БЕЛГОРОДСКАЯ ОБЛАСТЬ

АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО РАЙОНА «КРАСНЕНСКИЙ РАЙОН»

РАСПОРЯЖЕНИЕ

«20» декабря 2024 г. с. Красное № 874-р

Об обеспечении информационной безопасности в администрации Красненского района

Во исполнении пункта 1.8 Протокола заседания комиссии по информационной безопасности при Губернаторе Белгородской области от 26 декабря 2023 г. № 2023/3:

1. В целях повышения устойчивости и безопасности функционирования информационных ресурсов администрации Красненского района утвердить политику информационной безопасности администрации Красненского района (приложение № 1).

2. Контроль за исполнением распоряжения возложить на первого заместителя главы администрации муниципального района - руководителя аппарата главы администрации муниципального района Боеву Г.И.

Глава администрации Красненского района **А.Ф. Полторабатько**

Приложение № 1

Утверждено
распоряжением администрации
Красненского района
от «20» декабря 2024 г.
№ 324

Политика
информационной безопасности администрации Красненского района

1. Общие положения

1.1. Политика информационной безопасности администрации Красненского района (далее - Политика информационной безопасности) разработана в соответствии с требованиями:

- Конституции Российской Федерации;
- Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Указа Президента Российской Федерации от 5 декабря 2016 года № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;
- Указа Президента Российской Федерации от 2 июля 2021 года № 400 «О Стратегии национальной безопасности Российской Федерации»;
- требованиями нормативных актов федерального органа исполнительной власти, уполномоченного в области безопасности, федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации.

1.2. Политика информационной безопасности является документом, доступным любым сотрудникам администрации Красненского района и подведомственных учреждений, иных организаций и учреждений, являющихся пользователями информационных систем администрации Красненского района и представляет собой официально принятую администрацией Красненского района систему взглядов на проблему обеспечения информационной безопасности. Политика информационной безопасности устанавливает принципы построения системы управления информационной безопасностью на основе систематизированного изложения целей, процессов и процедур информационной безопасности.

1.3. Соблюдение требований информационной безопасности позволяет обеспечить соответствие правовым, регулятивным требованиям при обработке различного типа информации и обеспечить защиту информации, обрабатываемой в информационных системах администрации Красненского района, в контексте изменения законодательства Российской Федерации, а

также развития информационных технологий в рамках проводимой цифровой трансформации, обработки больших массивов данных.

1.4. Требования информационной безопасности соответствуют целям деятельности администрации Красненского района и предназначены для снижения рисков, связанных с информационной безопасностью.

1.5. Политика информационной безопасности в области обеспечения информационной безопасности и защиты информации наряду с прочим включает выполнение в практической деятельности требований:

- действующего законодательства Российской Федерации в области безопасности, безопасности информационных технологий и защиты информации, безопасности персональных данных, служебной тайны, государственной тайны и других правовых актов;

- нормативных актов федеральных органов исполнительной власти, уполномоченных в области обеспечения физической безопасности и технической защиты информации, противодействия техническим разведкам и обеспечения информационной безопасности и приватности.

1.6. Требования обеспечения информационной безопасности соблюдаются сотрудниками администрации Красненского района и подведомственных учреждениями, а также другими сторонами как это определено положениями внутренних правовых актов администрации Красненского района, а также требованиями соглашений, одной из сторон которых является администрация Красненского района.

1.7. Политика информационной безопасности распространяется на все бизнес- процессы, протекающие в администрации Красненского района, обязательна для применения всеми пользователями информационных ресурсов администрации Красненского района.

1.8. Положения Политики информационной безопасности учитываются при разработке локальных политик информационной безопасности подведомственных учреждений.

2. Список терминов и определений

2.1. Бизнес-процесс - последовательность технологически связанных операций по выполнению возложенных полномочий на администрацию Красненского района и подведомственные учреждения.

2.2. Головное подразделение - исполнительный орган Красненского района, на который администрацией Красненского района возложены функции по координации и реализации единой политики в области информационной безопасности в администрации Красненского района. Для выполнения функции головного подразделения могут привлекаться учреждения (организации), обладающие необходимыми для осуществления такой деятельности лицензиями Федеральной службы по техническому и экспортному контролю и Федеральной службы безопасности Российской Федерации.

