АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ СЕВЕРСКИЙ МУНИЦИПАЛЬНЫЙ РАЙОН КРАСНОДАРСКОГО КРАЯ

П О С Т А Н О В Л Е Н И Е

от 23.01.2026 № 136

станица Северская

Об утверждении Политики управления событиями безопасности администрации муниципального образования Северский муниципальный район Краснодарского края

Во исполнение требований статьи 18.1. Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», руководствуясь постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», 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», 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 управления событиями 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 (Поляшенко Е.А.) 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

Подлинник электронного документа, подписанного электронной подписью, хранится в системе электронного документооборота администрации МО Северский район Краснодарского края
Сертификат 27BF79EDE7CC0C5654D5CC1FAE5B2BD4
Владелец **Чеверев Алексей Юрьевич**
Действителен с 30.12.2025 по 25.03.2027

А.Ю. Чеверев

Приложение

УТВЕРЖДЕНА
постановлением администрации
муниципального образования
Северский муниципальный район
Краснодарского края
от 23.01.2026 № 136

ПОЛИТИКА
управления событиями безопасности информации администрации муниципального образования Северский муниципальный район Краснодарского края

1. Общие положения

1.1. Политика управления событиями безопасности информации администрации муниципального образования Северский муниципальный район Краснодарского края (далее – Политика) устанавливает единый системный подход к процессу управления событиями (их регистрация, учёт, сбор, хранение и обработка) безопасности информации в администрации муниципального образования Северский муниципальный район Краснодарского края (далее – Администрация).

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».

1.3. Управление событиями безопасности информации осуществляется с целью своевременного выявления фактов, оказывающих негативное воздействие на информационные системы Администрации (выявления инцидентов информационной безопасности).

1.4. Под событием безопасности информации понимается любое проявление состояния информационной системы и системы её защиты, указывающие на возможность нарушения:

конфиденциальности, целостности или доступности информации, обрабатываемой в информационной системе;

доступности компонентов информационной системы (АРМ, серверов, активного сетевого оборудования);

штатного функционирования компонентов информационных систем и средств защиты информации;

нарушения процедур, установленных организационно-распорядительными документами по защите информации.

1.5. Под инцидентом информационной безопасности понимается одно или серия событий безопасности информации, связанных с нарушением, установленных в Администрации политик безопасности информации.

2. Регистрация, учёт, сбор и хранение событий безопасности информации

2.1. Перечень событий безопасности информации, подлежащих регистрации в информационных системах Администрации, приведён в приложении 1 к настоящей Политике.

2.2. Перечень событий безопасности, подлежащих регистрации, должен пересматриваться, в том числе по результатам контроля (мониторинга) обеспечения уровня защищённости информации, содержащейся в информационных системах, но не реже чем 1 раз в год.

2.3. При регистрации событий безопасности информации регистрации подлежат следующие характеристики событий безопасности информации:

тип события безопасности информации;

дата и время события безопасности информации;

идентификационная информация источника события безопасности информации;

результат события безопасности информации (успешно или неуспешно);

субъект доступа (пользователь и (или) процесс), связанный с данным событием безопасности информации.

2.4. Источниками событий безопасности информации являются:

средства регистрации событий системного и прикладного программного обеспечения;

средства регистрации событий активного сетевого оборудования;

средства системы обеспечения информационной безопасности Администрации;

средства системы пожарно-охранной сигнализации и системы контроля и управления доступом;

работники Администрации;

работники других организаций, имеющих доступ к информационным системам Администрации.

2.5. Должен обеспечиваться непрерывный сбор событий безопасности информации, генерируемых компонентами информационных систем (АРМ, серверами, активным сетевым оборудованием) и средствами защиты информации.

2.6. Регистрация, учёт и хранение событий безопасности информации должны обеспечиваться ответственными лицами, срок хранения событий безопасности информации должен составлять не менее 12 месяцев.

