ПРАВИТЕЛЬСТВО КАЛИНИНГРАДСКОЙ ОБЛАСТИ

П О С Т А Н О В Л Е Н И Е

от 01 октября 2024 г. № 376-п
Калининград

Об утверждении политики информационной безопасности в Правительстве Калининградской области

В соответствии с Указом Президента Российской Федерации от 01 мая 2022 года № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» Правительство Калининградской области **п о с т а н о в л я е т:**

1. Утвердить прилагаемую политику информационной безопасности в Правительстве Калининградской области.

2. Постановление вступает в силу со дня его официального опубликования.

Губернатор
Калининградской области А.С. Беспрозванных

УТВЕРЖДЕНА
постановлением Правительства
Калининградской области
от 01 октября 2024 г. № 376-п

ПОЛИТИКА
информационной безопасности в Правительстве Калининградской области

Глава 1. Общие положения

1. Настоящая политика является документом в сфере обеспечения информационной безопасности в Правительстве Калининградской области (далее – информационная безопасность), определяет принципы формирования системы информационной безопасности, субъектов, ответственных за организацию и поддержание информационной безопасности, объекты, подлежащие защите, средства защиты информации и меры по обеспечению информационной безопасности, правовую основу обеспечения информационной безопасности и направлена на формирование системы информационной безопасности.

2. Настоящая политика основывается на положениях Конституции Российской Федерации, федеральных конституционных законов, федеральных законов, актов Президента Российской Федерации и актов Правительства Российской Федерации, международных договоров Российской Федерации, нормативных правовых актов федеральных органов исполнительной власти, уполномоченных в области обеспечения информационной безопасности, других нормативных правовых документов в сфере обеспечения информационной безопасности, а также правовых актов Калининградской области.

3. Целью настоящей политики является формирование системы информационной безопасности посредством закрепления положений, регламентирующих организацию и поддержание информационной безопасности.

4. Работники Правительства Калининградской области, а также юридические, физические лица и индивидуальные предприниматели, допущенные в Правительстве Калининградской области к работе в единой информационно-телекоммуникационной сети Правительства Калининградской области для проведения работ по гражданско-правовым договорам (далее – работники), должны руководствоваться положениями настоящей политики.

Глава 2. Принципы формирования системы информационной безопасности

5. Формирование системы информационной безопасности основывается

на принципах:

1) законности;

2) системности;

3) комплексности защиты информации;

4) непрерывности защиты информации;

5) своевременности защиты информации;

6) непрерывности совершенствования и преемственности;

7) разумной достаточности (экономической целесообразности);

8) персональной ответственности;

9) минимизации полномочий;

10) гибкости;

11) открытости алгоритмов и механизмов защиты информации;

12) простоты применения средств защиты информации;

13) обоснованности и технической реализуемости;

14) специализации и профессионализма;

15) обязательности контроля.

6. Принцип законности предполагает разработку системы информационной безопасности и ее функционирование в соответствии с законодательством Российской Федерации.

7. Принцип системности предполагает формирование системы информационной безопасности как совокупности взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблем обеспечения информационной безопасности.

8. Принцип комплексности защиты информации предполагает согласованное принятие мер по созданию правовых, технических, организационных и финансовых условий в целях регулирования, реализации, развития информационной безопасности и осуществление разнородных мероприятий по обеспечению информационной безопасности, функционирующих согласованно, взаимно дополняющих друг друга в практическом и техническом смыслах.

9. Принцип непрерывности защиты информации означает, что обеспечение защиты информации должно осуществляться непрерывно и целенаправленно.

10. Принцип своевременности защиты информации предполагает упреждающий характер принятия мер по созданию правовых, технических, организационных и финансовых условий в целях регулирования, реализации и развития информационной безопасности, внедрения средств информационной безопасности и реализации мероприятий по обеспечению информационной безопасности.