2.3. Информационная безопасность (ИБ) - в Политике

информационной безопасности состояние защищенности технологических процессов и бизнес- процессов, объединяющих в своем составе сотрудников, технические и программные средства обработки информации, информацию в условиях угроз в информационной сфере.

2.4. Информационная система - совокупность программно-аппаратных комплексов, применяемых для обеспечения бизнес-процессов администрации Красненского района.

2.5. Инцидент информационной безопасности - это появление одного или нескольких нежелательных рисковых событий информационной безопасности, с которыми связана значительная вероятность нарушения конфиденциальности, целостности или доступности информационных активов и инфраструктуры, и создания угрозы информационной безопасности.

2.6. ИТ-подразделение - отдел (выделенный специалист), ответственный за развитие, эксплуатацию и сопровождение информационных систем, информационных инфраструктур администрации Красненского района.

2.7. Куратор - заместитель руководителя органа власти, подведомственного учреждения, иной организации и учреждения, являющегося пользователем информационных систем администрации Красненского района, курирующий вопросы информационной безопасности. Назначается приказом (распоряжением) руководителя органа власти, подведомственного учреждения, иной организации и учреждения, являющихся пользователями информационных систем администрации Красненского района.

2.8. Модель нарушителя - описательное представление опыта, знаний, доступных ресурсов возможных нарушителей ИБ, необходимых им для реализации угрозы ИБ, и возможной мотивации действий.

2.9. Модель угроз - описательное представление свойств или характеристик угроз безопасности информации.

2.10. Ответственное лицо - руководитель, ответственный за обеспечение информационной безопасности в администрации Красненского района, в том числе за обнаружение, предупреждение и ликвидацию последствий компьютерных атак, и реагирование на компьютерные инциденты. Назначается администрацией Красненского района.

Ответственное лицо в своей деятельности руководствуется Положением о руководителе, ответственном за обеспечение информационной безопасности в администрации Красненского района, утвержденным распоряжением администрации Красненского района.

2.11. Ответственное подразделение - отдел (выделенный специалист) по информационной безопасности в органе власти, подведомственном учреждении, иной организации и учреждении, являющийся пользователем информационных систем администрации Красненского района. Основные функции - выполнение Политики информационной безопасности, разработка,

внедрение и поддержка систем обеспечения информационной безопасности информационных систем и информационных инфраструктур, также обеспечивающих обнаружение, предупреждение, ликвидацию последствий компьютерных атак и реагирование на компьютерные инциденты.

2.12. Пользователь информационной системы администрации Красненского района - администрация Красненского района, подведомственное учреждение, использующие в своей деятельности информационные системы и информационные инфраструктуры администрации Красненского района.

2.13. Рисковое событие информационной безопасности - это событие, обусловленное риском, повлекшее или способное повлечь за собой нарушение бесперебойного функционирования информационных систем и информационных инфраструктур, утечку и/или искажения обрабатываемой информации в администрации Красненского района в результате действий пользователей, а также по причине внешних событий.

2.14. Сотрудник пользователя информационной системы - сотрудник администрации Красненского района, подведомственного учреждения, обладающий возможностью использования информационных систем и информационных инфраструктур администрации Красненского района.

2.15. Угроза информационной безопасности - риск, влияющий на нарушение одного (или нескольких) свойств информации - целостности, конфиденциальности, доступности информационных систем и информационных инфраструктур (объектов защиты) администрации Красненского района.

2.16. Уязвимость - слабость одного или нескольких активов, которая может быть использована одной или несколькими угрозами (ГОСТ Р ИСО/МЭК 13 3 3 5-1-2006).

3. Объект защиты

3.1. Основными объектами защиты системы информационной безопасности являются:

- информационные ресурсы, содержащие сведения, составляющие государственную тайну, служебную тайну, персональные данные и иную защищаемую законом информацию, а также открыто распространяемую информацию о деятельности администрации Красненского района, независимо от формы и вида ее представления;

- процессы обработки информации в информационных системах - информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации;

- информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы.

-

4. Цели и задачи деятельности по обеспечению информационной безопасности

4.1. Целью деятельности по обеспечению информационной безопасности является снижение угроз информационной безопасности.

4.2. Основные задачи деятельности по обеспечению информационной безопасности:

- выявление потенциальных угроз информационной безопасности и уязвимостей объектов защиты;
- предотвращение инцидентов информационной безопасности;
- исключение либо минимизация выявленных угроз.

