



**АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ
СЕВЕРСКИЙ МУНИЦИПАЛЬНЫЙ РАЙОН
КРАСНОДАРСКОГО КРАЯ**

ПОСТАНОВЛЕНИЕ

от 18.09.2026

№ 1565

станция Северская

**Об утверждении Политики
сетевой безопасности администрации
муниципального образования Северский
муниципальный район Краснодарского края**

В целях выполнения приказа Федеральной службы по техническому и экспортному контролю России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и методического документа Федеральной службы по техническому и экспортному контролю России от 11 февраля 2014 года «Меры защиты информации в государственных информационных системах», руководствуясь статьями 31, 66 Устава муниципального образования Северский муниципальный район Краснодарского края, **п о с т а н о в л я ю:**

1. Утвердить Политику сетевой безопасности администрации муниципального образования Северский муниципальный район Краснодарского края (далее – Администрация), согласно приложению к настоящему постановлению.

2. Управлению информатизации и информационной безопасности (Сергиевская Н.Н.):

1) опубликовать настоящее постановление на официальном Интернет-портале Администрации в разделе «Информатизация»;

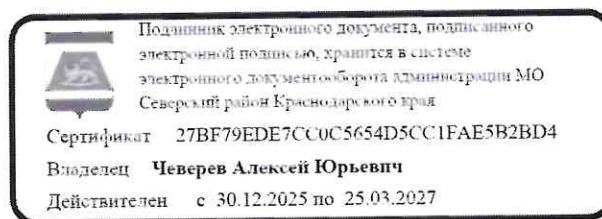
2) ознакомить под подпись с настоящим постановлением сотрудников Администрации, обрабатывающих персональные данные в Администрации.

3. Управлению по связям с общественностью (Сафина Л.К.) разместить настоящее постановление на официальном сайте Администрации в информационно-телекоммуникационной сети «Интернет» в разделе «Муниципальные правовые акты».

4. Контроль за выполнением настоящего постановления возложить на заместителя главы администрации (начальника финансового управления) Леуцкую К.В.

5. Постановление вступает в силу со дня его подписания.

Глава
муниципального
образования
Северский
муниципальный район
Краснодарского края



А.Ю. Чевереv

Приложение

УТВЕРЖДЕНА

постановлением администрации
муниципального образования
Северский муниципальный район
Краснодарского края
от 18.09.2016 № 1565

ПОЛИТИКА

сетевой безопасности администрации муниципального образования Северский муниципальный район Краснодарского края

1. Общие положения

1.1. Политика сетевой безопасности (далее – Политика) администрации муниципального образования Северский муниципальный район Краснодарского края (далее – Администрация) регулирует вопросы обеспечения сетевой безопасности локально-вычислительной сети Администрации, как части комплекса мер по обеспечению безопасности информации в Администрации.

1.2. Настоящая политика разработана в соответствии с:

приказом Федеральной службы по техническому и экспортному контролю России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

методическим документом Федеральной службы по техническому и экспортному контролю России от 11 февраля 2014 года «Меры защиты информации в государственных информационных системах».

1.3. Настоящая политика определяет требования сетевой безопасности, технологии и механизмы обеспечения безопасности сетевой инфраструктуры, а также принципы управления сетевой безопасностью.

2. Общие требования по обеспечению сетевой безопасности

2.1. Локально-вычислительная сеть (далее – ЛВС) является составной частью информационных систем Администрации, обеспечивающая его функционирование.

2.2. ЛВС подлежит защите от воздействий (как внутренних, так и внешних), которые могут привести к:

нарушению непрерывности функционирования информационных процессов;
нарушению конфиденциальности защищаемой информации;

целостности защищаемой информации и правил разграничения доступа к информационным ресурсам;

нарушению доступности защищаемой информации и сервисов информационных систем.

2.3. Средства, используемые в составе ЛВС для обеспечения необходимого уровня безопасности информации, должны обеспечивать:

доступность, целостность и конфиденциальность информационных ресурсов;
защиту каналов передачи данных и управления, их доступность;
защиту сетевого трафика от перехвата;
защищённый удалённый доступ в информационную систему;
простоту используемых технологий защиты информации и их эксплуатации;
прозрачность используемых средств и механизмов защиты для пользователей.

2.4. С целью обеспечения выполнения указанных требований в составе ЛВС должны применяться следующие технологии сетевой безопасности:

межсетевое экранирование;
обнаружение и предотвращение вторжений;
криптографическая защита информации.