11. Принцип непрерывности совершенствования и преемственности предполагает постоянное совершенствование системы информационной безопасности на основе преемственности организационных и технических решений, технических и технологических наработок, анализа функционирования информационных систем и системы их защиты с учетом

изменений методов и средств неправомерного получения информации с использованием технических средств, осуществляющих обнаружение, прием и обработку информативных сигналов, нормативных требований по защите информации, а также с учетом достигнутого опыта субъектов Российской Федерации в сфере информационной безопасности.

12. Принцип разумной достаточности (экономической целесообразности) предполагает соответствие уровня затрат на обеспечение информационной безопасности ценности информационных ресурсов и величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения.

13. Принцип персональной ответственности предполагает возложение ответственности за нарушение информационной безопасности в соответствии с положениями настоящей политики на каждого работника в рамках его должностного регламента (инструкции) и (или) трудового договора.

14. Принцип минимизации полномочий означает предоставление работникам прав доступа к совокупности информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров, только в тех случае и объеме, какие необходимы для выполнения их должностных (служебных) обязанностей.

15. Принцип гибкости предполагает способность системы информационной безопасности реагировать на изменения внешней среды и условий осуществления Правительством Калининградской области своей деятельности, в том числе на изменения организационной и штатной структуры Правительства Калининградской области, изменения существующих информационных систем или введение в эксплуатацию новых информационных систем и новых технических средств.

16. Принцип открытости алгоритмов и механизмов защиты информации состоит в том, что защита информации не должна обеспечиваться только за счет конфиденциальности структурной организации и алгоритмов функционирования ее подсистем, а знание алгоритмов работы системы защиты информации не должно давать возможность ее преодоления (даже ее разработчикам), при этом информация об используемых системах и механизмах защиты информации не должна быть общедоступна.

17. Принцип простоты применения средств защиты информации заключается в том, что механизмы и методы защиты информации должны быть интуитивно понятны и просты в использовании. Применение средств защиты информации не должно быть связано с выполнением действий, требующих значительных дополнительных трудозатрат или малопонятных для квалифицированного пользователя действий.

18. Принцип обоснованности и технической реализуемости заключается в том, что информационные технологии, технические и программные средства,

средства и меры защиты информации должны быть реализованы в соответствии с требованиями законодательства Российской Федерации, обоснованы с точки зрения достижения необходимого уровня информационной безопасности и экономической целесообразности, а также должны соответствовать установленным нормам и требованиям информационной безопасности.

19. Принцип специализации и профессионализма предполагает привлечение к реализации мер по созданию правовых, технических, организационных и финансовых условий в целях регулирования, реализации, развития информационной безопасности и осуществление разнородных мероприятий по обеспечению информационной безопасности лицами, специализирующимися на обеспечении информационной безопасности, имеющими опыт практической работы в этой области.

20. Принцип обязательности контроля предполагает обязательность и своевременность выявления и пресечения попыток нарушения в Правительстве Калининградской области установленных правил, обеспечения информационной безопасности на основе используемых систем, средств защиты информации, средств оперативного контроля и регистрации.

Глава 3. Субъекты, ответственные за организацию и поддержание информационной безопасности, и объекты, подлежащие защите от компьютерных инцидентов, которые могут привести к сбоям или нарушению функционирования государственных информационных систем Калининградской области и информационных систем Калининградской области и (или) возникновению угроз безопасности информации

21. Деятельность по обеспечению информационной безопасности, в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты, которые могут привести к сбоям или нарушению функционирования государственных информационных систем Калининградской области и информационных систем Калининградской области и (или) возникновению угроз безопасности информации (далее – инциденты), координируется заместителем Председателя Правительства Калининградской области – министром цифровых технологий и связи Калининградской области, ответственным за обеспечение информационной безопасности в соответствии с распределением обязанностей между членами Правительства Калининградской области.

22. Информационную безопасность обеспечивает Отдел по обеспечению информационной безопасности Правительства Калининградской области во взаимодействии с Министерством цифровых технологий и связи Калининградской области и государственным казенным учреждением Калининградской области «Центр цифровых технологий» (далее – учреждение).