2.7. Сведения о событиях безопасности информации подлежат защите от неправомерного доступа, уничтожения или модифицирования. Доступ к данным сведениям должен быть ограничен, кроме уполномоченных на это лиц.

3. Мониторинг и анализ событий безопасности информации

3.1. Мониторинг и анализ событий безопасности информации осуществляется с целью выявления инцидентов информационной безопасности.

3.2. Мониторинг событий информационной безопасности может осуществляться как с использованием средств автоматизации (средств, относящихся к средствам сбора и корреляции событий безопасности информации – SIEM), так и без использования таковых.

3.3. Мониторинг и анализ событий безопасности информации осуществляется:

в части средств системы обеспечения информационной безопасности Администрации - администратором информационной безопасности;

в части средств обеспечения функционирования информационных систем (системного и прикладного программного обеспечения, активного сетевого оборудования) – администратором информационных систем. В результате анализа событий безопасности информации он должен информировать администратора информационной безопасности о событиях, имеющих признаки инцидентов, а также непосредственно об инцидентах информационной безопасности.

3.4. Периодичность мониторинга и анализа событий безопасности информации зависит от степени критичности информационного ресурса (системы) или средства обработки информации и составляет:

для информационных ресурсов (систем) или средств обработки информации, имеющих высокую критичность – ежедневно;

для информационных ресурсов (систем) или средств обработки информации, имеющих среднюю критичность – не реже одного раза в неделю;

для информационных ресурсов (систем) или средств обработки информации, имеющих низкую критичность – не реже одного раза в месяц.

3.5. К инцидентам информационной безопасности относятся следующие категории негативных событий (группы событий) безопасности информации:

разглашение защищаемой информации работниками, имеющими право доступа к ней (передача защищаемой информации третьим лицам, не имеющим права доступа к ней; передача защищаемой информации по открытым каналам связи; обработка защищаемой информации на незащищённых технических средствах; публикация защищаемой информации в СМИ; копирование защищаемой информации на неучтённые съёмные носители информации; утрата съёмных и (или) бумажных носителей информации или передача их лицам, не имеющим права доступа к ним);

неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации (несанкционированное изменение, копирование защищаемой информации);

ошибки обслуживающего персонала при эксплуатации информационных систем;

несанкционированный доступ к защищаемой информации лицами, не имеющими права доступа к ней (подключение технических средств к информационным системам; использование закладочных устройств, маскировка под зарегистрированного пользователя; использование недекларированных возможностей программного обеспечения; использование программных закладок и применение программных вирусов; хищение носителей защищаемой информации; нарушение функционирования технических средств обработки защищаемой информации);

дефекты, сбои, отказы, программного обеспечения и аварии технических средств и систем обеспечения их отказоустойчивого функционирования;

природные явления, стихийные бедствия (пожары, наводнения, землетрясения, грозовые разряды).

4. Порядок управления инцидентами информационной безопасности

4.1. Общий порядок управления инцидентами информационной безопасности включает:

обнаружение и информирование об инциденте информационной безопасности;

регистрация инцидента информационной безопасности;

локализация и устранение последствий инцидента информационной безопасности;

расследование инцидента информационной безопасности и реализация действий, предупреждающих его повторное возникновение (корректирующие меры).

5. Обнаружение и информирование об инциденте информационной безопасности

5.1. При обнаружении инцидента информационной безопасности (или события безопасности информации, имеющего признаки инцидента) должен быть незамедлительно проинформирован администратор информационной безопасности (средствами служебной электронной почты и посредством телефонной связи).

5.2. В случае невозможности информирования администратора информационной безопасности об инциденте информационной безопасности (посредством телефонной связи) о случившемся инциденте информационной безопасности должен быть уведомлёно (посредством телефонной связи) лицо, замещающее его.

5.3. Сообщение о случившемся инциденте информационной безопасности должно содержать следующую информацию:

Ф.И.О., должность работника, выявившего инцидент информационной безопасности;

время обнаружения инцидента информационной безопасности;

описание инцидента информационной безопасности.