2.5. С целью минимизации возможных точек доступа к сетям связи общего пользования (в том числе сети Интернет) использование технологий беспроводной передачи данных на территории Администрации запрещено:

2.6. Для регистрации сетевых узлов (автоматизированных рабочих мест, серверов и активного сетевого оборудования) в сети используются физические адреса (MAC-адреса) и IP-адреса. Для каждого сетевого узла задается IP-адрес маршрутизатора (адрес шлюза по умолчанию), через который он может связываться с компьютерами в других локальных сетях и сети Интернет. Присваивание этих параметров производится автоматически функционалом DHCP-сервера.

2.7. Доступ к средствам (устройствам) сетевой безопасности предоставляется работникам, наделённым соответствующими полномочиями.

3. Межсетевое экранирование

3.1. Средствами межсетевого экранирования должен реализовываться следующий функционал:

идентификация сетевых устройств по IP-адресам и (или) MAC-адресам;
аутентификация сетевых устройств, по одному из протоколов: Remote Authentication Dial-In User Service (RADIUS); Terminal Access Controller Access Control Systems (TACACS); Lightweight Directory Access Protocol (LDAP); Kerberos;

фильтрация информационных потоков по протоколам (например, TCP, UDP, IP), портам и адресам назначения, а также определение маршрутов передачи информации (требования к фильтрации устанавливаются в соответствии с заявками пользователей на доступ к информационным ресурсам (системам) в порядке, установленном политикой использования информационных ресурсов (систем) Администрации, а также потребностями администраторов, обусловленными необходимостью администрирования информационных ресурсов (систем) и средств обработки информации);

завершение сетевых соединений (например, открепление пары порт/адрес (TCP/IP)) по их завершении и (или) по истечении заданного Администратором временного интервала неактивности сетевого соединения).

3.2. С целью выполнения указанных требований могут применяться:

программные и программно-аппаратные средства межсетевого экранирования уровня периметра сети – на внешней границе информационной системы;

программные средства межсетевого экранирования уровня хоста – на внутренних узлах сегментов информационных систем (автоматизированных рабочих местах (далее – АРМ) и серверах информационных систем);

иное активное сетевое оборудование (коммутаторы, маршрутизаторы и прочее), реализующие необходимый функционал.

3.3. Используемые средства межсетевого экранирования должны иметь соответствующие действующие сертификаты соответствия, выданные Федеральной службой по техническому и экспортному контролю России.

3.4. Средства межсетевого экранирования могут интегрироваться со средствами антивирусной защиты информации с целью обеспечения антивирусной защиты информации периметра ЛВС.

4. Обнаружение и предотвращение вторжений

4.1. Система обнаружения и предотвращения вторжений (далее - COB) позволяет распознавать вредоносную активность внутри сети. COB должна иметь в своем составе следующие компоненты:

регистрацию событий безопасности (датчики);

анализ событий безопасности и распознавания компьютерных атак (анализаторы);

базу решающих правил (базу сигнатур), содержащую информацию о характерных признаках компьютерных атак.

4.2. Средствами обнаружения вторжений должны реализовываться следующие функции:

отслеживание атак в режиме реального времени;

использование сигнатурных и эвристических методов для анализа сетевого трафика;

создание профилей (наборы сигнатур, релевантных для защиты определенных сервисов);

задавать правила, определяющие действия для выбранного типа трафика (IP, ICMP, TCP, UDP)

протоколирование нештатных ситуаций, а также попыток проведения вторжений и предотвращение угроз в журнале регистраций событий, а также предоставление отчетов;

защита от атак на сетевые протоколы на различных уровнях модели OSI;

возможность анализа собранных данных COB о сетевом трафике в режиме, близком к реальному масштабу времени;

централизованное управление (администрирование) компонентами средств, установленными в различных сегментах информационных систем;

обновление (из доверенных источников) базы решающих правил;

контроль целостности обновлений базы решающих правил;

уведомление о необходимости обновления и непосредственном обновлении базы решающих правил.

4.3. Средства предотвращения вторжений должны иметь в своем составе следующие компоненты:

- блокирование атак в режиме реального времени;
- обрыв соединения и оповещение администратора безопасности;
- протоколирование нештатных ситуаций в журнале регистраций событий и предоставление отчетов.

