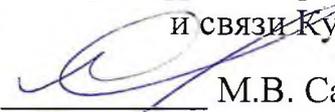


УТВЕРЖДАЮ  
министр цифрового развития  
и связи Кузбасса

  
М.В. Садиков  
«17» марта 2020 г.

**МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ**  
**органам местного самоуправления и подведомственным учреждениям**  
**по соблюдению информационной безопасности при работе с**  
**информационными системами и ресурсами**

**I. Антивирусная защита**

Автоматизированные рабочие места и информационные системы и ресурсы должны быть оборудованы сертифицированными средствами антивирусной защиты с периодичностью обновления, установленной регламентирующими документами органа местного самоуправления Кемеровской области - Кузбасса (далее – ОМСУ) и подведомственных учреждений.

В случае обнаружения вирусов и вредоносного кода незамедлительно прекратить использование автоматизированного рабочего места до момента полного удаления вирусов и вредоносного кода.

При получении электронного письма, вызывающего подозрение пользователя на его содержание и вложения, необходимо удалить его не переходя по ссылкам и не открывая вложенные файлы.

**II. Парольная защита и идентификация пользователя**

В информационных системах должны использоваться только персонифицированные учетные записи пользователей, в том числе администраторов.

Для идентификации пользователей в операционных системах, программном обеспечении и почтовых клиентах использовать «сложные» логины и пароли, состоящие из заглавных и прописных букв, цифр и специальных символов длиной не менее 8-ми символов. Не рекомендуется в качестве паролей использовать имена близких лиц, домашних животных, даты рождения и т.п., которые могут быть легко подобраны злоумышленниками.

Проводить регулярную смену паролей.

Не сохранять пароли в текстовых файлах на автоматизированном рабочем месте, либо иных электронных носителях.

Не передавать пароли, коды доступа к техническим средствам и системам, для исключения использования учетной записи другим лицом, в

случае отсутствия пользователя на рабочем месте (отпуск, временная нетрудоспособность и т.п.).

При отсутствии пользователя информационной системы на рабочем месте по причине отпуска, временной нетрудоспособности, увольнения необходимо производить блокировку учетной записи.

### **III. Удаленный доступ**

Исключить использование средств удаленного администрирования на технических средствах и системах. В случаях удаленной технической поддержки, необходимо использовать программные и технические средства, имеющие сертификат соответствия в зависимости от уровня обрабатываемой информации в информационной системе.

### **IV. Использование лицензионного программного обеспечения и сертифицированных средств защиты информации**

Использовать в работе только лицензионные версии операционных систем, прикладного программного обеспечения и средств защиты информации.

Для защиты информационных систем и ресурсов при передаче информации по каналам связи применять сертифицированные средства защиты информации и средства криптографической защиты информации, использовать действующие сертифицированные средства защиты информации.

### **V. Место расположения баз данных информационных систем и ресурсов**

Технические средства и базы данных информационных систем и ресурсов должны располагаться на территории Российской Федерации.

При расположении баз данных информационных систем и ресурсов в пределах контролируемой зоны ОМСУ (подведомственного учреждения) должен быть разработан в ОМСУ порядок доступа к защищаемым ресурсам.

При расположении баз данных информационных систем и ресурсов за пределами контролируемой зоны ОМСУ (подведомственного учреждения) должна быть обеспечена защита информации в соответствии с действующим законодательством.

### **VI. Закупочные процедуры**

При проведении закупочных процедур на оказание услуг по созданию, сопровождению информационных систем и ресурсов обязательно предъявлять требования к поставщику услуг по соблюдению

информационной безопасности в соответствии с уровнем обрабатываемой информации, наличие необходимых лицензий на оказание услуг ФСБ России и ФСТЭК России.

## **VII. Проверки и запросы контролирующих органов**

Обо всех проверках, результатах и вынесенных представлениях, проводимых контролирующими органами уведомлять Министерство цифрового развития и связи Кузбасса в срок не позднее 5-ти рабочих дней.

Начальник отдела данных  
и информационной безопасности



С.С. Фомин