6. Регистрация инцидента информационной безопасности

6.1. Регистрация инцидентов информационной безопасности осуществляется администратором информационной безопасности в журнале учёта инцидентов информационной безопасности (форма журнала представлена в приложении 2 к настоящей Политике).

6.2. На каждый инцидент информационной безопасности администратором информационной безопасности формируется карточка инцидента информационной безопасности (форма карточки приведена в приложении 3 к настоящей Политике).

6.3. До момента полного заполнения карточки инцидента информационной безопасности и, соответственно, закрытия инцидента она своевременно заполняется и ведётся в электронном виде, после чего распечатывается и хранится на бумажном носителе.

6.4. На этапе регистрации инцидента подлежат заполнению следующие разделы карточки:

общие сведения об инциденте информационной безопасности;

содержание инцидента информационной безопасности;

воздействие инцидента на информационные ресурсы (системы) или средства обработки информации.

6.5. Критичность инцидента зависит от критичности информационных ресурсов (систем) или средств обработки информации, затронутых инцидентом, а также области распространения (действия) инцидента, и определяется по следующей таблице:

Область распространения и действия инцидента ИБ	Критичность информационного ресурса (системы) или средства обработки информации		
	высокая	средняя	низкая
Выходящий за пределы Администрации	Высокая	Высокая	Средняя
Администрация в целом	Высокая	Высокая	Средняя
Пределы отдельного отдела	Высокая	Средняя	Низкая
Пределы одного информационного ресурса (системы)	Средняя	Низкая	Низкая

7. Локализация и устранение последствий инцидента информационной безопасности

7.1. Срок реагирования на инцидент информационной безопасности напрямую зависит от степени критичности инцидента и составляет:

для инцидентов, имеющих высокую критичность – незамедлительное реагирование;

для инцидентов, имеющих среднюю критичность – срок реагирования не более одного рабочего дня;

для инцидентов, имеющих низкую критичность – срок реагирования не более пяти рабочих дней.

7.2. Под реагированием на инцидент информационной безопасности понимается назначение ответственных лиц за локализацию и устранение последствий инцидента информационной безопасности. Ответственные лица назначаются администратором информационной безопасности по Администрации, или лицом, замещающим его.

7.3. В первую очередь осуществляется локализация инцидента информационной безопасности – предпринимаются все необходимые и доступные меры по сдерживанию/пресечению распространения негативного воздействия инцидента на информационные системы, а позже (или одновременно) проводятся работы по устранению последствий инцидента информационной безопасности. Могут назначаться различные ответственные за данные процессы лица.

7.4. Ответственные лица сообщают планируемый срок локализации и устранения последствий инцидента информационной безопасности, а также отчитываются администратору информационной безопасности о степени выполнения работ.

7.5. Процесс локализации и устранения последствий инцидента информационной безопасности своевременно отражается в Карточке инцидента информационной безопасности.

8. Расследование инцидента информационной безопасности и реализация корректирующих мер

8.1. Процедура расследования инцидента информационной безопасности предназначена для выявления причин (условий и факторов), вызвавших инцидент информационной безопасности, и/или негативную тенденцию развития связанной с этим инцидентом ситуации, а также анализа и оценки адекватности и эффективности действий, предпринятых, по управлению инцидентом информационной безопасности.

8.2. Для проведения процедуры расследования инцидента информационной безопасности привлекается комиссия Администрации, утвержденная главой муниципального образования Северский муниципальный район Краснодарского края.

8.3. В процессе расследования инцидента информационной безопасности на основании анализируемых данных должен быть установлен нарушитель информационной безопасности (для внутренних категорий нарушителей – должно быть выявлено конкретное физическое лицо), чьи действия (умышленные или неумышленные) привели к возникновению инцидента информационной безопасности.