5. Угрозы информационной безопасности

5.1. Все множество потенциальных угроз безопасности информации делится на три класса по природе их возникновения: антропогенные, техногенные и естественные (природные).

5.2. Возникновение антропогенных угроз обусловлено деятельностью человека. Среди них можно выделить угрозы, возникающие вследствие как непреднамеренных (неумышленных) действий: угрозы, вызванные ошибками в проектировании информационной системы и ее элементов, ошибками в действиях персонала и т.п., так и угрозы, возникающие в силу умышленных действий, связанные с корыстными, идейными или иными устремлениями людей.

К антропогенным угрозам относятся угрозы, связанные с нестабильностью и противоречивостью требований регуляторов и контрольных органов, с действиями Сотрудников пользователя информационных систем администрации Красненского района.

5.3. Возникновение техногенных угроз обусловлено воздействиями на объект угрозы объективных физических процессов техногенного характера, технического состояния окружения объекта угрозы или его самого, не обусловленных напрямую деятельностью человека.

К техногенным угрозам могут быть отнесены сбои, в том числе в работе, или разрушение систем, созданных человеком.

5.4. Возникновение естественных (природных) угроз обусловлено воздействиями на объект угрозы объективных физических процессов природного характера, стихийных природных явлений, состояний физической среды, не обусловленных напрямую деятельностью человека.

К естественным (природным) угрозам относятся угрозы метеорологические, атмосферные, геофизические, геомагнитные и пр., включая экстремальные климатические условия, метеорологические явления, стихийные бедствия.

Источники угроз по отношению к инфраструктуре администрации Красненского района могут быть как внешними, так и внутренними.

6. Модель нарушителя информационной безопасности

По отношению к администрации Красненского района нарушители подразделяются на внешних и внутренних.

6.1. Внутренние нарушители.

В качестве потенциальных внутренних нарушителей рассматриваются:

- зарегистрированные Пользователи информационных систем, функционирующих в администрации Красненского района;
- Сотрудники пользователей информационных систем администрации Красненского района, не являющиеся зарегистрированными и не допущенные к информационным системам администрации Красненского района;
- ИТ-подразделения;
- Сотрудники пользователей информационных систем администрации Красненского района;
- сотрудники, обеспечивающие физическую безопасность Пользователям информационных систем администрации Красненского района;
- физические лица, имеющие доступ к информационным системам администрации Красненского района.

6.2. Внешние нарушители.

В качестве потенциальных внешних нарушителей рассматриваются:

- бывшие Сотрудники пользователей информационных систем администрации Красненского района, которые являлись Пользователями информационных систем администрации Красненского района;
- представители организаций, взаимодействующих по вопросам технического обеспечения информационных инфраструктур и информационных систем администрации Красненского района;
- внешние Пользователи информационных систем и информационных инфраструктур администрации Красненского района;
- посетители зданий и помещений администрации Красненского района и подведомственных учреждений, осуществляющих свою деятельность с применением информационных систем и информационных инфраструктур (объектов защиты) администрации Красненского района;
- члены преступных организаций, сотрудники спецслужб или лица, действующие по их заданию;
- лица, случайно или умышленно проникшие в корпоративную информационную инфраструктуру и информационные системы администрации Красненского района из внешних телекоммуникационных сетей (хакеры).

6.3. В отношении внутренних и внешних нарушителей принимаются следующие ограничения и предположения о характере их возможных действий:

- нарушитель скрывает свои несанкционированные действия от других сотрудников;

- несанкционированные действия нарушителя могут быть следствием ошибок пользователей, эксплуатирующего и обслуживающего персонала (ИТ-подразделений), а также недостатков принятой технологии обработки, хранения и передачи информации;

- в своей деятельности вероятный нарушитель может использовать любое имеющееся средство перехвата информации, воздействия на информацию и информационные системы, адекватные финансовые средства для подкупа персонала, шантаж, методы социальной инженерии и другие средства и методы для достижения стоящих перед ним целей;

- внешний нарушитель может действовать в сговоре с внутренним нарушителем.

7. Основные положения по обеспечению информационной безопасности

7.1. Требования об обеспечении информационной безопасности обязательны к соблюдению всеми Сотрудниками пользователей информационных систем администрации Красненского района.

