РОССИЙСКАЯ ФЕДЕРАЦИЯ
БЕЛГОРОДСКАЯ ОБЛАСТЬ
АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО РАЙОНА
«КРАСНОЯРУЖСКИЙ РАЙОН»

РАСПОРЯЖЕНИЕ

« 12 » февраля 2025 года № 78

Об утверждении политики информационной безопасности в администрации Краснояружского района

Во исполнение Указа Президента Российской Федерации от 1 мая 2022 года № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» и в целях повышения устойчивости и безопасности функционирования информационных ресурсов администрации Краснояружского района:

1. Утвердить политику информационной безопасности в администрации Краснояружского района (прилагается).
2. Контроль за исполнением настоящего распоряжения возложить на заместителя главы администрации района, руководителя аппарата – Носова М.В.

Глава администрации Краснояружского района **В.В. Кутоманов**

Администрация Краснояружского района Белгородской области * Управление делами

Утверждена
распоряжением администрации
Краснояружского района
от «12» февраля 2025 года
№ 78

Политика информационной безопасности администрации Краснояружского района

1. Общие положения

1.1. Политика информационной безопасности администрации Краснояружского 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»;
- нормативными актами 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 Краснояружского района, сотрудникам подведомственных учреждений, являющихся пользователями информационных систем администрации Краснояружского района и представляет собой официально принятую администрацией Краснояружского 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 администрации Краснояружского района.

1.4. Требования информационной безопасности соответствуют целям деятельности администрации Краснояружского 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 Краснояружского района, сотрудниками подведомственных учреждений.

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

1.8. Положения Политики информационной безопасности учитываются при разработке локальных политик информационной безопасности иных органов местного самоуправления и подведомственных им учреждений Краснояружского района.

2.Список терминов и определений

2.1. Бизнес процесс - последовательность технологически связанных операций по выполнению возложенных полномочий на администрацию Краснояружского района, органы местного самоуправления и подведомственные им учреждения Краснояружского района.

2.2. 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.

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

2.4. 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.

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

Краснояружского района.

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

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

2.8. Ответственное лицо - сотрудник, ответственный за обеспечение информационной безопасности в администрации Краснояружского района, в том числе за обнаружение, предупреждение и ликвидацию последствий компьютерных атак, и реагирование на компьютерные инциденты.

2.9. 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 Краснояружского района в результате действий пользователей, а так же по причине внешних событий.

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

2.11. Уязвимость - слабость одного или нескольких активов, которая может быть использована одной или несколькими угрозами.

3. Объект защиты

3.1. Основными объектами защиты системы информационной безопасности являются:

- инфраструктурные ресурсы, содержащие сведения, составляющие государственную тайну, служебную тайну, персональные данные и иную защищаемую законом информацию, а также открыто распространяемую информацию о деятельности администрации Краснояружского 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.

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 Краснояружского района могут быть как внешними, так и внутренними.

6. Модель нарушителя информационной безопасности.

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

6.1. Внутренние нарушители.

В качестве потенциальных внутренних нарушителей рассматриваются:

- зарегистрированные Пользователи информационных систем, функционирующих в администрации Краснояружского района;

- сотрудники пользователей информационных систем администрации Краснояружского района не являющиеся зарегистрированными и не допущенные к информационным системам администрации Краснояружского района;

- ИТ-подразделения;

- сотрудники пользователей информационных систем администрации Краснояружского района;

- сотрудники, обеспечивающие физическую безопасность Пользователям информационных систем администрации Краснояружского района;

- физические лица, имеющие доступ к информационным системам администрации Краснояружского района.

6.2. Внешние нарушители.

В качестве потенциальных внешних нарушителей рассматриваются:

- бывшие сотрудники пользователей информационных систем администрации Краснояружского района, которые являлись пользователями информационных систем администрации Краснояружского района;

- представители организаций, взаимодействующих по вопросам технического обеспечения информационных инфраструктур и информационных систем администрации Краснояружского района;

- внешние пользователи информационных систем и информационных инфраструктур администрации Краснояружского района;

- посетители зданий и помещений администрации Краснояружского 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 Краснояружского 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 Краснояружского района.

7.2. 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.

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

7.4. С целью поддержки заданного уровня защищенности пользователи информационных систем администрации Краснояружского района должны придерживаться процессного подхода в построении системы менеджмента информационной безопасности.

Система менеджмента информационной безопасности для информационных систем и информационных инфраструктур администрации Краснояружского 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.

7.5. При планировании мероприятий по обеспечению информационной безопасности у пользователей информационных систем администрации Краснояружского района должны осуществляться

следующие мероприятия:

7.5.1. Определение и распределение ролей сотрудников пользователей информационных систем администрации Краснояружского района, связанных с обеспечением информационной безопасности.

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

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

- 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 Краснояружского района;

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

- выявление возможных негативных последствий для информационных систем и информационных инфраструктур администрации Краснояружского 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 Краснояружского 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 Краснояружского района, в случае наступления рисковых событий;

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

7.6. В рамках реализации деятельности по обеспечению информационной безопасности в администрации Краснояружского 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;
- повышение уровня знаний сотрудников пользователей информационных систем администрации Краснояружского района в вопросах обеспечения информационной безопасности;
- обеспечение регламентации и управления доступом к программным и программно-техническим средствам и сервисам автоматизированных систем, информационных систем администрации Краснояружского района и информации, обрабатываемой в них;
- применение средств криптографической защиты информации;
- обеспечение бесперебойной работы информационных систем и информационных инфраструктур;
- применение централизованных средств защиты от вредоносного программного обеспечения, а для наиболее критичных информационных систем применение эшелонированной системы антивирусной защиты;
- обеспечение информационной безопасности при использовании доступа в сеть Интернет и услуг электронной почты.

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

8. Заключительные положения

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

8.2. В случае изменения действующего законодательства Российской Федерации и иных правовых актов незамедлительно организуется подготовка и внесение соответствующих изменений в положения действующей Политики информационной безопасности.

8.3. 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.

8.4. Ответственным за внесение изменений в Политику информационной безопасности является специалист по информационной безопасности.