8.4. По итогам расследования инцидента информационной безопасности комиссией Администрации разрабатывается комплекс мер, направленных на:

недопущение (минимизацию вероятности) возможности повторения инцидента в будущем – разработка корректирующих мер;

выявление нарушителей информационной безопасности (если его не удалось установить в процессе расследования инцидента).

8.5. При разработке корректирующих мер должны учитываться их возможные воздействия на процесс функционирования информационных систем (в том числе должна быть оценена возможная степень негативного влияния на работу пользователей информационных систем), а также стоимость (экономическая обоснованность) реализации данных мер.

8.6. Результат разработки корректирующих мер (отчёт) передаётся главе муниципального образования Северский муниципальный район Краснодарского края или лицу, замещающему его, для принятия дальнейших решений по реализации данных мер.

8.7. Процесс расследования инцидента информационной безопасности и реализация корректирующих мер своевременно отражается в Карточке инцидента информационной безопасности.

8.8. После выполнения всех действий по регистрации, локализации, устранению последствий, расследования инцидента информационной безопасности и принятия корректирующих мер инцидент должен быть закрыт (разрешён), о чем делается запись в журнале учёта инцидентов информационной безопасности и карточке инцидента информационной безопасности.

9. Ответственность за исполнение положений настоящей Политики

9.1. Все работники Администрации обязаны информировать администратора информационной безопасности об инцидентах информационной безопасности, событиях безопасности информации (имеющих признаки инцидента) и, при необходимости, принимать участие в расследовании инцидента информационной безопасности вместе с комиссией Администрации.

9.2. Администратор информационной безопасности несёт ответственность за:

пересмотр (не реже одного раза в год) Перечня событий безопасности информации информационных систем Администрации;

принятие решения по реализации корректирующих мер (в соответствии с предоставленными отчётами);

регистрацию инцидентов информационной безопасности в Журнале учёта инцидентов информационной безопасности;

согласование перечня лиц, ответственных за локализацию и устранение последствий инцидентов информационной безопасности;

ведение карточек инцидентов информационной безопасности;

определение лиц, ответственных за локализацию и устранение последствий инцидентов информационной безопасности;

контроль сроков локализации и устранение последствий инцидентов информационной безопасности;

анализ проведённой работы по локализации и устранению ответственными лицами последствий инцидентов информационной безопасности;

участие в составе комиссии Администрации в рамках расследования инцидентов информационной безопасности;

обеспечение непрерывности регистрации, учёта, сбора и хранения (сроком не менее 12 месяцев) событий безопасности информации в соответствии с требованиями настоящей Политики (в зоне своей ответственности);

реализацию комплекса мер по защите сведений о событиях безопасности информации от неправомерного доступа, уничтожения или модифицирования (в зоне своей ответственности);

своевременный мониторинг и анализ событий безопасности информации с целью выявления информационной безопасности (в зоне своей ответственности).

9.3. Администратор информационных систем несет ответственность за:

обеспечение непрерывности регистрации, учёта, сбора и хранения (сроком не менее 12 месяцев) событий безопасности информации в соответствии с требованиями настоящей Политики (в зоне своей ответственности);

реализацию комплекса мер по защите сведений о событиях безопасности информации от неправомерного доступа, уничтожения или модифицирования (в зоне своей ответственности);

своевременный мониторинг и анализ событий безопасности информации с целью выявления информационной безопасности (в зоне своей ответственности);

участие в составе комиссии Администрации в рамках расследования инцидентов информационной безопасности (при необходимости, определяемой администратором информационной безопасности);

9.4. 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

Приложение 1
к политике управления событиями
безопасности информации
администрации муниципального
образования Северский
муниципальный район
Краснодарского края

ФОРМА

ПЕРЕЧЕНЬ
типов событий безопасности информации, подлежащих регистрации в администрации муниципального образования Северский муниципальный район