7.2. На территории Красненского района приветствуется и поощряется деятельность Сотрудников пользователей информационных систем администрации Красненского района по обеспечению информационной безопасности.

7.3. Неисполнение или некачественное исполнение Пользователями информационных систем обязанностей по обеспечению информационной безопасности повлечет лишение доступа к информационным системам, а также применение к виновным административных мер воздействия, степень которых определяется действующим законодательством Российской Федерации.

7.4. Политика информационной безопасности в части противодействия угрозам информационной безопасности заключается в сбалансированной реализации взаимодополняющих мер по обеспечению безопасности: от организационных мер на уровне администрации Красненского района до специализированных мер информационной безопасности по каждому выявленному риску, основанных на оценке рисков информационной безопасности.

7.5. С целью поддержки заданного уровня защищенности Пользователи информационных систем администрации Красненского района должны придерживаться процессного подхода в построении системы менеджмента информационной безопасности.

Система менеджмента информационной безопасности для информационных систем и информационных инфраструктур администрации Красненского района основывается на осуществлении основных процессов (планирование, реализация и эксплуатация защитных мер, проверка (мониторинг и анализ), совершенствование), соответствующих требованиям федеральных органов исполнительной власти, уполномоченных в области

обеспечения безопасности и противодействия техническим разведкам и технической защиты информации, и стандартов по обеспечению информационной безопасности. Реализация этих процессов осуществляется в виде непрерывного цикла - «планирование - реализация - проверка - совершенствование - планирование - ...», направленного на постоянное совершенствование деятельности по обеспечению информационной безопасности и повышение ее эффективности.

На всех этапах жизненного цикла управление информационной безопасностью информационных систем и информационных инфраструктур осуществляется с соблюдением норм действующего законодательства в области информационной безопасности, действующих на территории Российской Федерации и Белгородской области.

7.6. При планировании мероприятий по обеспечению информационной безопасности у Пользователей информационных систем администрации Красненского района должны осуществляться следующие мероприятия:

- 7.6.1. Определение и распределение ролей Сотрудников пользователей информационных систем администрации Красненского района, связанных с обеспечением информационной безопасности.

- 7.6.2. Оценка важности информационных активов с учетом потребности в обеспечении их свойств с точки зрения информационной безопасности.

- 7.6.3. Менеджмент рисков информационной безопасности (недопустимых событий), включающий:

- анализ влияния на информационную безопасность информационных систем и информационных инфраструктур администрации Красненского района внешних по отношению к информационным системам и информационным инфраструктурам администрации Красненского района событий, информационных технологий, применяемых в их деятельности;

- выявление проблем обеспечения информационной безопасности, анализ причин их возникновения и прогнозирование их развития;

- определение моделей угроз информационной безопасности для информационных систем и информационных инфраструктур администрации Красненского района;

- выявление, анализ и оценка значимых для информационных систем и информационных инфраструктур администрации Красненского района угроз информационной безопасности;

- выявление возможных негативных последствий для информационных систем и информационных инфраструктур администрации Красненского района, наступающих в результате проявления факторов риска информационной безопасности, в том числе связанных с нарушением свойств безопасности их информационных активов;

- идентификацию и анализ рисковых событий информационной безопасности;

- оценку величины рисков информационной безопасности и

определение среди них рисков (недопустимых событий), неприемлемых для информационных систем и информационных инфраструктур администрации Красненского района;

- обработку результатов оценки рисков информационной безопасности;

- оптимизацию рисков информационной безопасности за счет выбора и применения защитных мер, противодействующих проявлениям факторов риска и минимизирующих возможные негативные последствия для информационных систем и информационных инфраструктур администрации Красненского района, в случае наступления рисковых событий;

- оценку влияния защитных мер на цели основной деятельности для информационных систем и информационных инфраструктур администрации Красненского района;

- оценку затрат на реализацию защитных мер;

- рассмотрение и оценку различных вариантов решения задач по обеспечению информационной безопасности;

- разработку планов управления рисками, предусматривающих различные защитные меры и варианты их применения, и выбор из них такого, реализация которого максимально положительно скажется на целях деятельности информационных систем и информационных инфраструктур администрации Красненского района, и будет оптимальна с точки зрения произведенных затрат и ожидаемого эффекта;

- документальное оформление целей и задач обеспечения информационной безопасности для информационных систем и информационных инфраструктур администрации Красненского района, поддержка в актуальном состоянии нормативно-методического обеспечения деятельности в сфере информационной безопасности.

