



**ПОСТАНОВЛЕНИЕ
ПРАВИТЕЛЬСТВА КАБАРДИНО-БАЛКАРСКОЙ РЕСПУБЛИКИ
КЪЭБЭРДЕЙ-БАЛЪКЪЭР РЕСПУБЛИКЭМ И ПРАВИТЕЛЬСТВЭМ И
УНАФЭ**

**КЪАБАРТЫ-МАЛЪЪАР РЕСПУБЛИКАНЫ ПРАВИТЕЛЬСТВОСУНУ
БЕГИМИ**

26 июля 2024 г.

№ 116-ПП

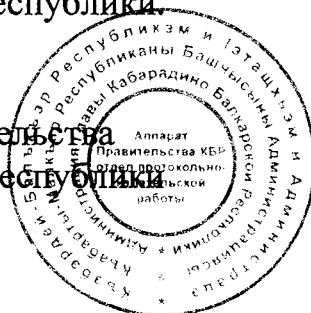
г. Нальчик

**Об утверждении Положения
о заместителе Председателя Правительства
Кабардино-Балкарской Республики,
ответственном за обеспечение информационной безопасности
в Правительстве Кабардино-Балкарской Республики**

В соответствии с подпунктом «а» пункта 1 Указа 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)» Правительство Кабардино-Балкарской Республики **п о с т а н о в л я е т :**

Утвердить прилагаемое Положение о заместителе Председателя Правительства Кабардино-Балкарской Республики, ответственном за обеспечение информационной безопасности в Правительстве Кабардино-Балкарской Республики.

Председатель Правительства
Кабардино-Балкарской Республики



А.Мусуков

УТВЕРЖДЕНО

постановлением Правительства
Кабардино-Балкарской Республики
от 26 июля 2024 г. № 116-ПП

ПОЛОЖЕНИЕ

о заместителе Председателя Правительства Кабардино-Балкарской Республики, ответственном за обеспечение информационной безопасности в Правительстве Кабардино-Балкарской Республики

I. Общие положения

1. Настоящее Положение определяет полномочия, права и обязанности заместителя Председателя Правительства Кабардино-Балкарской Республики, ответственного за обеспечение информационной безопасности в Правительстве Кабардино-Балкарской Республики (далее – Правительство), в том числе за обнаружение, предупреждение и ликвидацию последствий компьютерных атак, и реагирование на компьютерные инциденты (далее – ответственное лицо).

2. Ответственное лицо определяется решением Правительства.

3. Ответственное лицо входит в состав коллегиальных органов, созданных в целях обеспечения информационной безопасности.

4. Указания и поручения ответственного лица в части обеспечения информационной безопасности являются обязательными для исполнения всеми лицами, замещающими государственные должности, государственными служащими и работниками органов исполнительной власти.

II. Квалификационные требования к ответственному лицу

5. 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) он должен пройти обучение по программе профессиональной переподготовки по направлению «Информационная безопасность».

6. Для ответственного лица требуются наличие следующих знаний,

умений и профессиональных компетенций:

а) принципы организации деятельности, специфика обеспечения информационной безопасности в Правительстве;

б) влияние информационных технологий на деятельность Правительства, в том числе:

роль и место информационных технологий (степень интеграции информационных технологий в деятельности Правительства);

зависимость основных процессов функционирования Правительства от информационных технологий;

в) информационно-телекоммуникационные технологии, в том числе:

современные информационно-телекоммуникационные технологии, используемые в Правительстве;

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 оснащённости программными (программно-техническими) средствами;

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

г) 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 Правительства, реализации и контроля их достижения;

принципы и направления стратегического развития информационной безопасности в Правительстве;

правила разработки, утверждения и отмены организационно-распорядительных документов по вопросам обеспечения информационной безопасности в органе, состав и содержание таких документов;

порядок организации работ по обеспечению информационной безопасности в Правительстве;

основные негативные последствия, наступление которых возможно в результате реализации угроз безопасности информации, способы и методы обеспечения и поддержания необходимого уровня (состояния) информационной безопасности Правительства для исключения (невозможности реализации) негативных последствий, а также порядок

проведения практических проверок и контроля результативности применяемых способов и методов обеспечения информационной безопасности Правительства;