1. Физический доступ к информационным ресурсам (системам), средствам обработки информации и средствам обеспечения их отказоустойчивости:

физический доступ работников и иных лиц в защищаемые помещения;

физический доступ третьих лиц в серверные помещения (проводящих работы по обслуживанию, ремонту, сопровождению и настройке серверного, активного сетевого и прочего оборудования, располагающегося в серверных помещениях);

изменение (в том числе замена, добавление или изъятие) состава средств обработки информации[1)];

замена и (или) модификация аппаратной конфигурации средств обработки информации;

осуществление действий со съёмными носителями информации[1)];

осуществление действий с дополнительными идентификаторами, используемыми для доступа к информационным ресурсам (системам);

вынос за пределы организации средств вычислительной техники;

передача средств вычислительной техники между подразделениями Администрации;

передача средств вычислительной техники и их компонентов в сторонние организации;

2. Использование информационных ресурсов (систем) и средств обработки защищаемой информации: предоставление аутентификационной и ключевой информации на доступ к информационным ресурсам (системам) и средствам обработки защищаемой информации (в том числе по использованию служебной электронной почты и сети Интернет);

[1)] Регистрация, учёт, выдача, использование (подключение), утилизация (уничтожение).

изменение прав доступа к информационным ресурсам (системам) и средствам обработки защищаемой информации;

изменение и (или) компрометация аутентификационной или ключевой информации;

аутентификация и идентификация пользователей информационных ресурсов (систем) и средств обработки защищаемой информации (в том числе неуспешная);

удалённый доступ к информационным ресурсам (системам) и средствам обработки защищаемой информации (с указанием протокола доступа);

действия, совершаемые с защищаемой информацией;

завершение сеансов работы пользователей информационных ресурсов (систем) и средств обработки защищаемой информации;

вывод на печать защищаемой информации;

отключение/перезагрузка или приостановление работы средств обработки защищаемой информации;

изменение параметров настроек средств обработки защищаемой информации;

изменение состава и версий программного обеспечения (в том числе баз сигнатур средств антивирусной защиты информации и средств обнаружения вторжений);

сбои и отказы работоспособности информационных ресурсов (систем) и средств обработки защищаемой информации;

достижение пороговых значений основных показателей функционирования технических средств (степени загрузки: процессорных мощностей, дискового пространства, оперативной памяти, каналов связи и прочее);

восстановление работоспособности информационных ресурсов (систем) и средств обработки защищаемой информации;

архивирование, резервирование и восстановление защищаемой информации;

выполнение операций, связанных с эксплуатацией и администрированием информационных ресурсов (систем) и средств обработки защищаемой информации.

Настоящий перечень подлежит обязательному ежегодному пересмотру!

Начальник управления информатизации
и информационной безопасности Н.Н.Сергиевская

Приложение 2
к политике управления событиями
безопасности информации
администрации муниципального
образования Северский
муниципальный район
Краснодарского края

ФОРМА

ЖУРНАЛ УЧЁТА
инцидентов информационной безопасности

№ п/п	№ карточки инциден-та ИБ	Дата и время возникнове-ния инцидента ИБ	Дата и время регистрации инцидента ИБ	Ф.И.О. и должность работника, обнаружившего инцидент ИБ	Критичность инцидента ИБ	Затронутые информационные ресурсы (системы) и средств обработки информации	Ф.И.О. и должность лица, ответственного за устранение инцидента	Дата и время устране-ния инциден-та ИБ
1	2	3	4	5	6	7	8	9
1								
2								

Начальник управления информатизации
и информационной безопасности

Н.Н.Сергиевская

Приложение 3
к политике использования средств
криптографической защиты
администрации муниципального
образования Северский
муниципальный район
Краснодарского края