7.7. В рамках реализации деятельности по обеспечению информационной безопасности в администрации Красненского района осуществляется менеджмент инцидентов информационной безопасности, включающий:

- сбор информации о событиях информационной безопасности;

- выявление и анализ инцидентов информационной безопасности;

- расследование инцидентов информационной безопасности;

- оперативное реагирование на инцидент информационной безопасности;

- минимизация негативных последствий инцидентов информационной безопасности;

- оперативное доведение до руководителей Пользователей информационных систем администрации Красненского района информации по наиболее значимым инцидентам информационной безопасности и оперативное принятие решений по ним, включая регламентирование порядка реагирования на инциденты информационной безопасности;

- выполнение принятых решений по всем инцидентам

информационной безопасности в установленные сроки;

- пересмотр применяемых требований, мер и механизмов по обеспечению информационной безопасности по результатам рассмотрения инцидентов информационной безопасности;

- повышение уровня знаний Сотрудников пользователей информационных систем администрации Красненского района в вопросах обеспечения информационной безопасности;

- обеспечение регламентации и управления доступом к программным и программно-техническим средствам и сервисам автоматизированных систем, информационных систем администрации Красненского района и информации, обрабатываемой в них;

- применение средств криптографической защиты информации;

- обеспечение бесперебойной работы информационных систем,

информационных инфраструктур, автоматизированных систем и сетей связи;

- обеспечение возобновления работы информационных систем, информационных инфраструктур, автоматизированных систем и сетей связи после прерываний и нештатных ситуаций;

- применение централизованных средств защиты от вредоносного программного обеспечения, а для наиболее критичных информационных систем применение эшелонированной системы антивирусной защиты;

- обеспечение информационной безопасности на стадиях жизненного цикла информационных систем администрации Красненского района, связанных с проектированием, разработкой, приобретением, поставкой, вводом в действие, сопровождением (сервисным обслуживанием);

- обеспечение информационной безопасности при использовании доступа в сеть Интернет и услуг электронной почты;

- контроль доступа в здания и помещения администрации Красненского района Пользователей информационных систем администрации Красненского района.

7.8. Обеспечение защиты информации от утечки по техническим каналам, включающее:

- применение мер и технических средств, снижающих вероятность несанкционированного получения информации в устной форме - пассивная защита;

- применение мер и технических средств, создающих помехи при несанкционированном получении информации - активная защита;

- применение мер и технических средств, позволяющих выявлять каналы несанкционированного получения информации - поиск.

7.9. В целях проверки соблюдения деятельности по обеспечению информационной безопасности Пользователями информационных систем администрации Красненского района Ответственным лицом и Головным подразделением с привлечением учреждений (организаций), имеющих лицензии Федеральной службы по техническому и экспортному контролю и

Федеральной службы безопасности Российской Федерации, осуществляется:

- контроль правильности реализации и эксплуатации защитных мер;
- контроль изменений конфигурации информационных систем и подсистем, а также информационных инфраструктур администрации Красненского района;
- мониторинг рисков (недопустимых событий) и соответствующий их пересмотр;
- контроль реализации и исполнения требований Сотрудниками пользователей информационных систем администрации Красненского района действующих правовых документов по обеспечению информационной безопасности администрации Красненского района;
- контроль деятельности Сотрудников пользователей информационных систем администрации Красненского района, направленный на выявление и предотвращение использования информационных систем администрации Красненского района в личных интересах.

7.10. В целях совершенствования деятельности по обеспечению информационной безопасности в администрации Красненского района осуществляется периодическое, а при необходимости оперативное уточнение (пересмотр) целей и задач обеспечения информационной безопасности.

8. Организационная основа деятельности по обеспечению информационной безопасности

8.1. В целях выполнения задач по обеспечению информационной безопасности в соответствии с рекомендациями требований федеральных органов исполнительной власти, уполномоченных в области обеспечения безопасности и противодействия техническим разведкам и технической защиты информации, и российских стандартов по информационной безопасности в информационных системах и информационных, инфраструктурах администрации Красненского района определена следующая вертикаль взаимодействия по вопросам информационной безопасности:

- Ответственное лицо;
- Куратор;
- Головное подразделение;
- Ответственное подразделение;
- Сотрудник.

