ГУБЕРНАТОР КРАСНОДАРСКОГО КРАЯ

ПОСТАНОВЛЕНИЕ

от 26.10.2023 № 868

г. Краснодар

Об утверждении Положения о заместителе Губернатора Краснодарского края, ответственном за обеспечение информационной безопасности администрации Краснодарского края

В соответствии с Указом Президента Российской Федерации от 1 мая 2022 г. № 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации", постановлением Правительства Российской Федерации от 15 июля 2022 г. № 1272 "Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)" п о с т а н о в л я ю:

1. Утвердить Положение о заместителе Губернатора Краснодарского края, ответственном за обеспечение информационной безопасности администрации Краснодарского края, согласно приложению к настоящему постановлению.

2. Департаменту информационной политики Краснодарского края (Жукова Г.А.) обеспечить размещение (опубликование) настоящего постановления (без приложения к нему) на сайте в информационно-телекоммуникационной сети "Интернет" http://admkrai.krasnodar.ru и направление на "Официальный интернет-портал правовой информации" (www.pravo.gov.ru).

3.Контроль за выполнением настоящего постановления оставляю за собой.

4. Постановление вступает в силу на следующий день после его официального опубликования.

Губернатор
Краснодарского края В.И. Кондратьев

Приложение

УТВЕРЖДЕНО
постановлением Губернатора
Краснодарского края
от 26.10.2023 № 868

ПОЛОЖЕНИЕ
о заместителе Губернатора Краснодарского края, ответственном за обеспечение информационной безопасности администрации Краснодарского края

1. Общие положения

1.1. Настоящее Положение определяет полномочия, права и обязанности заместителя Губернатора Краснодарского края, ответственного за обеспечение информационной безопасности администрации Краснодарского края, в том числе за обнаружение, предупреждение и ликвидацию последствий компьютерных атак, и реагирование на компьютерные инциденты (далее – ответственное лицо).

1.2. Ответственное лицо определяется Губернатором Краснодарского края.

1.3. Ответственное лицо осуществляет свою деятельность на основании законодательства Российской Федерации с учетом особенностей деятельности администрации Краснодарского края и подчиняется непосредственно Губернатору Краснодарского края.

1.4. Ответственное лицо входит в состав Совета по защите информации при администрации Краснодарского края.

1.5. Указания и поручения ответственного лица в части обеспечения информационной безопасности являются обязательными для исполнения всеми государственными гражданскими служащими в администрации Краснодарского края и работниками, замещающими должности, не являющиеся должностями государственной гражданской службы Краснодарского края.

2. Квалификационные требования к ответственному лицу

2.1. Ответственное лицо должно иметь высшее образование (не ниже уровня специалитета, магистратуры) по направлению обеспечения информационной безопасности. Если ответственное лицо имеет высшее образование по другому направлению подготовки (специальности), оно должно пройти обучение по программе профессиональной переподготовки по направлению "Информационная безопасность".

2.2. Для ответственного лица требуется наличие следующих знаний, умений и профессиональных компетенций:

1) основные (в том числе производственные, бизнес и управленческие) процессы администрации Краснодарского края, специфика обеспечения информационной безопасности администрации Краснодарского края;

2) влияние информационных технологий на деятельность администрации Краснодарского края, в том числе:

роль и место информационных технологий (в том числе степень интеграции информационных технологий) в процессах функционирования администрации Краснодарского края;

зависимость основных процессов функционирования администрации Краснодарского края от информационных технологий;

3) информационно-телекоммуникационные технологии, в том числе:

современные информационно-телекоммуникационные технологии, используемые в администрации Краснодарского края;

способы построения информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления формирования информационных ресурсов (далее – системы и сети), в том числе ограниченного доступа;

типовые архитектуры систем и сетей, требования к их оснащенности программными (программно-техническими) средствами;

принципы построения и функционирования современных операционных систем, систем управления базами данных, систем и сетей, основных протоколов систем и сетей;

