что стоит галка «Блокировать экран»
Выставить в поле «После бездействия» - 15 минут

### 6.1. Требования к удаленным рабочим местам.

Подключение удаленного рабочего места к ЛВС АПК производится только по защищенным каналам. На удаленных рабочих местах должны быть установлены:

1. Программные средства криптографической защиты информации, сертифицированные ФСБ России:
   - ViPNet Client версии не ниже 4.5 в сеть № 2301;
   - Континент АП к СД Минцифры Кузбасса (ЦУС № 60490).
2. Средство защиты информации от несанкционированного доступа Secret Net Studio версии не ниже 8.6.

3. Антивирус.