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 органов исполнительной власти Кабардино-Балкарской Республики 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 в Правительстве;

формулирование измеримых и практических результатов деятельности по обеспечению информационной безопасности Правительства;

организация разработки политики (правил, процедур), регламентирующей вопросы информационной безопасности в Правительстве (далее – политика);

внедрение политики;

организация контроля и анализа применения политики;

организация мероприятий по разработке единых инструментов и механизмов контроля и органах исполнительной власти Кабардино-Балкарской Республики;

поддержка и совершенствование деятельности по обеспечению информационной безопасности в Правительстве и органах исполнительной власти Кабардино-Балкарской Республики;

организация мероприятий по определению угроз безопасности информации систем и сетей, а также по формированию требований к обеспечению информационной безопасности в Правительстве;

организация внедрения способов и средств для обеспечения информационной безопасности в Правительстве и органах исполнительной власти Кабардино-Балкарской Республики;

организация мероприятий по анализу и контролю состояния информационной безопасности Правительства и модернизации (трансформации) процессов функционирования Правительства в целях

обеспечения информационной безопасности в Правительстве;

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 Правительства и реагированию на компьютерные инциденты;

организация мероприятий по отслеживанию и контролю достижения целей информационной безопасности (фактически достигнутый эффект и результат) в Правительстве и органах исполнительной власти Кабардино-Балкарской Республики.

7. От ответственного лица требуется знание нормативных правовых актов Российской Федерации, методических документов, международных и национальных стандартов в области:

а) защиты государственной тайны;

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

в) обеспечения безопасности критической информационной инфраструктуры Российской Федерации;

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

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

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

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

III. Должностные обязанности ответственного лица

8. Ответственное лицо принимает участие в формировании политики Правительства, отвечает за согласование стратегии развития Правительства в части вопросов обеспечения информационной безопасности.

9. Ответственное лицо организует:

а) разработку политики, направленной на обеспечение и поддержание стабильной деятельности Правительства и процессов его функционирования в случае проведения компьютерных атак, отвечает за согласование и утверждение политики в Правительстве, реализацию мероприятий, предусмотренных политикой, отслеживает и контролирует результаты реализации политики;

б) работу по обеспечению информационной безопасности Правительства, 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;

в) реализацию и контроль проведения в Правительстве 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;

г) беспрепятственный доступ (в том числе удаленный) должностным лицам Федеральной службы безопасности Российской Федерации и ее территориальных органов к информационным ресурсам, принадлежащим Правительству либо используемым Правительством, доступ к которым обеспечивается посредством использования информационно-телекоммуникационной сети «Интернет», в целях осуществления мониторинга их защищенности, а также работникам органов исполнительной власти, осуществляющих функции по обеспечению информационной безопасности;

д) 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 Правительству либо используемых Правительством, доступ к которым обеспечивается посредством использования информационно-телекоммуникационной сети «Интернет»;

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

ж) развитие информационной безопасности, формирование и развитие навыков работников органов исполнительной власти Кабардино-Балкарской Республики в сфере информационной безопасности;

з) разработку и реализацию мероприятий по обеспечению информационной безопасности в Правительстве в соответствии

с требованиями к обеспечению информационной безопасности, установленными федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации;

и) контроль пользователей информационных ресурсов Правительства в части соблюдения ими режима конфиденциальности информации, правил работы со съемными машинными носителями информации, выполнения организационных и технических мер по защите информации;

к) планирование мероприятий по обеспечению информационной безопасности в Правительстве и органах исполнительной власти Кабардино-Балкарской Республики;

л) подготовку правовых актов, иных организационно-распорядительных документов по вопросам обеспечения информационной безопасности в Правительстве, осуществляет согласование иных документов органа в части обеспечения информационной безопасности;

м) проведение научно-исследовательских и опытно-конструкторских работ по вопросам обеспечения информационной безопасности в Правительстве и органах исполнительной власти Кабардино-Балкарской Республики;

н) проведение контроля за состоянием обеспечения информационной безопасности в Правительстве и органах исполнительной власти Кабардино-Балкарской Республики, включая оценку защищенности систем и сетей, операторами которых являются Правительство, органы исполнительной власти Кабардино-Балкарской Республики и их подведомственные организации.