4) обеспечение информационной безопасности, в том числе:

цели, задачи, основы организации, ключевые элементы, основные способы и средства обеспечения информационной безопасности;

цели обеспечения информационной безопасности применительно к основным процессам функционирования администрации Краснодарского края, реализации и контроля их достижения;

принципы и направления стратегического развития информационной безопасности в администрации Краснодарского края;

правила разработки, утверждения и отмены организационно-распорядительных документов по вопросам обеспечения информационной безопасности администрации Краснодарского края, состав и содержание таких документов;

порядок организации работ по обеспечению информационной безопасности администрации Краснодарского края;

основные негативные последствия, наступление которых возможно в результате реализации угроз безопасности информации, способы и методы обеспечения и поддержания необходимого уровня (состояния) информационной безопасности администрации Краснодарского края для исключения (невозможности реализации) негативных последствий, а также порядок проведения практических проверок и контроля результативности применяемых способов и методов обеспечения информационной безопасности администрации Краснодарского края;

основные угрозы безопасности информации, предпосылки их возникновения и возможные пути их реализации, а также порядок оценки таких угроз;

возможности и назначения типовых программных, программно-аппаратных (технических) средств обеспечения информационной безопасности;

способы и средства проведения компьютерных атак, актуальные тактики и техники нарушителей;

порядок организации взаимодействия структурных подразделений администрации Краснодарского края при решении вопросов обеспечения информационной безопасности;

управление проектами по информационной безопасности;

антикризисное управление и принятие управленческих решений при реагировании на кризисы и компьютерные инциденты;

планирование деятельности по обеспечению информационной безопасности администрации Краснодарского края;

формулирование измеримых и практических результатов деятельности по обеспечению информационной безопасности администрации Краснодарского края;

организация разработки политики (правил, процедур), регламентирующей вопросы информационной безопасности администрации Краснодарского края и подведомственных ей организаций (далее – политика);

внедрение политики;

организация контроля и анализа применения политики;

организация мероприятий по разработке единых инструментов и механизмов контроля деятельности по обеспечению информационной безопасности в администрации Краснодарского края и в подведомственных ей организациях;

поддержка и совершенствование деятельности по обеспечению информационной безопасности в администрации Краснодарского края и ее подведомственных организациях;

организация мероприятий по определению угроз безопасности информации систем и сетей, а также по формированию требований к обеспечению информационной безопасности в администрации Краснодарского края и ее подведомственных организациях;

организация внедрения способов и средств для обеспечения информационной безопасности в администрации Краснодарского края и в подведомственных ей организациях;

организация мероприятий по анализу и контролю состояния информационной безопасности администрации Краснодарского края и модернизации (трансформации) процессов функционирования администрации Краснодарского края в целях обеспечения информационной безопасности в администрации Краснодарского края;

обеспечение информационной безопасности в ходе эксплуатации систем и сетей, а также при выводе их из эксплуатации;

организация мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные ресурсы администрации Краснодарского края и реагированию на компьютерные инциденты;

организация мероприятий по отслеживанию и контролю достижения целей информационной безопасности (фактически достигнутый эффект и результат) администрации Краснодарского края и подведомственных ей организаций.

2.3. С учетом области и вида деятельности администрации Краснодарского края от ответственного лица требуется знание нормативных правовых актов Российской Федерации, методических документов, международных и национальных стандартов в области:

1) защиты государственной тайны;

2) защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в том числе персональных данных;

3) обеспечения безопасности критической информационной инфраструктуры Российской Федерации;

4) обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты;

5) создания и обеспечения безопасного функционирования государственных информационных систем и информационных систем в защищенном исполнении;

6) создания, обеспечения технических условий установки и эксплуатации средств защиты информации;

7) иных нормативных правовых актов и стандартов в области информационной безопасности.

3. Должностные обязанности ответственного лица

3.1. Ответственное лицо принимает участие в формировании политики, отвечает за согласование стратегии развития администрации Краснодарского края в части вопросов обеспечения информационной безопасности.