23. Объектами, подлежащими защите от инцидентов, являются:

1) государственные информационные системы Калининградской области и информационные системы Калининградской области, созданные

Правительством Калининградской области (в том числе машинные носители информации, автоматизированные рабочие места, серверы, средства обработки буквенно-цифровой, графической, видео- и речевой информации, микропрограммное, общесистемное, прикладное программное обеспечение) (далее – информационные системы);

2) информационно-телекоммуникационные сети, используемые Правительством Калининградской области (в том числе телекоммуникационное оборудование, программное обеспечение, система управления, линии связи), формирующие единое информационное пространство и цифровую среду взаимодействия;

3) служебные цифровые устройства и периферийное оборудование (в том числе принтеры, сканеры, ip-телефоны, цифровые камеры, смартфоны), используемые работниками;

4) сети электросвязи, используемые для организации взаимодействия Правительства Калининградской области с иными физическими и юридическими лицами и передачи информации, места выхода в информационно-телекоммуникационную сеть «Интернет»;

5) архитектура и конфигурация информационных систем, информационно-телекоммуникационных сетей и систем информационной безопасности, используемых Правительством Калининградской области (персональные данные, иная информация конфиденциального характера, в том числе представляющая коммерческую ценность в силу неизвестности третьим лицам).

Глава 4. Средства защиты информации и меры по обеспечению информационной безопасности

24. В целях защиты информации в Правительстве Калининградской области применяются средства защиты информации, входящие в государственный реестр сертифицированных средств защиты информации, формируемый Федеральной службой по техническому и экспортному контролю.

25. В состав мер по обеспечению информационной безопасности входят:

1) идентификация и аутентификация работников и объектов, подлежащих защите от инцидентов;

2) управление доступом работников к объектам, подлежащим защите от инцидентов;

3) ограничение программной среды;

4) защита машинных носителей информации, на которых хранится и (или) обрабатывается информация;

5) регистрация событий безопасности;

6) антивирусная защита;

7) обнаружение (предотвращение) вторжений;

8) контроль (анализ) защищенности информации;

9) обеспечение целостности;

10) обеспечение доступности;

11) защита среды виртуализации;

12) защита технических средств;

13) защита информационных систем;

14) выявление инцидентов и реагирование на них;

15) управление конфигурациями информационных систем и систем защиты информации.

26. Меры по идентификации и аутентификации работников и объектов, подлежащих защите от инцидентов, должны обеспечивать присвоение работникам и объектам, подлежащим защите от инцидентов, уникальных признаков (идентификаторов) (далее – идентификаторы), сравнение предъявляемого работниками и объектами, подлежащими защите от инцидентов, идентификаторов с перечнем присвоенных идентификаторов, а также проверку принадлежности работникам и объектам, подлежащим защите от инцидентов, предъявленного им идентификатора (подтверждение подлинности).

27. Меры по управлению доступом работников к объектам, подлежащим защите от инцидентов, должны обеспечивать управление правами и привилегиями работников, разграничение доступа работников к объектам, подлежащим защите от инцидентов, на основе совокупности установленных в информационных системах правил разграничения доступа, а также обеспечивать контроль за соблюдением этих правил.

28. Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационных системах программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационных системах программного обеспечения.

29. Меры по защите машинных носителей информации (средств обработки (хранения) информации, съемных машинных носителей информации) должны исключать возможность несанкционированного доступа к машинным носителям и хранящейся на них информации, а также несанкционированное использование съемных машинных носителей информации.

30. Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационных системах, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

31. Меры по антивирусной защите должны обеспечивать обнаружение в информационных системах компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение таких программ и информации.

32. Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационных системах, направленных на несанкционированный доступ к информации, специальных воздействий на информационные системы и (или) информацию в целях

добывания, уничтожения, искажения информации и блокирования доступа к информации, а также реагирование на эти действия.

33. Меры по контролю (анализу) защищенности информации должны обеспечивать контроль уровня защищенности информации путем проведения систематических мероприятий по обеспечению информационной безопасности и тестированию работоспособности системы защиты.

34. Меры по обеспечению целостности должны обеспечивать обнаружение фактов несанкционированного доступа к информации, а также возможность восстановления информации.