Вертикаль взаимодействия может быть изменена с учетом тенденций развития настоящей Политики информационной безопасности.

8.2. Оперативная деятельность и планирование деятельности по обеспечению информационной безопасности в информационных системах и информационных инфраструктурах администрации Красненского района осуществляются Ответственным лицом и Головным подразделением. Также Головным подразделением осуществляется координация деятельности Ответственных подразделений администрации района. Определение

потребности и координация деятельности подведомственных учреждений по вопросам информационной безопасности осуществляется Ответственными подразделениями.

8.3. Задачами Головного подразделения являются:

- установление потребностей для информационных систем и информационных инфраструктур администрации Красненского района в применении мер обеспечения информационной безопасности, определяемых как требованиями внутренних нормативных документов, так и требованиями нормативных актов Российской Федерации;

- соблюдение действующего законодательства Российской Федерации, нормативных актов федеральных органов исполнительной власти, уполномоченных в области обеспечения безопасности и противодействия техническим разведкам и технической защиты информации;

- разработка и пересмотр внутренних правовых документов по обеспечению информационной безопасности для информационных систем и информационных инфраструктур администрации Красненского района, включая планы, политики, положения, регламенты, инструкции, методики, перечни сведений и иные виды внутренних правовых документов;

- осуществление контроля актуальности и непротиворечивости внутренних правовых документов (политик, планов, методик и т.д.), затрагивающих вопросы информационной безопасности в информационных системах и информационных инфраструктурах администрации Красненского района;

- обучение и контроль знаний Сотрудников пользователей информационных систем администрации Красненского района в области обеспечения информационной безопасности и кибергигиены;

- планирование применения, участие в поставке и эксплуатации средств обеспечения информационной безопасности на объектах, информационных инфраструктурах и информационных системах, функционирующих в администрации Красненского района;

- выявление и предотвращение реализации угроз информационной безопасности в информационных системах и информационных инфраструктурах администрации Красненского района;

- выявление и организация реагирования на инциденты информационной безопасности в информационных системах и информационных инфраструктурах администрации Красненского района;

- информирование Ответственного лица и Кураторов об угрозах и рисковых событиях информационной безопасности;

- прогнозирование и предупреждение инцидентов информационной безопасности в информационных системах и информационных инфраструктурах администрации Красненского района;

- пресечение несанкционированных действий нарушителей информационной безопасности:

- поддержка базы инцидентов информационной безопасности, анализ,

разработка оптимальных процедур реагирования на инциденты и обучение сотрудников Ответственных подразделений;

- типизация решений по применению мер и средств обеспечения информационной безопасности и распространение типовых решений;

- обеспечение эксплуатации средств и механизмов обеспечения информационной безопасности информационных систем и информационных инфраструктур администрации Красненского района;

- мониторинг и оценка информационной безопасности, включая оценку полноты и достаточности защитных мер и видов деятельности по обеспечению информационной безопасности;

- мониторинг обеспечения информационной безопасности в информационных системах и информационных инфраструктурах администрации Красненского района,

в том числе на основании информации об инцидентах информационной безопасности, результатах мониторинга, оценки и аудита информационной безопасности;

- информирование Ответственного лица и Кураторов об угрозах информационной безопасности, влияющих на деятельность информационных систем и информационных инфраструктур администрации Красненского района.

8.4. Задачами Ответственного подразделения являются:

- установление потребностей в применении мер обеспечения информационной безопасности, определяемых как внутренними требованиями, так и требованиями нормативных актов Российской Федерации;

- соблюдение действующего федерального законодательства, нормативных актов федеральных органов исполнительной власти, уполномоченных в области обеспечения безопасности и противодействия техническим разведкам и технической защиты информации;

- разработка и пересмотр внутренних правовых актов по обеспечению информационной безопасности, включая планы, политики, положения, регламенты, инструкции, методики, перечни сведений и иные виды внутренних правовых актов;

- осуществление контроля актуальности и соответствия действующему законодательству внутренних правовых актов (политик, планов, методик и т.д.) администрации района и подведомственных учреждений, являющихся Пользователями информационных систем и информационных инфраструктур администрации Красненского района, затрагивающих вопросы информационной безопасности;

- обучение, контроль и непосредственная работа с Сотрудниками пользователей информационных систем администрации Красненского района в области обеспечения информационной безопасности и кибергигиены;