3.2. Ответственное лицо:

1) организует разработку политики, направленной в том числе на обеспечение и поддержание стабильной деятельности администрации Краснодарского края и процессов ее функционирования в случае проведения компьютерных атак, отвечает за согласование и утверждение политики в администрации Краснодарского края, реализацию мероприятий, предусмотренных политикой, отслеживает и контролирует результаты реализации политики;

2) организует работу по обеспечению информационной безопасности администрации Краснодарского края, в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты, формулированию перечня негативных последствий, проведению мероприятий по их недопущению,

отслеживанию и контролю эффективности (результативности) таких мероприятий, а также по необходимому информационному обмену;

3) организует реализацию и контроль проведения в администрации Краснодарского края организационных и технических мер, решения о необходимости осуществления которых принимаются Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю с учетом меняющихся угроз в информационной сфере, а также самостоятельно ответственным лицом в результате своей деятельности;

4) организует беспрепятственный доступ (в том числе удаленный) должностным лицам Федеральной службы безопасности Российской Федерации и ее территориальных органов к информационным ресурсам, принадлежащим администрации Краснодарского края либо используемым администрацией Краснодарского края, доступ к которым обеспечивается посредством использования информационно-телекоммуникационной сети "Интернет", в целях осуществления мониторинга их защищенности, а также работникам структурного подразделения администрации Краснодарского края, осуществляющего функции по обеспечению информационной безопасности администрации Краснодарского края;

5) организует взаимодействие с должностными лицами Федеральной службы безопасности Российской Федерации и ее территориальных органов, в том числе контроль исполнения указаний, данных Федеральной службой безопасности Российской Федерации и ее территориальными органами по результатам мониторинга защищенности информационных ресурсов, принадлежащих администрации Краснодарского края, либо используемых администрацией Краснодарского края, доступ к которым обеспечивается посредством использования информационно-телекоммуникационной сети "Интернет";

6) организует контроль за выполнением требований нормативных правовых актов, нормативно-технической документации, за соблюдением установленного порядка выполнения работ при решении вопросов, касающихся защиты информации;

7) организует развитие информационной безопасности, формирование и развитие навыков в сфере информационной безопасности государственных гражданских служащих в администрации Краснодарского края и работников, замещающих должности, не являющиеся должностями государственной гражданской службы Краснодарского края;

8) организует разработку и реализацию мероприятий по обеспечению информационной безопасности в администрации Краснодарского края в соответствии с требованиями к обеспечению информационной безопасности, установленными федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации;

9) организует контроль пользователей информационных ресурсов администрации Краснодарского края в части соблюдения ими режима конфиденциальности информации, правил работы со съемными машинными

носителями информации, выполнения организационных и технических мер по защите информации;

10) организует планирование мероприятий по обеспечению информационной безопасности в администрации Краснодарского края и в подведомственных ей организациях;

11) организует подготовку правовых актов, иных организационно-распорядительных документов по вопросам обеспечения информационной безопасности в администрации Краснодарского края, осуществляет согласование иных документов администрации Краснодарского края в части обеспечения информационной безопасности;

12) организует проведение научно-исследовательских и опытно-конструкторских работ по вопросам обеспечения информационной безопасности (при наличии таковых) в администрации Краснодарского края и в подведомственных ей организациях;

13) организует проведение контроля за состоянием обеспечения информационной безопасности в администрации Краснодарского края и в подведомственных ей организациях, включая оценку защищенности систем и сетей, оператором которых является администрация Краснодарского края и ее подведомственные организации.