ФОРМА

КАРТОЧКА
инцидента информационной безопасности № ____

№ п/п	Наименование характеристики инцидента ИБ:	Описание
1	2	3
1. Общие сведения об инциденте ИБ		
1.1	Номер записи согласно Журналу учёта инцидентов ИБ	
1.2	Дата и время возникновения инцидента ИБ	
1.3	Дата и время регистрации инцидента ИБ	
1.4	Источник информации об инциденте ИБ (работник или техническое средство)	
1.5	Ф.И.О. и должность работника, обнаружившего инцидент ИБ	
1.6	Контактные данные работника, обнаружившего инцидент	
1.7	Наименование технического средства, при использовании которого обнаружен инцидент ИБ	
1.8	Описание инцидента ИБ	

№ п/п	Наименование характеристики инцидента ИБ:	Описание
1	2	3
2. Содержание инцидента ИБ		
2.1	Сведения о нарушении установленных организационно-распорядительными документами требований по обеспечению ИБ («нет» «наименование документа, регламентирующего требование; № пункта документа»)	
2.2	Данные о нарушителе требований по обеспечению ИБ	«нет» «Фамилия И.О., должность нарушителя»
2.3	Категория инцидента ИБ	«случайный» «преднамеренный»
2.4	Тип инцидента ИБ	«свершившийся» «попытка осуществления инцидента ИБ» «подозрение на инцидент ИБ»
3. Воздействие инцидента на информационные ресурсы (системы) и средства обработки защищаемой информации		
3.1	Типы объектов (ресурсов), затронутых инцидентом	«файлы/базы данных, содержащие защищаемую информацию» «автоматизированные рабочие места» «серверы информационных систем» «активное сетевое оборудование» «средства защиты информации» «носители информации (в том числе бумажные носители)» «системное/прикладное программное обеспечение» «линии и сети передачи данных» «помещения, здания, сооружения, инженерные сети и коммуникации»
3.2	Нарушенные свойства безопасности:	«конфиденциальность» «целостность» «доступность»

№ п/п	Наименование характеристики инцидента ИБ:	Описание
1	2	3
3.3	Область распространения и действия инцидента ИБ	«пределы одного информационного ресурса (системы)» «пределы отдельного отдела» «Администрация в целом» «выходящий за пределы Администрации»
3.4	Критичность инцидента ИБ	«высокая» «средняя» «низкая»
4. Локализация и устранение последствий инцидента ИБ		
4.1	Информирование об инциденте ИБ	«дата и время информирования и кому сообщено»
4.2	Назначение ответственного лица за локализацию инцидента ИБ	«дата и время, Ф.И.О., должность ответственного лица»
4.3	Планируемый срок локализации инцидента ИБ	«планируемый срок, определённый ответственным лицом»
4.4	Сведения о локализации инцидента ИБ	«дата и время, описание предпринятых действий»
4.5	Назначение ответственного лица за устранение последствий инцидента ИБ	«дата и время, Ф.И.О., должность ответственных лиц»
4.6	Планируемый срок устранения последствий инцидента ИБ	«планируемый срок, определённый ответственным лицом»
4.7	Сведения об устранении последствий инцидента ИБ	«дата и время, описание предпринятых действий»
5. Расследование инцидента ИБ и реализация корректирующих мер		
5.1	Сведения о комиссии по расследованию инцидента ИБ	«комиссия Администрация, состав ее членов»
5.2	Сведения о причинах возникновения инцидента ИБ	«описание»
5.3	Сведения о лицах, понесших ответственность за инцидент ИБ	«Ф.И.О., должность лица, вид ответственности»
5.4	Степень вероятности повторного возникновения инцидента ИБ	«нет» «минимальная» «средняя»

№ п/п	Наименование характеристики инцидента ИБ:	Описание
1	2	3
		«высокая»
5.5	Перечень корректирующих мер, направленных на предупреждение повторного возникновения инцидента	«описание»

Дата, время закрытия инцидента ИБ: _____

Ф.И.О., подпись администратора ИБ _____

Начальник управления информатизации
и информационной безопасности Н.Н.Сергиевская