4.4. С целью выполнения указанных требований могут применяться:

- программные и программно-аппаратные средства обнаружения вторжений уровня периметра сети – на внешней границе информационной системы;
- программные средства обнаружения вторжений уровня хоста – на внутренних узлах сегментов информационных систем.

4.5. Используемые средства обнаружения вторжений должны иметь соответствующие действующие сертификаты соответствия, выданные Федеральной службой по техническому и экспортному контролю России.

5. Криптографическая защита информации

5.1. Средства криптографической защиты информации, передаваемой по каналам связи, должны применяться в случае, если:

- передача защищаемой информации, в том числе персональных данных, осуществляется по каналам связи, не защищенным от перехвата нарушителем передаваемой по ним информации или от несанкционированных воздействий на эту информацию (например, при передаче защищаемой информации по информационно-телекоммуникационным сетям общего пользования; удаленном доступе к информационным ресурсам (системам) и средствам обработки информации, в том числе для администрирования);

- хранение защищаемой информации осуществляется на носителях информации, несанкционированный доступ к которым со стороны нарушителя не может быть исключен с помощью некриптографических методов и способов.

5.2. Используемые средства криптографической защиты информации, передаваемой по каналам связи, должны иметь соответствующие действующие сертификаты соответствия, выданные Федеральная служба безопасности России.

5.3. С целью выполнения указанных требований могут применяться:

- программно-аппаратные средства криптографической защиты информации, передаваемой по каналам связи (криптографические шлюзы) – на внешней границе информационной системы;

- программные средства и (или) программно-аппаратные средств криптографической защиты информации (в том числе средства электронной подписи) – на внутренних узлах сегментов информационных систем (автоматизированных рабочих местах (далее – АРМ) и серверах информационных систем).

5.4. Эксплуатация средств криптографической защиты информации, должна осуществляться в соответствии с Политикой использования средств криптографической защиты информации Администрации.

6. Ответственность за исполнение положений настоящей политики

Основные функции администрирования ЛВС Администрации выполняют уполномоченные работники управления информатизации и информационной безопасности Администрации.

6.1. Администрирование ЛВС включает в себя реализацию следующих основных функций:

- планирование, создание и сопровождение кабельной системы ЛВС Администрации;

- организацию и сопровождение системы локальных сетей (VLAN), коммутаторов уровня доступа, магистральных коммутаторов и маршрутизаторов ЛВС Администрации;

- составление и поддержку адресного плана Администрации;

- организацию и сопровождение внешних каналов связи, внешней маршрутизации ЛВС Администрации с сетью Интернет;

- взаимодействие с операторами связи;

- организацию и поддержку доменной службы имён;

- организацию и поддержку домена службы каталогов (MS Active Directory) Администрации, регистрацию объектов доменов и сопровождение их учётных записей;

- организацию и поддержку сетевых информационных ресурсов Администрации в форме файловых серверов, серверов баз данных;

- разработку и реализацию мероприятий по защите ресурсов ЛВС от несанкционированного доступа;

- обеспечение резервного копирования и восстановления общих информационных ресурсов Администрации и информационных ресурсов подразделений Администрации (по их запросам).

6.2. Администратор информационных систем несет ответственность за:

- знание структуры локально-вычислительной сети;

- ведение учёта назначенных сетевым узлам IP-адресов;

- настройку параметров активного сетевого оборудования в соответствии с положениями настоящей политики;

- настройку параметров фильтрации и маршрутизации информационных потоков в соответствии с установленными правилами;

- обеспечение резервирования критически важного активного сетевого оборудования и принятие мер по восстановлению работоспособности данного оборудования;

- незамедлительное информирование о произошедших инцидентах, связанных с нарушением информационной безопасности (или при возникновении подозрения о возможности появления инцидента, связанного с нарушением информационной безопасности) администратора информационной безопасности.

6.3. Пользователь несёт личную ответственность за весь информационный обмен между его компьютером и другими компьютерами в ЛВС и за её пределами. В случае если с данного компьютера производился несанкционированный доступ к информации на других компьютерах и в случаях других серьёзных нарушений правил пользования сетью, по решению Администратора информационной

безопасности, АРМ пользователя отключается от сети, учётная запись пользователя блокируется.

6.4. Лица, виновные в нарушении положений настоящей политики, могут быть привлечены к дисциплинарной, материальной, гражданско-правовой и административной ответственности.

Начальник управления информатизации
и информационной безопасности



Н.Н.Сергиевская