3.3. Ответственное лицо:

1) осуществляет регулярный контроль текущего уровня (состояния) информационной безопасности в администрации Краснодарского края, а также отвечает за реализацию мероприятий, направленных на поддержание и развитие уровня (состояния) информационной безопасности администрации Краснодарского края, в том числе с учетом появления новых угроз безопасности информации и современных способов и методов проведения компьютерных атак;

2) осуществляет регулярное и своевременное информирование Губернатора Краснодарского края о компьютерных инцидентах, текущем уровне (состоянии) информационной безопасности администрации Краснодарского края и результатах практических учений по противодействию компьютерным атакам;

3) организует контроль за ведением организационно-распорядительной документации, статистического учета и отчетности по курируемым направлениям;

4) организует разработку и согласование требований к системам и сетям, оператором которых является администрация Краснодарского края, в части обеспечения информационной безопасности.

3.4. Ответственное лицо:

1) организует и контролирует проведение мероприятий по анализу и оценке состояния информационной безопасности администрации Краснодарского края и контролирует их результаты;

2) организует и контролирует функционирование системы обеспечения информационной безопасности администрации Краснодарского края;

3) координирует деятельность иных структурных подразделений администрации Краснодарского края по вопросам обеспечения информационной безопасности.

3.5. Ответственное лицо организует работу по согласованию политики, технических заданий и иной основополагающей документации в сфере информационных технологий, цифровизации и цифровой трансформации администрации Краснодарского края.

3.6. Ответственное лицо с использованием нормативных правовых документов и методических материалов Федеральной службы безопасности Российской Федерации организует обнаружение, предупреждение и ликвидацию последствий компьютерных атак, реагирование на компьютерные инциденты с информационными ресурсами администрации Краснодарского края, а также взаимодействие с Национальным координационным центром по компьютерным инцидентам одним (или несколькими) из следующих способов:

1) заключением соглашения о взаимодействии с Федеральной службой безопасности Российской Федерации (Национальным координационным центром по компьютерным инцидентам), включающего в том числе права и обязанности сторон, порядок проведения совместных мероприятий, регламент информационного обмена, порядок и сроки представления отчетности, порядок и формы контроля;

2) силами структурного подразделения администрации Краснодарского края, ответственного за обеспечение информационной безопасности администрации Краснодарского края, с его аккредитацией как центра государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

3) силами организаций, являющихся аккредитованными центрами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

3.7. Ответственное лицо обеспечивает планирование и реализацию мероприятий по переводу систем и сетей на отечественные средства защиты информации, а также контроль за соблюдением запрета на использование средств защиты информации, странами происхождения которых являются иностранные государства в соответствии с пунктом 6 Указа Президента Российской Федерации от 1 мая 2022 г. № 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации".

3.8. Ответственное лицо сопровождает мероприятия по разработке (модернизации) систем и сетей в части информационной безопасности, а также требований нормативных правовых актов, нормативно-технических и методических документов по защите информации и выполнения этих требований.

3.9. Ответственное лицо организует работу по унификации способов и средств обеспечения информационной безопасности, иных технических

решений в администрации Краснодарского края и в подведомственных ей организациях.

3.10. Ответственное лицо организует принятие мер по совершенствованию обеспечения информационной безопасности администрации Краснодарского края и подведомственных ей организаций.

3.11. Ответственное лицо повышает на постоянной основе профессиональную компетенцию, знания и навыки в области обеспечения информационной безопасности.

3.12. Ответственное лицо выполняет иные обязанности, исходя из возложенных полномочий в рамках обеспечения информационной безопасности администрации Краснодарского края и подведомственных ей организаций.

3.13. Ответственное лицо:

1) соблюдает и обеспечивает выполнение законодательства Российской Федерации;

2) в случаях, установленных законодательством Российской Федерации, согласовывает политику с Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю;

3) представляет по запросам Федеральной службы безопасности Российской Федерации и Федеральной службы по техническому и экспортному контролю достоверные сведения о результатах реализации политики (фактически достигнутом эффекте и результате) и текущем уровне (состоянии) информационной безопасности в администрации Краснодарского края;

4) поддерживает уровень квалификации и постоянно развивает свои навыки в области информационной безопасности, необходимые для обеспечения информационной безопасности в администрации Краснодарского края;

5) организовывает при необходимости проведение и участвует в пределах своей компетенции в отраслевых, межотраслевых, межрегиональных и международных выставках, семинарах, конференциях, работе межведомственных рабочих групп, отраслевых экспертных сообществ, международных органов и организаций;

6) участвует в пределах компетенции в осуществлении закупок товаров, работ, услуг для обеспечения нужд в сфере информационной безопасности.