35. Меры по обеспечению доступности должны обеспечивать авторизованный доступ пользователей, имеющих права доступа, к информации.

36. Меры по защите среды виртуализации должны исключать несанкционированный доступ к информации, обрабатываемой в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействие на них, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также к системе резервного копирования и создаваемым ею копиям.

37. Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим информацию, средствам, обеспечивающим функционирование информационных систем, и в помещения, в которых они постоянно расположены, и обеспечивать защиту технических средств от внешних воздействий, а также защиту информации, представленной в виде информативных электрических сигналов и физических полей.

38. Меры по защите информационных систем, ее средств, систем связи и передачи данных должны обеспечивать защиту информации при взаимодействии информационных систем или их отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение информационной безопасности.

39. Меры по выявлению инцидентов и реагированию на них должны обеспечивать обнаружение, идентификацию, анализ инцидентов в информационных системах, а также принятие мер по устранению и предупреждению инцидентов.

40. Меры по управлению конфигурациями информационных систем и систем защиты информации должны обеспечивать управление изменениями конфигурации информационных систем и системы защиты информации, анализ потенциального воздействия планируемых изменений на обеспечение безопасности информации, а также документирование этих изменений.

Глава 5. Правовая основа обеспечения информационной безопасности

41. В целях обеспечения информационной безопасности разрабатываются для использования в работе и поддерживаются в актуальном состоянии следующие локальные нормативные акты:

1) план (программа) работ по обеспечению информационной безопасности;

2) руководство по защите в Правительстве Калининградской области информации, не содержащей сведения, составляющие государственную тайну;

3) руководство по организации в Правительстве Калининградской области защиты информации, содержащей сведения, составляющие служебную тайну;

4) модели угроз безопасности в Правительстве Калининградской области;

5) о защите персональных данных при их обработке в Правительстве Калининградской области;

6) инструкцию по использованию в Правительстве Калининградской области средств защиты информации;

7) инструкцию по организации в Правительстве Калининградской области антивирусной защиты в информационных системах;

8) инструкцию по организации в Правительстве Калининградской области парольной защиты в информационных системах;

9) инструкцию для пользователей по обеспечению в Правительстве Калининградской области правил информационной безопасности при работе в информационных системах;

10) инструкцию по учету, маркировке, очистке и утилизации машинных носителей информации в Правительстве Калининградской области;

11) инструкцию по обеспечению в Правительстве Калининградской области информационной безопасности при подключении и использовании информационно-вычислительной сети общего пользования.

42. Для соблюдения требований информационной безопасности разрабатываются организационно-распорядительные документы, регламентирующие в Правительстве Калининградской области порядок и правила:

1) создания, управления учетными данными и предоставления прав доступа к информационным ресурсам;

2) организации парольной защиты;

3) организации работы в единой информационно-телекоммуникационной сети Правительства Калининградской области;

4) безопасной работы пользователей с информационными ресурсами;

5) организации антивирусной защиты;

6) использования служебной электронной почты;

7) безопасного взаимодействия с информационно-телекоммуникационной сетью «Интернет»;

8) осуществления удаленной работы с информационными ресурсами;

9) подключения к другим информационным системам и сетям передачи

данных (в том числе беспроводным, а также предоставляемым в рамках исполнения гражданско-правовых договоров);

10) резервного копирования и восстановления информационных ресурсов;

11) обращения с машинными носителями информации ограниченного доступа;

12) осуществления мониторинга и контроля состояния информационной безопасности, обнаружения, предупреждения и ликвидации последствий компьютерных атак;

13) реагирования на инциденты;

14) взаимодействия с Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности в части информационной безопасности.

Глава 6. Ответственность

43. Правительство Калининградской области, Министерство цифровых технологий и связи Калининградской области и учреждение совместно несут ответственность за планирование, организацию, реализацию и контроль мероприятий по обеспечению информационной безопасности в Правительстве Калининградской области в соответствии с законодательством Российской Федерации.

44. За нарушение требований настоящей политики работники несут ответственность в соответствии с законодательством Российской Федерации.