УТВЕРЖДЕНА
приказом государственного автономного
учреждения Республики Коми
«Центр информационных технологий»
от 19.08.2020 № 94
(приложение № 6)

ПОЛИТИКА
информационной безопасности
«Права администратора у пользователей АРМ домена RK.local»

1. Общие положения

Настоящая политика информационной безопасности «Права администратора у пользователей АРМ домена RK.local» (далее – Политика) определяет обязательные требования при организации и поддержке функционирования АРМ под управлением ОС Windows, введенных в домен RK.local.

2. Термины и обозначения

АРМ - автоматизированное рабочее место.

ГАУ РК «ЦИТ» - государственное автономное учреждение «Центр информационных технологий».

ОС - операционная система.

Основная учетная запись пользователя - доменная персонифицированная учетная запись (для работы на АРМ, с общими дисками, почтой).

ПО - программное обеспечение.

3. Требования по управлению доступом

3.1. Основная учетная запись пользователя не должна иметь прав администратора на АРМ (не включена в группу «Администраторы» и «Опытные пользователи») за исключением случаев, указанных в пункте 3.2 настоящей Политики.

3.2. При технической невозможности работы отдельных программ без прав администратора производится попытка выдачи пользователю отдельных полномочий (например, запись в папку программы, выдача отдельных разрешений в локальной политике безопасности), если проблема не решена:

– в случае, если полномочия администратора необходимы пользователю не чаще 1 - 2 раза в месяц, ввод учетных данных по заявке, направленной в службу технической поддержки ГАУ РК «ЦИТ» осуществляет управление технического сопровождения АРМ и оргтехники ГАУ РК «ЦИТ»;

– в случае, если полномочия администратора необходимы пользователю чаще, ему выдается дополнительная персональная доменная учетная запись с префиксом а3-, которая добавляется в локальную группу администраторов на конкретных АРМ;

– в случае технической невозможности использования дополнительной учетной записи а3- права администратора оставляются.

3.3. Постоянная работа на АРМ под дополнительной учетной записью а3-, а также использование ее для целей, не соответствующих целям ее выдачи (а именно - запуска отдельных программ), запрещена.

3.4. Локальные учетные записи ОС АРМ должны быть заблокированы, за исключением случая, указанного в пункте 3.5 настоящей Политики.

3.5. При технической необходимости наличия служебной локальной учетной записи для функционирования отдельных программ такая учетная запись не блокируется. При этом служебные учетные записи для типового ПО, развернутого на многих АРМ, должны называться одинаково (при наличии технической возможности). При наличии технической возможности на такие учетные записи должен быть установлен уникальный неизвестный пользователю сложный пароль.

3.6. Дополнительным учетным записям а3- должен быть (уже при создании) запрещен доступ по сети средствами ОС Windows на другие АРМ домена rk.local, за исключением случаев, когда это необходимо конкретному владельцу учетной записи.

3.7. Все случаи невозможности удаления прав администратора (выдачи дополнительных полномочий), а также невозможности блокировки локальных учетных записей (далее — исключения) должны быть предварительно согласованы с управлением по безопасности ГАУ РК «ЦИТ». Заявка на согласование подается через Службу технической поддержки ГАУ РК «ЦИТ» или официальным письмом (служебной запиской). Выдающие полномочия (настраивающие ПО) лица обязаны придерживаться согласованных алгоритмов настройки исключений для этого ПО, а управление по безопасности ГАУ РК «ЦИТ» должно обеспечивать им оперативное предоставление доступа к указанным алгоритмам.

3.8. В случае, когда проводится настройка исключений (выдача полномочий администратора, выдача дополнительных полномочий, сохранение локальной учетной записи), лица, осуществляющие данные действия, должны уведомлять об этом управление по безопасности ГАУ РК «ЦИТ» не позднее 2 рабочих дней после изменений, за исключением следующих случаев:

– в алгоритме указано, что уведомление не нужно;

– конкретное исключение для конкретного лица (группы лиц) на конкретном АРМ (группе АРМ) прошло согласование с управлением по безопасности ГАУ РК «ЦИТ».

3.9. Учет и предоставление доступа к результатам учета выданных полномочий администратора, а также иных исключений на основании уведомлений и выданных согласований осуществляет управление по безопасности ГАУ РК «ЦИТ».

3.10. Контроль соблюдения требований настоящей Политики осуществляет управление по безопасности ГАУ РК «ЦИТ».