4. Права ответственного лица

Ответственное лицо имеет право:

1) давать указания и поручения государственным гражданским служащим в администрации Краснодарского края и работникам, замещающим должности, не являющиеся должностями государственной гражданской службы Краснодарского края, в части обеспечения информационной безопасности;

2) запрашивать от государственных гражданских служащих в администрации Краснодарского края и работников, замещающих должности, не являющиеся должностями государственной гражданской службы

Краснодарского края, информацию и материалы, необходимые для реализации возложенных на ответственное лицо прав и обязанностей;

3) участвовать в заседаниях (совещаниях) коллегиальных и иных органов администрации Краснодарского края, принятии решений по вопросам деятельности администрации Краснодарского края, а также по внесению предложений по совершенствованию деятельности администрации Краснодарского края;

4) участвовать в разработке политики, выносить политику на обсуждение, утверждение Совету по защите информации при администрации Краснодарского края либо иному коллегиальному органу администрации Краснодарского края по вопросам защиты информации;

5) представлять результаты реализации политики Совету по защите информации при администрации Краснодарского края либо иному коллегиальному органу администрации Краснодарского края по вопросам защиты информации;

6) принимать решения по вопросам обеспечения информационной безопасности администрации Краснодарского края;

7) взаимодействовать с Федеральной службой безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю и иными федеральными органами исполнительной власти по вопросам обеспечения информационной безопасности, в том числе по вопросам совершенствования законодательства Российской Федерации в области обеспечения информационной безопасности;

8) вносить предложения о привлечении организаций, имеющих соответствующие лицензии на деятельность в области защиты информации, в соответствии с законодательством Российской Федерации к проведению работ по обеспечению информационной безопасности;

9) инициировать проверки уровня (состояния) обеспечения информационной безопасности администрации Краснодарского края, иных органов исполнительной власти Краснодарского края, подведомственных администрации Краснодарского края организаций;

10) организовывать мероприятия по информационной безопасности, разработку и представление Губернатору Краснодарского края предложений по внесению изменений в процессы функционирования, принятию других мер, направленных на недопущение реализации негативных последствий;

11) получать доступ в установленном порядке к сведениям, составляющим государственную тайну, если исполнение обязанностей ответственного лица связано с использованием таких сведений и наличием необходимых прав и полномочий;

12) получать доступ в установленном порядке в связи с исполнением своих обязанностей в государственные органы, органы местного самоуправления, общественные объединения и другие организации;

13) обеспечивать надлежащие организационно-технические условия, необходимые для исполнения обязанностей ответственного лица.

5. Ответственность ответственного лица

Ответственное лицо в соответствии с законодательством Российской Федерации несет ответственность:

1) за неисполнение или ненадлежащее исполнение своих обязанностей;

2) за действия (бездействие), ведущие к нарушению прав и законных интересов администрации Краснодарского края;

3) за разглашение государственной тайны и иных сведений, ставших ему известными в связи с исполнением своих обязанностей;

4) за достижение целей обеспечения информационной безопасности;

5) за поддержание и непрерывное развитие информационной безопасности администрации Краснодарского края для исключения (невозможности реализации) негативных последствий;

6) за организацию мероприятий по разработке (модернизации) систем и сетей в части информационной безопасности администрации Краснодарского края;

7) за нарушения требований по обеспечению информационной безопасности;

8) за нарушения в обеспечении защиты систем и сетей, повлекшие негативные последствия.

Руководитель департамента
информатизации и связи
Краснодарского края С.В. Завальный