- планирование применения, участие в поставке и эксплуатации

средств обеспечения информационной безопасности на средства вычислительной техники, информационные инфраструктуры, информационные системы, принадлежащие Пользователям информационных систем, имеющих взаимодействие с информационными системами администрации Красненского района;

- выявление и предотвращение реализации угроз информационной безопасности;

- выявление инцидентов информационной безопасности и реагирование на них;

- информирование руководителей Пользователей информационных систем об угрозах и рисковых событиях информационной безопасности;

- прогнозирование и предупреждение инцидентов информационной безопасности;

- пресечение несанкционированных действий нарушителей информационной безопасности;

- поддержка базы инцидентов информационной безопасности, анализ, разработка оптимальных процедур реагирования на инциденты и обучение сотрудников Ответственных подразделений;

- типизация решений по применению мер и средств обеспечения информационной безопасности и распространение типовых решений на подведомственные учреждения, являющиеся Пользователями информационных систем администрации Красненского района;

- обеспечение эксплуатации средств и механизмов обеспечения информационной безопасности;

- мониторинг и оценка информационной безопасности, включая оценку полноты и достаточности защитных мер и видов деятельности по обеспечению информационной безопасности в подведомственных учреждениях, являющихся Пользователями информационных систем администрации Красненского района;

- контроль обеспечения информационной безопасности в подведомственных учреждениях, являющихся Пользователями информационных систем администрации Красненского района, в том числе на основании информации об инцидентах информационной безопасности, результатах мониторинга, оценки и аудита информационной безопасности;

- информирование Головного подразделения, Куратора и руководителей подведомственных им учреждений об угрозах информационной безопасности, влияющих на их деятельность.

8.5. Основными функциями Куратора в вопросах информационной безопасности являются:

- координация и внедрение информационной безопасности в подведомственных учреждениях, являющихся Пользователями информационных систем администрации Красненского района;

- взаимодействие с Головным подразделением по вопросам информационной безопасности с целью совершенствования мер по

повышению защищенности обрабатываемой информации;

- согласование основополагающих правовых документов в сфере информационных технологий, цифровизации и цифровой трансформации и информационной безопасности с Ответственным лицом.

8.6. Основными задачами Сотрудников пользователей информационных систем администрации Красненского района при выполнении возложенных на них обязанностей и в рамках их участия в деятельности по обеспечению информационной безопасности являются:

- соблюдение требований информационной безопасности, устанавливаемых действующим законодательством Российской Федерации, правовыми актами Белгородской области, Пользователей информационных систем администрации Красненского района;

- выявление и предотвращение реализации угроз информационной безопасности в пределах своей компетенции;

- выявление и реагирование на инциденты информационной безопасности;

- информирование в установленном порядке непосредственного руководителя и Ответственного подразделения о выявленных угрозах и рисковых событиях информационной безопасности;

- прогнозирование и предупреждение инцидентов информационной безопасности в пределах своей компетенции;

- мониторинг и оценка информационной безопасности в рамках своего участка работы (рабочего места, структурного подразделения) в пределах своей компетенции.

9. Финансирование

9.1. Финансирование расходов на реализацию положений Политики информационной безопасности в администрации Красненского района осуществляется в пределах средств, предусмотренных районным бюджетом на реализацию функций, возложенных на Головное подразделение, связанных с использованием современных информационно-коммуникационных технологий и Пользователей информационных систем администрации Красненского района.

10. Заключительные положения

10.1. Требования Политики информационной безопасности могут развиваться другими правовыми актами Белгородской области, которые дополняют и уточняют ее.

10.2. В случае изменения действующего законодательства Российской Федерации и иных правовых актов Головное подразделение обязано незамедлительно организовать подготовку и внесение соответствующих изменений в положения действующей Политики информационной безопасности.

10.3. Внесение изменений в Политику информационной безопасности

осуществляется на периодической и внеплановой основе:

- периодическое внесение изменений в Политику информационной безопасности осуществляется не реже одного раза в 24 месяца;

- внеплановое внесение изменений в Политику информационной безопасности может производиться по результатам мониторинга и анализа инцидентов информационной безопасности, актуальности, достаточности и эффективности используемых мер обеспечения информационной безопасности, результатам проведения внутренних аудитов информационной безопасности и других контрольных мероприятий.

10.4. Ответственным за внесение изменений в Политику информационной безопасности является Головное подразделение.