10. Ответственное лицо осуществляет:

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

б) регулярное и своевременное информирование Председателя Правительства Кабардино-Балкарской Республики о компьютерных инцидентах, текущем уровне (состоянии) информационной безопасности в Правительстве и результатах практических учений по противодействию компьютерным атакам;

в) контроль за ведением организационно-распорядительной документации и отчетности по вопросам информационной безопасности;

г) согласование требований к системам и сетям, оператором которых является Правительство, органы исполнительной власти Кабардино-Балкарской Республики и их подведомственные организации, в части обеспечения информационной безопасности.

11. Ответственное лицо:

а) организует и контролирует проведение мероприятий по анализу и оценке состояния информационной безопасности Правительства и контролирует их результаты;

б) организует и контролирует функционирование системы обеспечения информационной безопасности в Правительстве, координирует функционирование систем обеспечения информационной безопасности в органах исполнительной власти Кабардино-Балкарской Республики.

12. Ответственное лицо согласовывает политику, технические задания и иную основополагающую документацию в сфере информационных технологий, цифровизации и цифровой трансформации Правительства.

13. 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 Правительства, а также взаимодействие с Национальным координационным центром по компьютерным инцидентам одним (или несколькими) из следующих способов:

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

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

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

14. 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».

15. 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.

16. Ответственное лицо проводит работу по унификации способов и средств по обеспечению информационной безопасности, иных технических решений в Правительстве и органах исполнительной власти Кабардино-Балкарской Республики.

17. Ответственное лицо принимает меры по совершенствованию обеспечения информационной безопасности в Правительстве и органах исполнительной власти Кабардино-Балкарской Республики.

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

19. Ответственное лицо выполняет иные обязанности, исходя из возложенных полномочий и поставленных Председателем Правительства Кабардино-Балкарской Республики задач в рамках обеспечения информационной безопасности Правительства и органов исполнительной власти Кабардино-Балкарской Республики.

20. Ответственное лицо:

а) соблюдает и обеспечивает выполнение законодательства Российской Федерации;

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

в) 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 Правительстве;

г) поддерживает уровень квалификации и постоянно развивает свои навыки в области информационной безопасности, необходимые

для обеспечения информационной безопасности в Правительстве;

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

IV. Права ответственного лица

21. Ответственное лицо имеет право:

а) давать указания и поручения лицам, замещающим государственные должности, государственным служащим и работникам органов исполнительной власти в части обеспечения информационной безопасности;

б) запрашивать от лиц, замещающих государственные должности, государственных служащих и работников органов исполнительной власти информацию и материалы, необходимые для реализации возложенных на ответственное лицо прав и обязанностей;

в) участвовать в заседаниях (совещаниях) коллегиальных органов Правительства, принятии решений по вопросам деятельности Правительства, а также по внесению предложений по совершенствованию деятельности Правительства;

г) участвовать в разработке политики, выносить политику на обсуждение и утверждение Правительством;

д) представлять результаты реализации политики Правительству;

е) принимать решения по вопросам обеспечения информационной безопасности Правительства;

ж) 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;

з) 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;

и) инициировать проверки уровня (состояния) обеспечения информационной безопасности в Правительстве и органах исполнительной власти Кабардино-Балкарской Республики;

к) организовывать на объектах Правительства мероприятия по информационной безопасности, разработку и представление

Правительству предложений по внесению изменений в процессы функционирования, принятию других мер, направленных на недопущение реализации негативных последствий;

л) 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;

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

V. Ответственность ответственного лица

22. Ответственное лицо в соответствии с законодательством Российской Федерации несет ответственность за:

а) неисполнение или ненадлежащее исполнение своих обязанностей;

б) действия (бездействие), ведущие к нарушению прав и законных интересов Правительства;

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

г) достижение целей обеспечения информационной безопасности;

д) за поддержание и непрерывное развитие информационной безопасности Правительства для исключения (невозможности реализации) негативных последствий;

е) организацию мероприятий по разработке (модернизации) систем и сетей в части информационной безопасности Правительства;

ж) нарушения требований по обеспечению информационной безопасности;

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

Сергей / Березов А.Р.